

PRAKSISOVERSIGTER • SAMLET UDGAVE

Praksis inden for *IT-ret*

Databeskyttelse og digital forvaltning – Datatilsynets praksis.

OVERSIGTER

18

AFGØRELSE

492

PERIODE

2002–2026

18 OVERSIGTER

Indhold

01	AI-forordningen – risikoklassificering, tilsyn og sanktioner	22 afg.
02	AI-systemer og persondata	23 afg.
03	Cookies og samtykke	14 afg.
04	Databedrageri (§ 279 a) – doktrin og afgrænsning	7 afg.
05	Datatilsynets afgørelser	86 afg.
06	Datatilsynsbøder og GDPR-overtrædelser (databrud)	58 afg.
07	DSA/DMA – platformes due diligence-forpligtelser og håndhævelse	20 afg.
08	GDPR-erstatning (databeskyttelsesforordningen art. 82)	20 afg.
09	Hacking og uberettiget adgang til IT-systemer (§ 263, § 263 a)	12 afg.
10	IT-leverancekontrakter – forsinkelse, mangler og ophævelse	41 afg.
11	MitID / NemID-misbrug og digital identitetstyveri	34 afg.
12	MobilePay og betalingstjeneste-bedrageri	18 afg.
13	Obligatorisk digital post, fritagelse og MitID-forvaltning	36 afg.
14	Persondatabehandling i ansættelsesforhold	21 afg.
15	Platformsansvar for ulovligt indhold (DSA, DMA og AVMS)	14 afg.
16	Ret til at blive glemt	19 afg.
17	Sletning fra RKI / Experian – kreditoplysningsbureauer (DBL §§ 19-22)	25 afg.
18	SMS-phishing / smishing-bedrageri	22 afg.

Hver oversigt er et selvstændigt kapitel med introduktion, principper, gennemgang, lovgrundlag og citerede afgørelser. Titlerne er klikbare, og kapitlerne findes også som bogmærker i PDF-læseren.

01

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over AI-forordningen – risikoklassificering, tilsyn og sanktioner

Fra forbudt AI-praksis til bødeudmåling – dansk tilsynsarkitektur og den praksis der findes indtil videre

Version 2 · Opdateret 3. sep. 2026 · 22 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

AI-forordningen (forordning (EU) 2024/1689) indfører en risikobaseret regulering af kunstig intelligens med fire niveauer – forbudt praksis, højrisiko, gennemsigtighedspligtig og fri anvendelse – og suppleres i Danmark af lov om supplerende bestemmelser til forordningen om kunstig intelligens (lov nr. 467 af 14. maj 2025), der udpeger Digitaliseringsstyrelsen, Datatilsynet og Domstolsstyrelsen som nationale kompetente myndigheder og strafbelægger overtrædelser med bøde. Egentlig forordningspraksis findes endnu ikke: der er hverken offentliggjorte afgørelser om forbudt AI-praksis eller domme om bødeudmåling efter gennemførelseslovens § 10. Til gengæld er der en betydelig og retningsgivende praksis fra Datatilsynet, EU-Domstolen, Folketingets Ombudsmand og Ligebehandlingsnævnet om de samme materielle spørgsmål – behandlingsgrundlag for AI-løsninger, biometri, forklaringspligt ved automatiserede afgørelser, menneskeligt tilsyn og algoritmisk profilering – som med stor sandsynlighed bliver den fortolkningsmæssige rygrad, når forordningen skal håndhæves.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** AI-forordningen finder anvendelse trinvist: forbudte AI-praksisser fra 2. februar 2025, sanktionskapitlet fra 2. august 2025, hovedparten fra 2. august 2026 og produktrelateret højrisiko efter art. 6, stk. 1, først fra 2. august 2027 – forbudt AI-praksis kunne derfor først sanktioneres fra august 2025.
- 02** Danmark er som følge af retsforbeholdet ikke bundet af art. 5, stk. 1, litra h (realtids fjernidentifikation til retshåndhævelse), af stk. 2-6, af art. 26, stk. 10, og af litra d og g i det omfang de vedrører politisamarbejde og retligt samarbejde i straffesager.
- 03** Tilsynet er delt: Digitaliseringsstyrelsen dækker art. 5, stk. 1, litra a-c og e-f og er tillige bemyndigende myndighed og centralt kontaktpunkt; Datatilsynet dækker litra d og g uden for retsforbeholdet; Domstolsstyrelsen dækker domstolenes administrative AI-brug.
- 04** Bruger domstolene AI som led i deres judicielle funktion, træffes afgørelsen af vedkommende ret selv med kæreadgang til højere ret inden for en frist på 4 uger – ikke af en markedsovervågningsmyndighed.

- 05** De nationale kompetente myndigheders afgørelser kan ikke påklages administrativt, jf. gennemførelseslovens § 3; prøvelsen sker direkte ved domstolene efter grundlovens § 63, hvilket ifølge forarbejderne er nødvendigt for at sikre den uafhængighed forordningens art. 70, stk. 1, kræver.
- 06** Markedsovervågningsmyndighederne har adgang til erhvervsmæssige lokaliteter uden retskendelse, kan foretage tekniske undersøgelser af AI-systemet på stedet, lade sig bistå af uafhængige sagkyndige og kræve politiets bistand.
- 07** Overtrædelse af art. 5, stk. 1, litra a-g sanktioneres i dansk ret som strafferetlig bøde efter § 10 – ikke som administrativ bøde – men bødeudmålingen skal følge forordningens art. 99, stk. 3 og 5 (loft på 35 mio. EUR/7 % henholdsvis 7,5 mio. EUR/1 %) og hensynene i art. 99, stk. 7.
- 08** Forældelsesfristen er sat til 5 år i § 10, stk. 4 – en bevidst fravigelse af straffelovens § 93, stk. 11, om 2 år, begrundet i sagernes forventede størrelse og kompleksitet.
- 09** Offentlige myndigheder kan kun ifalde strafansvar efter straffelovens kap. 5, når de optræder som driftsherre på linje med private; lovovertrædelser begået som led i myndighedsudøvelse kan alene udløse personligt strafansvar.
- 10** Datatilsynet skelner skarpt mellem udvikling og drift af AI-løsninger: eksisterende opgavehjemler kan bære udviklings- og gentræningsfasen, men driften af en beslutningsstøttende AI-løsning kræver et klarere supplerende nationalt retsgrundlag.
- 11** Automatiseringsbias – at sagsbehandlere tillægger AI-outputtet større vægt end egen faglig vurdering – indgår som selvstændigt skærpende hensyn både i Datatilsynets vurdering af indgriben og i forordningens art. 14, stk. 4, litra b, om menneskeligt tilsyn.
- 12** EU-Domstolen kræver, at den dataansvarlige forklarer den konkret anvendte procedure og de anvendte principper bag en automatiseret afgørelse i kortfattet og letforståelig form; forretningshemmeligheder kan ikke generelt afskære indsigten, men skal afvejes konkret af tilsynsmyndigheden eller domstolen.
- 13** Ren stemmeanalyse uden stemmegenkendelse er ikke biometrisk behandling omfattet af forbuddet i GDPR art. 9, stk. 1, når formålet ikke er entydig identifikation – en sontring der er direkte relevant for afgrænsningen af følelsesgenkendelse og biometrisk kategorisering i AI-forordningens art. 5, stk. 1, litra f og g.
- 14** Dansk domspraksis om kunstig intelligens er indtil videre udelukkende strafferetlig og hviler på straffeloven – ikke på AI-forordningen; AI-genereret materiale bedømmes efter de almindelige gerningsindhold.

Den risikobaserede arkitektur og den trinvis anvendelse fra februar 2025 til august 2027

§ 1

AI-forordningen bygger på en risikopyramide: nogle former for AI-praksis er helt forbudt, en større gruppe klassificeres som højrisiko med krav til risikostyring, datakvalitet, dokumentation og menneskeligt tilsyn, en tredje gruppe er alene underlagt gennemsigtighedsforpligtelser, og resten er ureguleret. Forordningen trådte i kraft 2. august 2024, men anvendelsen er trinvis efter [artikel 113](#):

Bestemmelser	Anvendelse fra
Kapitel I (almindelige bestemmelser) og kapitel II (forbudte former for AI-praksis)	2. februar 2025
Kapitel III, afd. 4 (bemyndigende myndigheder og bemyndigede organer), kapitel V (AI-modeller til almen brug), VII (forvaltning), XII (sanktioner) samt art. 78 – dog ikke art. 101	2. august 2025
Forordningen i øvrigt	2. august 2026
Art. 6, stk. 1, om produktrelateret højrisiko og de tilsvarende forpligtelser	2. august 2027

Denne forskydning har en konkret retlig konsekvens, som lovgiver udtrykkeligt fremhævede i de almindelige bemærkninger til L 154: forbuddene galdt fra februar 2025, men kunne ikke sanktioneres, før sanktionskapitlet fandt anvendelse.

Kapitel XII om sanktioner finder imidlertid først anvendelse fra den 2. august 2025. Forbudte former for AI-praksis kan derfor først medføre sanktioner fra den 2. august 2025.

Den danske gennemførelseslov trådte følgelig i kraft netop den 2. august 2025, jf. [§ 12](#), og gælder ikke for Færøerne og Grønland, jf. [§ 13](#). Loven supplerer forordningen, hvis fulde tekst er optaget som bilag 1 til loven af rent praktiske hensyn – forordningen har direkte virkning i Danmark efter TEUF artikel 288, jf. [artikel 288 i TEUF](#).

Loven i sin nuværende skikkelse dækker altså kun det første trin. Digitaliseringsministeriet anførte allerede i forarbejderne, at der ville komme yderligere lovgivning: »Digitaliseringsministeriet vil hertil fremsætte forslag til yderligere supplerende lovgivning til de øvrige kapitler i forordningen om kunstig intelligens forud for, at disse dele af forordningen om kunstig intelligens skal finde anvendelse.« Det skete med [L 111 \(2025-26\)](#), fremsat 18. februar 2026, som skulle ophæve den gældende lov og etablere den fulde tilsyns- og sanktionsramme fra 2. august 2026. Lovforslaget bortfaldt ved samlingens afslutning.

LOV

AI-forordningen § 113

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 12](#)

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 13](#)

De otte forbudte former for AI-praksis i artikel 5 – og de dele

§ 2 Danmark ikke er bundet af

[Artikel 5, stk. 1](#) opregner otte former for AI-praksis, der er forbudt i EU:

- **litra a** – subliminale teknikker ud over den menneskelige bevidsthed eller bevidst manipulerende/vildledende teknikker, der i væsentlig grad fordrejer adfærden og forvolder betydelig skade
-

litra b – udnyttelse af sårbarheder på grundlag af alder, handicap eller en særlig social eller økonomisk situation

- **litra c** – social scoring, hvor evaluering eller klassificering over tid fører til skadelig eller ugunstig behandling
- **litra d** – prædiktiv politiarbejde-profilering, dvs. risikovurdering af, om en fysisk person vil begå en strafbar handling, når vurderingen *alene* er baseret på profilering eller vurdering af personlighedstræk
- **litra e** – opbygning eller udvidelse af ansigtsgenkendelsesdatabaser gennem ikkemåltrettet skrabning af ansigtsbilleder fra internettet eller kameraovervågning
- **litra f** – følelsesgenkendelse på arbejdspladser og uddannelsesinstitutioner, medmindre anvendelsen sker af medicinske eller sikkerhedsmæssige årsager
- **litra g** – biometrisk kategorisering med henblik på at udlede race, politiske anskuelser, fagforeningsmedlemskab, religiøs eller filosofisk overbevisning, seksuelle forhold eller seksuel orientering
- **litra h** – realtids biometrisk fjernidentifikation på offentlige steder med henblik på retshåndhævelse

Forbuddene er ikke absolutte i deres afgrænsning. Litra d finder ikke anvendelse på AI-systemer, der understøtter den menneskelige vurdering af en persons involvering i kriminel aktivitet, når vurderingen allerede hviler på objektive og verificerbare kendsgerninger direkte knyttet til den kriminelle aktivitet. Og litra g omfatter ikke mærkning eller filtrering af lovligt indhentede biometriske datasæt.

Retsforbeholdets rækkevidde. Forordningen er vedtaget med hjemmel i både artikel 114 og artikel 16 i TEUF, og de dele, der hviler på artikel 16 og vedrører behandling af personoplysninger under TEUF tredje del, afsnit V, kapitel 4 eller 5, er efter artikel 2a i protokol nr. 22 ikke bindende for Danmark. De almindelige bemærkninger til L 154 opregner præcist, hvad det omfatter:

Det følger af præambelbetragtning nr. 41 i forordningen om kunstig intelligens, at i medfør af artikel 2 og 2a i protokol nr. 22 om Danmarks stilling, er de regler, der er fastsat i artikel 5, stk. 1, litra g, i forordningen om kunstig intelligens, i det omfang den finder anvendelse på brugen af systemer til biometrisk kategorisering til aktiviteter inden for politisamarbejde og retligt samarbejde i straffesager, artikel 5, stk. 1, litra d, i det omfang den finder anvendelse på brugen af AI-systemer, der er omfattet af nævnte bestemmelse, artikel 5, stk. 1, litra h, og stk. 2-6, og artikel 26, stk. 10, ikke bindende for og finder ikke anvendelse i Danmark.

Det har en direkte og ofte overset konsekvens for straffebestemmelsen: [gennemførelseslovens § 10, stk. 1, nr. 1](#) strafbelægger kun art. 5, stk. 1, **litra a-g** – ikke litra h. Og Datatilsynets tilsynskompetence for litra d og g gælder efter forarbejderne udtrykkeligt kun »i det omfang disse ikke er omfattet af det danske retsforbehold«. Realtids fjernidentifikation til retshåndhævelse og den tilhørende ordning med forudgående judiciel tilladelse i art. 5, stk. 3, samt konsekvensanalysekravet i art. 5, stk. 2, sidste led, er dermed uden for den danske gennemførelse.

Digitaliseringsstyrelsen offentliggjorde i oktober 2025 en [vejledningspakke om forbudt brug af AI](#) som opfølgning på forordningen – den er indtil videre det primære danske fortolkningsbidrag til artikel 5, idet der endnu ikke foreligger offentliggjorte afgørelser efter [§ 7](#), som netop giver markedsovervågningsmyndighederne hjemmel til at offentliggøre deres afgørelser i sager om forbudt AI-praksis.

LOV

[AI-forordningen § 5, stk. 1](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1](#)

Klassificering af højrisiko-systemer efter artikel 6 – to spor og en betinget undtagelse

§ 3

Artikel 6 opererer med to selvstændige klassificeringsspor.

Produktspolet (stk. 1). Et AI-system er højrisiko, hvis det både (a) er tilsigtet anvendt som sikkerhedskomponent i – eller selv er – et produkt omfattet af EU-harmoniseringslovgivningen i bilag I, og (b) det pågældende produkt skal underkastes tredjeparts-overensstemmelsesvurdering efter samme lovgivning. Netop dette spor er det, der først finder anvendelse fra 2. august 2027.

Bilag III-spolet (stk. 2). De anvendelsesområder, bilag III opregner – herunder biometri, kritisk infrastruktur, uddannelse, beskæftigelse og personaleadministration, adgang til væsentlige offentlige og private ydelser, retshåndhævelse, migration og retspleje – er højrisiko i sig selv. Fagbevægelsens Hovedorganisation fremhævede i sit høringssvar til [L 111](#), at dette betyder, at »anvendelse af AI-systemer til personaleadministration og ledelse af medarbejdere betragtes som højrisiko-anvendelse«.

Undtagelsen i stk. 3 – og dens modundtagelse. Et bilag III-system er alligevel ikke højrisiko, hvis det ikke udgør en væsentlig risiko for sundhed, sikkerhed eller grundlæggende rettigheder, herunder ved ikke i væsentlig grad at påvirke resultatet af beslutningstagning. Det forudsætter, at systemet enten udfører en snæver proceduremæssig opgave, forbedrer resultatet af en tidligere afsluttet menneskelig aktivitet, påviser beslutningsmønstre uden at erstatte en menneskelig vurdering, eller udfører en forberedende opgave. Men undtagelsen har en hård grænse:

Uanset første afsnit betragtes et AI-system, der er omhandlet i bilag III, altid som højrisiko, hvis AI-systemet udfører profilering af fysiske personer.

Udbyderen skal dokumentere sin vurdering, inden systemet bringes i omsætning, og er uanset undtagelsen underlagt registreringsforpligtelsen i art. 49, stk. 2, jf. art. 6, stk. 4. Netop denne dokumentationsbyrde blev fremhævet som et praktisk problem i høringen over [L 111](#), hvor F&P pegede på de »de facto-krav, som ikke fremgår af forordningen« – hvad der kræves af en virksomhed for at *vis*, at den ikke falder under højrisiko.

Profileringsklausulen har konkret betydning for offentlige beslutningsstøtteværktøjer. Ligebehandlingsnævnet behandlede i [20-25601](#) Styrelsen for Arbejdsmarked og Rekrutterings profilafklaringsværktøj, der ved maskinlæring kobler et frivilligt spørgeskema med registerdata om alder, herkomst og ledighedshistorik for at forudsige risikoen for langtidsledighed. Nævnet frifandt styrelsen, fordi »herkomst« efter EU-Domstolens praksis i [C-668/15 Jyske Finans](#) ikke kan sidestilles med etnisk oprindelse. Afgørelsen angik alene forskelsbehandlingsloven – men værktøjet er et lærebogseksempel på et system, der efter AI-forordningen både ligger i bilag III (beskæftigelse) og udfører profilering af fysiske personer, og som derfor **altid** vil være højrisiko uanset stk. 3-undtagelsen.

Datatilsynets udtalelse i [2022-212-3676](#) om kommunernes AI-værktøj »Asta«, der skulle identificere nyledige dagpengemodtagere med forhøjet risiko for et langvarigt kontaktførelse, illustrerer den samme systemtype set fra databeskyttelsesretten.

LOV [AI-forordningen § 6, stk. 1-4](#)

PRAKSIS **Datatilsynet** · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta 18.05.2022
Ligebehandlingsnævnet · Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige 12.05.2022

Den danske tilsynsarkitektur – tre kompetente myndigheder og et fjerde spor for domstolene

§ 2 udmønter forordningens artikel 70, stk. 1, der kræver mindst én bemyndigende myndighed og mindst én markedsovervågningsmyndighed pr. medlemsstat. Danmark har valgt en delt model:

Myndighed	Rolle	Retligt grundlag
Digitaliseringsstyrelsen	Bemyndigende myndighed (art. 28, stk. 1), centralt kontaktpunkt (art. 70, stk. 2, 3. pkt.) og markedsovervågning af art. 5, stk. 1, litra a-c og e-f	§ 2, stk. 2
Datatilsynet	Markedsovervågning af art. 5, stk. 1, litra d og g – kun uden for retsforbeholdet	§ 2, stk. 3
Domstolsstyrelsen	Markedsovervågning af domstolenes AI-anvendelse, når domstolene <i>ikke</i> handler i deres egenskab af domstol	§ 2, stk. 4
Vedkommende ret selv	AI-anvendelse som led i domstolenes judicielle funktion; kære til højere ret, frist 4 uger	§ 2, stk. 5

Denne opdeling er ikke tilfældig. Forarbejderne til § 2 præciserer, at Domstolsstyrelsens »tilsyn alene omfatter domstolenes administrative forhold og ikke deres judicielle funktioner«, og at afgørelser om AI-anvendelse i den judicielle funktion træffes af retten selv med kære adgang – for særlige domstole uden almindelig ankeadgang til den landsret, i hvis kreds retten er beliggende. Domstolsstyrelsen har i august 2026 afholdt [en konference for retspræsidenter og dommere om etik og retssikkerhed ved AI i retterne](#).

Funktionel uafhængighed. Artikel 70, stk. 1, 2. pkt., kræver, at myndighederne udøver deres beføjelser »uafhængigt, upartisk og uden bias«. Forarbejderne omsætter det til et konkret instruktionsforbud:

De bemyndigende myndigheder og markedsovervågningsmyndigheder skal varetage deres opgaver og beføjelser uafhængigt af den pågældende ressortminister og skal være uafhængige af udefrakommende indblanding fra offentlige og private enheder. Dette indebærer også, at de bemyndigende myndigheder og markedsovervågningsmyndigheder ikke vil kunne modtage eller søge instrukser fra andre, herunder vedkommende ressortminister, uanset at de i øvrigt er organisatorisk underlagt det pågældende ressortministerium.

Uafhængigheden er dog ikke total isolation: forarbejderne åbner udtrykkeligt for, at en kompetent myndighed kan rådføre sig eller udveksle synspunkter med retshåndhævende myndigheder, krisestyringsmyndigheder eller andre markedsovervågnings- og datatilsynsmyndigheder og indhente teknisk bistand, når der er behov for særegen fagspecifik ekspertise.

Delingen af tilsynet blev kritiseret bredt under høringen over den kommende AI-lov, jf. [høringen af 16. september 2025](#). KL anbefalede at samle tilsynet hos Digitaliseringsstyrelsen for at sikre ensartet praksis, IT-Branchen advarede mod et fragmenteret tilsyn, F&P ønskede Finanstilsynet som sektormyndighed på forsikringsområdet, og Green Power Denmark ønskede Energistyrelsen. Institut for Menneskerettigheder fandt derimod, at sektoropdelingen giver mening, men understregede, at det i praksis bliver afgørende at sikre reel respekt for uafhængighedskravet – »især for de myndigheder, der ikke i forvejen er funktionelt uafhængige i

deres øvrige arbejde». Digitaliseringsstyrelsen fastholdt myndighedsstrukturen med henvisning til EU-retlige minimumskrav.

LOV

AI-forordningen § 70, stk. 1, 2

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2, stk. 1-5

§ 5 Markedsovervågningsbeføjelserne – oplysningskrav, kontrolbesøg uden retskendelse, påbud og midlertidigt forbud

Efter [artikel 74, stk. 1](#) finder markedsovervågningsforordningen (EU) 2019/1020 anvendelse på AI-systemer. Den er i dansk ret suppleret ved lov om produkter og markedsovervågning, men den lov gælder efter sin § 2 netop **ikke** produkter omfattet af AI-forordningen. Gennemførelseslovens §§ 4-9 udfylder derfor hullet. Digitaliseringsministeriet begrundede beføjelsernes omfang med, at markedsovervågningsmyndighedernes kompetence bør svare til det, de under alle omstændigheder skal besidde fra 2. august 2026 i medfør af henvisningen til markedsovervågningsforordningen.

Oplysningskrav (§ 5). Myndighederne kan af fysiske og juridiske personer omfattet af forordningens art. 2, stk. 1, litra a-f afkræve »alle oplysninger, som er nødvendige for myndighedernes tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under myndighedernes kompetence«. Forarbejderne til § 10 afgrænser bestemmelsen udtrykkeligt mod selvinkriminering: »Den foreslåede bestemmelse afgrænses af det almindelige forbud mod at udsætte andre for selvinkriminering, som det blandt andet kan udledes af Den Europæiske Menneskerettighedskonventions artikel 6 og § 10 i retssikkerhedsloven.«

Kontrolbesøg (§ 6). Myndighederne har »til enhver tid mod behørig legitimation og uden retskendelse adgang til alle erhvervsmæssige lokaliteter«, kan foretage tekniske undersøgelser af AI-systemet på stedet, kan lade sig bistå af uafhængige sagkyndige, og politiet yder om nødvendigt bistand. Digitaliseringsministeriet begrundede fraværet af retskendelseskrav både med effektivitetshensyn og med, at »muligheden for kontrolbesøg uden retskendelse vil have en afskrækkende effekt i forhold til udbredelsen af forbudte AI-systemer«. Netop dette punkt var det mest omstridte i høringen: DI, Dansk Erhverv og Danske Regioner kritiserede alle den vidtgående adgang uden retskendelse, men myndigheden fastholdt beføjelsen som nødvendig.

Påbud og midlertidigt forbud (§ 8). Myndighederne kan udstede påbud om overholdelse af art. 5, stk. 1, litra a-g, og kan udstede et midlertidigt forbud mod levering, markedsføring, udstilling eller anden tilgængeliggørelse af et AI-system, »hvis AI-systemet vurderes at kunne udgøre en risiko«. Forbuddets varighed kan ikke strække sig ud over, hvad der er nødvendigt for at træffe kontrolforanstaltninger til brug for undersøgelser eller vurderinger af systemets sikkerhed. Forarbejderne indsnævrer anvendelsesområdet betydeligt:

Bestemmelsen vil alene kunne anvendes i de tilfælde, hvor der er en formodning for, at et AI-system udgør en fare, og hvor det vurderes uforsvarligt ud fra et forsigtighedsprincip, at AI-systemet fortsat er i anvendelse, imens markedsovervågningsmyndigheden foretager de nødvendige undersøgelser af systemet med henblik på at træffe afgørelse.

Offentliggørelse (§ 7). Afgørelser i sager om forbudt AI-praksis kan offentliggøres for at oplyse offentligheden. Forarbejderne forbeholder dog fortrolige oplysninger om tekniske indretninger, fremgangsmåder og drifts- eller forretningsforhold af væsentlig økonomisk betydning, ligesom offentliggørelse er underlagt forordningens art. 78 om fortrolighed.

Bemyndigende myndighed (§ 9). Digitaliseringsstyrelsen kan efter forhandling med ministeren fastsætte regler om vurdering, udpegelse og notifikation af overensstemmelsesvurderingsorganer samt om suspension eller tilbagetrækning af udpegning efter art. 36, stk. 4, og kan delegere selve vurderingen til andre offentlige myndigheder eller private institutioner. Forarbejderne nævner som eksempel et krav om DANAK-akkreditering for organer, der ønsker notifikation.

LOV

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 5

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 6, stk. 1-4

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 8, stk. 1, 2

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 9, stk. 1, 2

Afskåret administrativ rekurs efter § 3 – retssikkerhedsprisen for uafhængighed

§ 6

§ 3 bestemmer kort og kategorisk, at de nationale kompetente myndigheders afgørelser efter forordningen, loven og regler udstedt i medfør heraf »ikke kan indbringes for anden administrativ myndighed«. Forarbejderne knytter bestemmelsen direkte til uafhængighedskravet:

Bestemmelsen udelukker, at de nationale kompetente myndigheders afgørelser er undergivet administrativ rekurs. Sådanne afgørelser kan indbringes direkte for domstolene efter grundlovens § 63. [...] Digitaliseringsministeriet vurderer, at det er nødvendigt for at sikre markedsovervågningsmyndighedernes uafhængighed, at en afgørelse truffet af markedsovervågningsmyndigheden ikke kan omgøres eller ændres af myndighedens sædvanlige overordnede.

Konstruktionen betyder, at der ikke findes noget klagenævn på AI-området, og at en operatør, der rammes af et påbud eller et midlertidigt forbud efter § 8, må gå direkte til domstolene. Det var et hovedkritikpunkt i høringen: DI efterlyste udtrykkeligt et uafhængigt klagenævn, F&P kritiserede den manglende administrative klageadgang sammen med bødemodellen, og Danske Regioner advarede om, at kombinationen af administrative bødeforlæg og manglende klageadgang »kan føre til forskelsbehandling mellem operatører og skabe præcedens uden domstolsprøvelse«. Digitaliseringsstyrelsen fastholdt strukturen og afviste et klagenævn.

Som praktisk retssikkerhedsmodvægt gælder alene forordningens art. 99, stk. 10, hvorefter udøvelsen af sanktionsbeføjelserne skal være underlagt »fornødne proceduremæssige sikkerhedsforanstaltninger i overensstemmelse med EU-retten og national ret, herunder effektive retsmidler og retfærdig procedure«, samt de almindelige forvaltningsretlige krav. Sidstnævnte er ikke ubetydelige: en tilsvarende afskæring af klageadgang findes på fødevareområdet, og Miljø- og Fødevareklagenævnet har i [23/11051](#) fastslået, at et administrativt bødeforlæg overhovedet ikke er en afgørelse i forvaltningsretlig forstand, men et tilbud om at afslutte en sag om en lovovertrædelse uden inddragelse af politi og domstole. Den sondring bliver relevant, hvis bemyndigelsen i § 11 til administrative bødeforelæg engang udmøntes.

LOV

AI-forordningen § 99, stk. 10

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 11

Sanktionssporet – strafferetlig bøde efter § 10, forordningens § 7 bødelofter og den 5-årige forældelse

Forordningens [artikel 99, stk. 9](#) overlader det til medlemsstaterne, om administrative bøder pålægges af domstole eller af andre organer. Danmark har valgt domstolssporet. Digitaliseringsministeriet konkluderede i de almindelige bemærkninger, at »sanktioner for overtrædelser af forordningens bestemmelser efter dansk ret fastsættes som en strafferetlig sanktion i henhold til artikel 99, stk. 9, 1. pkt., jf. artikel 99, stk. 3 og 5«. Formelt er der altså tale om **straf**, ikke om en administrativ bøde.

[§ 10, stk. 1](#) strafbelægger fem forhold: overtrædelse af art. 5, stk. 1, litra a-g (nr. 1); afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger efter art. 99, stk. 5 (nr. 2); undladelse af at efterkomme oplysningskrav efter § 5 eller hindring af adgang efter § 6, stk. 1 (nr. 3); hindring af tekniske undersøgelser efter § 6, stk. 2 (nr. 4); og undladelse af at efterkomme påbud eller midlertidige forbud efter § 8 (nr. 5). Forarbejderne giver konkrete eksempler på nr. 3 og 4: nægtelse af at udlevere adgangskoder, kryptering af alle oplysninger så myndigheden skal omgå krypteringen, og fysisk blokering af adgangen til lokaliteter.

Bødelofterne. Selv om bøden er strafferetlig, skal udmålingen holde sig inden for forordningens rammer:

Overtrædelsestype	Loft (fast beløb)	Loft (omsætning)	Hjemmel
Forbudt AI-praksis, art. 5	35 mio. EUR	7 % af global årsomsætning	art. 99, stk. 3
Operatør- og gennemsigtighedspligter (art. 16, 22, 23, 24, 26, 31, 33, 34, 50)	15 mio. EUR	3 %	art. 99, stk. 4
Ukorrekte/vildledende oplysninger	7,5 mio. EUR	1 %	art. 99, stk. 5

Det højeste af de to beløb gælder – men for SMV'er og iværksættervirksomheder gælder efter art. 99, stk. 6, omvendt det **laveste**. Forarbejderne til § 10 gengiver dette udtrykkeligt og fastslår, at »ved udmåling af bødestraf skal de fastsatte beløbsgrænser i henhold til artikel 99, stk. 3 og 5, i forordningen om kunstig intelligens overholdes«.

Udmålingskriterierne. Forarbejderne henviser til [artikel 99, stk. 7](#), der opregner ti hensyn: overtrædelsens art, grovhed og varighed samt konsekvenser; om andre markedsovervågningsmyndigheder allerede har bødet den samme operatør for samme overtrædelse; om andre myndigheder har bødet for overtrædelser af anden EU-ret eller national ret som følge af samme aktivitet; operatørens størrelse, omsætning og markedsandel; skærpende eller formildende faktorer såsom opnåede økonomiske fordele eller undgåede tab; graden af samarbejde; graden af ansvar under hensyn til de gennemførte tekniske og organisatoriske foranstaltninger; hvordan myndigheden fik kendskab til overtrædelsen, herunder om operatøren selv underrettede; om overtrædelsen var forsætlig eller uagtsom; og tiltag for at afbøde skaden. Straffelovens § 51, stk. 3, og kapitel 10 om straffens fastsættelse finder i øvrigt anvendelse.

Juridiske personer og offentlige myndigheder. § 10, stk. 3 hjemler strafansvar for juridiske personer efter straffelovens 5. kapitel. Forarbejderne trækker en vigtig grænse for offentlige myndigheder med henvisning til straffelovens § 27, stk. 2:

Statslige myndigheder og kommuner kan ifølge straffelovens § 27, stk. 2, alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private. [...] Reglerne i straffelovens kapitel 5 omfatter derimod ikke lovovertrædelser, der begås som led i myndighedsudøvelse. I sådanne tilfælde kan der alene blive tale om personligt strafansvar for de ansvarlige enkeltpersoner.

Forældelse. § 10, stk. 4 fastsætter en forældelsesfrist på 5 år. Det er en bevidst fravigelse: efter straffelovens § 93, stk. 11 ville fristen have været 2 år, når der ikke er hjemlet højere straf end fængsel i 1 år. Fravigelsen begrundes i, »at de omfattede straffesager kan antage en vis størrelse og kompleksitet«.

Subsidiaritetsklausulen. Bøden idømmes kun, »medmindre højere straf er forskyldt efter anden lovgivning«. Forarbejderne nævner det konkrete sammenstød med straffelovens §§ 162 og 163 om urigtige oplysninger til offentlige myndigheder: forholdet henføres da under den bestemmelse, der giver højest straf.

Den foreslåede bødemodel i det bortfaldne L 111. Det bortfaldne L 111 indeholdt en egentlig bødemodel med tre statiske grundbeløb – 700.000 EUR ved forbudt AI-praksis, 150.000 EUR ved overtrædelse af krav til højrisiko-systemer, gennemsigtighed og bemyndigede organer, og 37.500 EUR ved processuelle overtrædelser – samt tre dynamiske grundbeløb på henholdsvis 0,14 %, 0,03 % og 0,005 % af den globale årlige omsætning, som anvendes hvis de er højere. DI påpegede i høringssvaret, at fastsættelsen af bødeniveauet er overladt til medlemsstaterne, hvilket »kan give anledning til fragmentering i sanktionspraksis på tværs af EU«, og anbefalede koordinering med EU-praksis. Modellen er ikke gældende ret, da lovforslaget bortfaldt, men den er den hidtil klareste indikation af, hvilket niveau danske myndigheder forventer at lægge sig på.

LOV

AI-forordningen § 99, stk. 3-9

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1-4

Straffeloven § 27, stk. 2

Straffeloven § 93, stk. 11

§ 8 Datatilsynets AI-praksis – den afgørende sontring mellem udvikling og drift

Den vigtigste danske afgørelse om AI-løsninger i den offentlige sektor er Datatilsynets udtalelse i 2023-212-0015 af 17. november 2023 om et kommunalt beslutningsstøtteværktøj, der ved algoritmisk forudsigelse skulle identificere borgere med behov for vedligeholdende træning og rehabilitering. Tilsynet delte behandlingen i to faser og nåede modsatte resultater:

Fase	Supplerende retsgrundlag	Konklusion
Udvikling og gentræning	Serviceoven § 86 og § 112	Tilstrækkeligt
Drift (beslutningsstøtte i konkrete sager)	Samme bestemmelser	Ikke tilstrækkeligt klart

Begrundelsen er den centrale:

Kravene til klarheden af det retsgrundlag, som skal danne baggrund for jeres behandling af personoplysninger ved drift af en AI-løsning, afhænger af, hvor indgribende behandlingen er for borgerne. [...] Konsekvenserne for borgerne

er dermed ofte større, når AI-løsningen er i drift, og der stilles derfor højere krav til klarheden af det retsgrundlag, der danner baggrund for at anvende løsningen i drift.

Tilsynet opregnede de faktorer, der gjorde driften indgribende: løsningen producerer forudsigelser om enkeltpersoner, som myndigheden handler ud fra; der er risiko for, at medarbejdere tillægger AI'ens vurdering større vægt end deres egen faglige vurdering (**automatiseringsbias**); der behandles store mængder følsomme data; målgruppen er sårbare borgere; og AI kan finde sammenhænge ud over, hvad en menneskelig sagsbehandler kan, hvilket gør behandlingen grundlæggende forskellig fra traditionel sagsbehandling. Konklusionen var, at servicelovens opgavepålæg hverken regulerer rækkevidden af behandlingen eller muligheden for at anvende AI på den pågældende måde.

Denne dobbelthed går igen i [2024-212-0371](#) om Uddannelses- og Forskningsstyrelsens AI-løsning til screening af SU-handicaptillægsansøgninger, hvor løsningen skulle trænes på ca. 3.000 historiske sager og alene fungere som støtte uden at træffe endelige afgørelser, og i [2022-212-3676](#) om AI-værktøjet Asta, hvor tilsynet stillede krav til lovgivningsmæssig præcision ved profilering og behandling af følsomme data.

Konsekvensanalysen som fælles omdrejningspunkt. [AI-forordningens artikel 27](#) pålægger idriftsættere, der er offentligtretlige organer eller private enheder, som leverer offentlige tjenester, at foretage en konsekvensanalyse vedrørende grundlæggende rettigheder inden idriftsættelse af bilag III-højrisikosystemer. Analysen skal beskrive processerne, anvendelsesperioden, de berørte persongrupper, de specifikke risici for skade, gennemførelsen af menneskeligt tilsyn samt de foranstaltninger, herunder intern ledelse og klagemekanismer, der skal træffes, hvis risiciene opstår. Resultatet skal meddeles markedsovervågningsmyndigheden. Efter art. 27, stk. 4, **supplerer** analysen den databeskyttelsesretlige konsekvensanalyse efter GDPR art. 35 – den erstatter den ikke.

Datatilsynets praksis om GDPR-konsekvensanalyser er derfor direkte relevant. I [2023-423-0005](#) udtalte tilsynet alvorlig kritik af Københavns Kommunes konsekvensanalyse for AULA, og i [2023-423-0009](#) fik Hillerød Kommune både alvorlig kritik og påbud for manglende risikovurderinger og konsekvensanalyse. Mønsteret – at analyser udarbejdes for sent, for overfladisk eller slet ikke – er et af de mest sandsynlige første håndhævelsespunkter under artikel 27.

LOV	AI-forordningen § 27, stk. 1-5	Serviceloven § 86	Serviceloven § 112
PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger 12.06.2024 Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024 Datatilsynet · Alvorlig kritik og påbud til Hillerød Kommune for utilstrækkelig behandlingssikkerhed og manglende risikovurderinger 22.12.2023 Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor 17.11.2023 Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta 18.05.2022		

Biometri, følelsesgenkendelse og ansigtsgenkendelse – hvor grænserne allerede er blevet trukket

§ 9

Tre af artikel 5's forbud – litra e (ikkemåltrettet skrabning til ansigtsgenkendelsesdatabaser), litra f (følelsesgenkendelse på arbejdsplads og uddannelsesinstitution) og litra g (biometrisk kategorisering) – ligger tæt op ad områder, hvor Datatilsynet allerede har afsagt afgørelser under GDPR.

Følelses- og stemmeanalyse. I [2023-431-0018](#) af 27. juni 2024 undersøgte Datatilsynet af egen drift IDA Forsikrings AI-baserede transskribering og analyse af optagne telefonsamtaler, hvor systemet uddrager temaer, kvalitetsscoringer efter en samtalestandard og »root cause«-analyser. Tilsynet fandt for det første, at AI-analysen ikke er et selvstændigt behandlingsformål:

Det er i den forbindelse Datatilsynets opfattelse, at analysen af de optagne telefonsamtaler til brug for kvalitetssikring ikke skal anses for et selvstændigt formål. IDA Forsikring kan således basere analysen på samme grundlag som selve optagelsen af samtalen.

For det andet – og mere principielt for AI-forordningen – fandt tilsynet, at analysen ikke er omfattet af forbuddet mod behandling af særlige kategorier i GDPR art. 9, stk. 1: selv om stemme kan udgøre biometriske data efter art. 4, nr. 14, er formålet ikke entydigt at identificere hverken den, der ringer, eller medarbejderne, og systemet benytter ikke stemmegenkendende teknologi. Det er en mindre indgribende behandlingsform. Systemet analyserer kun ren tekst og tager ikke højde for tonefald, køn eller dialekter – hvilket tilsynet noterede primært kan føre til »falske positive« i kvalitetsscoringerne. Sagen faldt dog på samtykkets granularitet: der blev kun indhentet ét samlet samtykke til både dokumentations- og kvalitetssikringsformål, hvilket ikke var frivilligt og dermed ugyldigt.

Afgrænsningen har direkte betydning for art. 5, stk. 1, litra f og g: et system, der udleder *følelser* hos medarbejdere, ville falde under litra f, mens et system, der alene scorer sprogbrug i transskriberet tekst, ligger uden for. FH pegede i høringen over [L 111](#) netop på digital »stemmegenkendelse«, der indebærer en vurdering af en medarbejders humør og følelser, som eksempel på forbudt praksis på arbejdspladsen.

Ansigtsgenkendelse. I [2024-51-0012](#) af 18. december 2024 gav Datarådet F.C. København tilladelse efter [databeskyttelseslovens § 7, stk. 4](#) til automatisk ansigtsgenkendelse ved indgangene til Parken – men kun i forbindelse med fodboldkampe og under strenge vilkår, mens ansøgningen for koncerter og øvrige arrangementer blev afvist. Systemet sammenligner kameraoptagelser med fotos fra klubbens og politiets karantænelister. Afgørelsen viser en klar formålsbunden proportionalitetsprøvelse: den samme teknologi kan være lovlig til ét formål og ulovlig til et andet.

Skrabning af biometriske data. I [2023-211-0004](#) af 30. januar 2024 vurderede Datatilsynet etableringen og delingen af taledatasættet CoRal til udvikling af dansk taleteknologi. Tilsynet fastslog, at stemmeoptagelser er personoplysninger, men at art. 9-forbuddet ikke fandt anvendelse, fordi formålet ikke var entydig identifikation. Sagen illustrerer, at afgrænsningen af litra e i AI-forordningen – der forbyder oprettelse eller udvidelse af ansigtsgenkendelsesdatabaser gennem **ikkemåltrettet** indsamling – beror på både indsamlingsmetoden og formålet.

EU-Domstolens biometri-linje. Domstolen har i en række sager fastlagt strenge krav til myndigheders behandling af biometriske og genetiske data, som vil udgøre den ydre ramme for enhver dansk anvendelse af biometrisk AI:

- I [C-118/22](#) fastslog Store Afdeling, at ubegrænset opbevaring af politiregistrerede biometriske og genetiske data indtil den registreredes død uden periodisk nødvendighedsvurdering eller sletningsret er i strid med direktiv 2016/680 og chartret.

- I [C-80/23](#) fastslog Domstolen, at det er den kompetente myndighed selv – ikke domstolen – der skal efterprøve og godtgøre, at indsamlingen er »strengt nødvendig« efter art. 10 i direktiv 2016/680; en systematisk indsamling for alle sigtede uden konkret nødvendighedsvurdering er uforenelig med direktivet.
- Linjen er videreført i [C-57/23](#).
- I [C-548/21](#) fastslog Store Afdeling, at politiets adgang til data på en beslaglagt mobiltelefon kræver forudgående kontrol ved en domstol eller et uafhængigt forvaltningsorgan samt underretning af den registrerede.
- Og i [C-61/22](#) kendte Domstolen forordningen om biometriske identitetskort ugyldig på grund af forkert retsgrundlag, men opretholdt dens virkninger midlertidigt.

Disse afgørelser angår direktiv 2016/680 og ikke AI-forordningen, men de definerer det nødvendigheds- og proportionalitetsniveau, som biometriske AI-systemer under alle omstændigheder skal opfylde – også de områder, hvor det danske retsforbehold friholder Danmark fra selve forordningens forbud.

LOV	AI-forordningen § 5, stk. 1	Databeskyttelsesloven § 7, stk. 4	
PRAKSIS	EU-Domstolen · Beskyttelse af personoplysninger: Politiets indsamling og opbevaring af biometriske og genetiske data fra mistænkte		20.11.2025
	EU-Domstolen · Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar		28.11.2024
	EU-Domstolen · Politimyndigheders adgang til mobiltelefoner: Krav om retslig kontrol og proportionalitet ved databehandling i straffesager		04.10.2024
	EU-Domstolen · Ugyldighed af forordning om biometriske identitetskort pga. forkert retsgrundlag (C-61/22)		21.03.2024
	EU-Domstolen · Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten		30.01.2024
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken		18.12.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne		27.06.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse		30.01.2024

§ 10 Gennemsigtighed og forklaringspligt – EU-Domstolens praksis om automatiserede afgørelser

[AI-forordningens artikel 50](#) pålægger gennemsigtighedsforpligtelser i fire lag: brugere skal oplyses om, at de interagerer med et AI-system (stk. 1); syntetisk genereret lyd-, billed-, video- eller tekstindhold skal mærkes maskinlæsbart (stk. 2); idriftsættere af følelsesgenkendelses- og biometriske kategoriseringssystemer skal underrette de berørte (stk. 3); og deepfakes samt AI-genereret tekst om spørgsmål af offentlig interesse skal mærkes (stk. 4). Oplysningerne skal gives klart og synligt senest ved første interaktion eller eksponering, jf. stk. 5. Overtrædelse af artikel 50 er efter art. 99, stk. 4, litra g, sanktioneret med op til 15 mio. EUR/3 %.

Den materielt beslægtede forklaringspligt ved automatiserede afgørelser er allerede udviklet af EU-Domstolen under GDPR. I [C-634/21](#) (SCHUFA) fastslog Domstolen, at et kreditoplysningsbureaus automatiske beregning af en kreditscore i sig selv udgør en automatisk individuel afgørelse efter GDPR art. 22, stk. 1, når scoren er afgørende for, om en tredjepart indgår aftaleforholdet – en snæver fortolkning ville skabe et hul i beskyttelsen, fordi den registrerede da ville miste indsichtsretten i logikken efter art. 15, stk. 1, litra h.

I [C-203/22](#) (Dun & Bradstreet) af 27. februar 2025 præciserede Domstolen indholdet af forklaringspligten. Den registrerede har ikke krav på formlen eller en trin-for-trin-beskrivelse, men på en egentlig forklaring:

De »meningsfulde oplysninger om logikken« ... skal således beskrive den procedure og de principper, der konkret er anvendt, på en sådan måde, at den registrerede kan forstå, hvilke af vedkommendes personoplysninger der blev anvendt på hvilken måde, da den pågældende automatiske afgørelse blev truffet, idet kompleksiteten af de operationer, der skal udføres i forbindelse med en automatisk afgørelse, ikke kan fritage den dataansvarlige for forklaringspligten.

Domstolen tilføjede, at det for en profilering som den omtvistede kan være tilstrækkeligt at oplyse, i hvilket omfang en ændring i de indgåede data ville have givet et andet resultat – en modkontrafaktisk forklaringsmodel, der er direkte anvendelig på AI-systemer.

Om forholdet til forretningshemmeligheder fastslog Domstolen, at den dataansvarlige ikke selv må afgøre spørgsmålet:

I dette tilfælde skal de nævnte oplysninger også videregives til den kompetente tilsynsmyndighed eller den kompetente ret, som skal afveje de omhandlede rettigheder og interesser med henblik på at fastlægge omfanget af den registreredes ret til indsigt i personoplysninger vedrørende den pågældende.

En national regel, der generelt afskærer indsichtsretten, når videregivelse truer en forretningshemmelighed, er derfor uforenelig med forordningen. Det er en vigtig parallel til AI-forordningens art. 78 om fortrolighed og til [§ 7](#) om offentliggørelse af afgørelser, hvor forarbejderne netop forbeholder oplysninger om tekniske indretninger og forretningsforhold: forbeholdet må efter [C-203/22](#) antages at forudsætte en konkret afvejning, ikke en generel afskæring.

Datatilsynets ældre praksis peger i samme retning. I [2019-41-0031](#) behandlede tilsynet netop spørgsmålet om automatisk prisberegning og GDPR art. 22 i forbindelse med indsichtsretten.

Et beslægtet aktindsigtsspørgsmål er behandlet af Folketingets Ombudsmand i [FOB 2022-23](#), hvor en journalist havde bedt om aktindsigt i modeldokumentationen for Udbetaling Danmarks Machine Learning-modeller, der bruges til at prioritere sager til manuel kontrol af barselsdagpenge, børnetilskud og pension. Ombudsmanden kunne ikke tilsidesætte myndighedens vurdering af, at det af væsentlige hensyn til gennemførelsen af offentlig kontrol var nødvendigt at undtage oplysninger fra modeldokumentationen efter offentlighedslovens § 33, nr. 2. Modellerne blev ikke i sig selv brugt til at vurdere ydelsesretten – en sontring der svarer nøje til AI-forordningens skel mellem beslutningsstøtte og automatiseret afgørelse.

LOV

[AI-forordningen § 50, stk. 1-5](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7](#)

PRAKSIS

EU-Domstolen · Indsichtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder

27.02.2025

EU-Domstolen · Automatisk kreditscoring som en individuel afgørelse efter GDPR

07.12.2023

Menneskeligt tilsyn efter artikel 14 og de forvaltningsretlige krav – § 11 ombudsmandens praksis

[Artikel 14](#) kræver, at højrisiko-AI-systemer udformes, så fysiske personer effektivt kan overvåge dem i brugsperioden. Tilsynsforanstaltningerne skal stå i rimeligt forhold til risiciene, graden af autonomi og anvendelseskonteksten, og systemet skal leveres, så tilsynspersonen kan:

- forstå systemets kapacitet og begrænsninger og overvåge driften, herunder opdage uregelmæssigheder, funktionsforstyrrelser og uventet ydeevne
- være opmærksom på tendensen til at forlade sig på outputtet i overdreven grad – **automatiseringsbias** – navnlig ved systemer, der giver oplysninger eller anbefalinger til afgørelser truffet af mennesker
- fortolke outputtet korrekt
- beslutte ikke at anvende systemet eller se bort fra, tilsidesætte eller omgøre outputtet
- gribe ind eller afbryde systemet i en sikker tilstand ved en »stopknap«

For biometriske identifikationssystemer efter bilag III, punkt 1, litra a, gælder et skærpet krav i stk. 5: idriftsætteren må ikke handle på en identifikation, medmindre den er verificeret og bekræftet særskilt af mindst to fysiske personer med den nødvendige kompetence, uddannelse og myndighed – dog med undtagelse for retshåndhævelse, migrationsstyring, grænsekontrol og asylforvaltning, hvor kravet skønnes uforholdsmæssigt.

[Artikel 26](#) supplerer med idriftsætterforpligtelser: tilsynet skal overdrages til personer med den nødvendige kompetence og myndighed (stk. 2); inputdata skal være relevante og repræsentative i det omfang idriftsætteren kontrollerer dem (stk. 4); driften skal overvåges, og anvendelsen stilles i bero ved risiko (stk. 5); logfiler skal opbevares i mindst seks måneder (stk. 6); arbejdstagerrepræsentanter og berørte arbejdstagere skal informeres, inden systemet tages i brug på arbejdspladsen (stk. 7); og fysiske personer, der er genstand for et bilag III-system, som træffer eller bistår med at træffe beslutninger om dem, skal underrettes (stk. 11). Hertil kommer den generelle pligt i [artikel 4](#) til at sikre et tilstrækkeligt niveau af AI-færdigheder hos personalet.

Ombudsmandens parallelle krav. Folketingets Ombudsmand har uafhængigt af AI-forordningen udviklet en fast praksis om forvaltningsretlige krav til automatiserede systemer, som i vidt omfang dækker det samme terræn. I [FOB 2026-6](#) om Skatteforvaltningens automatiserede SMV-løsning sammenfattede ombudsmanden de generelle krav:

Det er et grundlæggende krav, at offentlige it-systemer kan understøtte en korrekt anvendelse af den relevante lovgivning – herunder forvaltningsretlige regler og principper. Dette kan bedst sikres ved en tidlig identifikation og systemindarbejdelse af de pågældende regelsæt.

Ombudsmanden fremhævede tillige den strukturelle risiko ved automatisering:

Automatiserede afgørelsessystemer forudsætter dermed også, at myndighederne på forhånd kan afgrænse, hvilket faktum der måtte være relevant i fremtidige sager, idet den faktiske del af beslutningsgrundlaget ikke længere bliver genstand for myndighedens konkrete vurdering. Automatiserede systemer indebærer derfor en risiko for, at myndighederne ikke fanger tilfælde med atypiske fakta eller tilfælde, hvor retsgrundlaget forpligter til at tage hensyn til forhold, der enten normalt ikke opstår eller normalt ikke er relevante.

Den juridiske ekspertise skal være til rådighed i alle væsentlige faser, systemet skal testes i den sammenhæng, hvor det skal anvendes, og myndigheden skal efter implementeringen følge op på, om systemet som forudsat understøtter en korrekt retsanvendelse. Ombudsmanden henviser i den forbindelse til [FOB 2025-13](#) om Vurderingsstyrelsens automatiske robotløsning, der førte til fejl, og til den ældre grundslag [FOB 2014-24](#) om SKATs EFI-system.

Den samme linje findes i [vejledningen om digitaliseringsklar lovgivning](#), der fastslår, at »brug af automatisk sagsbehandling ændrer ikke ved, at de forvaltningsretlige regler om f.eks. begrundelse, vejledning, partshøring, mv. skal overholdes«, og at en automatisk genereret begrundelse skal leve op til de almindelige krav i [forvaltningslovens § 24](#). En forudsætning for hel eller delvis automatisering er, at afgørelsen kan træffes efter rent objektive kriterier uden udøvelse af et individuelt skøn.

AI-forordningens artikel 14 og forvaltningsrettens krav peger dermed samme vej: menneskeligt tilsyn skal være reelt og ikke blot formelt, og systemet skal designes, så tilsynspersonen faktisk kan gennemskue og omgøre outputtet. Om afgrænsningen mellem beslutningsstøtte og bunden regel anvendelse kan der krydshenvises til [skoen-under-regel-pligtmaessigt-skoen](#).

LOV

[AI-forordningen § 4](#)[AI-forordningen § 14, stk. 1-5](#)[AI-forordningen § 26, stk. 1-12](#)[Forvaltningsloven § 24](#)

Sektorbekendtgørelser – hvordan Danmark har lukket § 12 hjemmelshullet efter Datatilsynets praksis

Datatilsynets konklusion i [2023-212-0015](#) om, at generelle opgavehjemler ikke er tilstrækkeligt klare til at bære **driften** af en beslutningsstøttende AI-løsning, har haft direkte lovgivningsmæssig virkning. Der er siden 2025 udstedt en række sektorspecifikke bekendtgørelser, der etablerer det supplerende nationale retsgrundlag:

Bekendtgørelse	Område	Ikrafttræden
Bekendtgørelse om Arbejdstilsynets anvendelse af kunstig intelligens	Tilsyns- og vejledningsopgaver efter arbejdsmiljølovens § 72	1. juli 2025
Bekendtgørelse om Uddannelses- og Forskningsstyrelsens anvendelse af kunstig intelligens ...	Sagsbehandling efter SU-loven	2025
Bekendtgørelse om STAR's behandling af personoplysninger med kunstig intelligens ...	Styrelsens opgavevaretagelse, herunder jobmatch på Jobnet	1. februar 2026
Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens ... i beskæftigelsesindsatsen	Kommunal beskæftigelsesindsats	1. februar 2026

De to sidste hviler på bemyndigelserne i § 52 a i lov om organisering og understøttelse af beskæftigelsesindsatsen, indsat ved lov nr. 1750 af 29. december 2025, jf. [startvejledningen](#). Formålet er ifølge vejledningen udtrykkeligt »at skabe et tilstrækkeligt klart nationalt retsgrundlag for STAR og kommunernes behandling af personoplysninger i kunstig intelligens-løsninger« – altså præcis den klarhed, Datatilsynet havde efterlyst.

Bekendtgørelserne indeholder tre gennemgående retlige greb, der ligger tæt op ad AI-forordningens systematik:

- **Forbud mod fuldautomatiske afgørelser.** Kommunerne kan efter bekendtgørelsens § 1, stk. 6, ikke træffe afgørelser, der alene er baseret på automatisk behandling, herunder profilering. [Vejledningen](#) præciserer, at bestemmelsen gengiver GDPR art. 22, stk. 1, og at AI-behandlingen »alene [skal være] sagsunderstøttende«.
- **Særsomt oplysningspligt om AI-anvendelse.** Efter § 2, stk. 4, skal kommunerne sikre, at det tydeligt fremgår for den registrerede, når kunstig intelligens anvendes. Vejledningen fastslår, at denne pligt »går således videre end den almindelige oplysningspligt efter databeskyttelsesforordningen, da den indeholder et eksplicit krav om at oplyse om anvendelsen af kunstig intelligens, hvilket ikke altid vil være et krav efter oplysningspligten i artikel 13 og artikel 14«. Det er reelt en national foregribelse af AI-forordningens art. 26, stk. 11, og art. 50.
- **Offentliggørelseskrav.** Både SU- og STAR-bekendtgørelserne pålægger styrelserne at offentliggøre, i hvilke tilfælde de anvender kunstig intelligens til at understøtte sagsbehandlingen.

Begrebsmæssigt henviser vejledningen til beskæftigelsesbekendtgørelsen direkte til forordningen: »For så vidt angår definitionen af kunstig intelligens, herunder hvordan bestemte typer af kunstig intelligens må og ikke må benyttes, henvises til AI-forordningen.« Begrebet »lignende digitale løsninger« er indsat for at fange teknologier, der minder om AI uden at opfylde forordningens definition.

Digitaliseringsstyrelsen sendte i februar 2026 [et lovforslag om generel hjemmel til udvikling og anvendelse af AI-systemer i den offentlige forvaltning](#) i høring – en tværgående afløsning for den nuværende sektorvise tilgang. Udkastet definerer »beslutningsstøtte« som situationer, hvor et AI-system anvendes som et fagligt understøttende redskab for en sagsbehandler, uden at systemet selv træffer afgørelser, og anerkender åbent, at grænsedragningen »ikke [er] fastlagt klart i retspraksis«, og at »fremtidig retspraksis vil bidrage til at præcisere, hvilken grad af menneskelig involvering« der kræves.

LOV

[AI-forordningen § 26, stk. 11](#)[AI-forordningen § 50, stk. 1](#)

PRAKSIS

Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor 17.11.2023

§ 13 Dansk domspraksis om kunstig intelligens er endnu strafferetlig, ikke forordningsretlig

Der findes endnu ingen offentliggjorte danske domme om AI-forordningen eller gennemførelseslovens § 10. Den domspraksis, der faktisk foreligger om kunstig intelligens, er strafferetlig og hviler udelukkende på straffeloven – men den er værd at kende, fordi den viser, hvordan danske domstole hidtil har håndteret AI-genereret materiale.

I [SS-3195/2024-RAN](#) af 8. januar 2025 behandlede Retten i Randers fremstilling, besiddelse og udbredelse af 36.209 AI-genererede, fotorealistiske børnepornografiske billeder. Tiltalte hævdede, at materialet var lovligt, og at formålet var at afholde pædofile fra at søge ægte overgrebsmateriale. Retten fandt billederne omfattet af [straffelovens § 235](#) og idømte fængsel i 1 år og 3 måneder, heraf 3 måneder ubetinget, idet der blev lagt væsentlig vægt på, at det ikke kunne bevises, at de anvendte AI-modeller var trænet på ægte børnepornografi.

Vestre Landsret stadfæstede skyldkendelsen, men skærpede straffen til ubetinget fængsel i 1 år og 6 måneder under dissens 5-1, jf. [S-0141-25](#) af 12. juni 2025. Procesbevillingsnævnet behandlede sagen under j.nr.

25/17215 og tog stilling til, om den principielle problemstilling om strafudmåling for rent fiktivt, AI-genereret materiale kunne indbringes for Højesteret, jf. [U 2025.3571 V](#).

Sagskomplekset illustrerer et generelt mønster: dansk ret har hidtil håndteret AI ved at anvende eksisterende gerningsindhold på nye teknologiske frembringelser, ikke ved at regulere teknologien som sådan. AI-forordningen vender denne logik om ved at regulere systemet, dets udbyder og dets idriftsætter forud for skaden. De to spor kan mødes: en deepfake, der ikke er mærket efter [artikel 50, stk. 4](#), kan efter omstændighederne både udløse bøde efter forordningsspor og straf efter straffelovens bestemmelser om freds- og ærekrænkelser – hvorved subsidiaritetsklausulen i [§ 10, stk. 1](#) (»medmindre højere straf er forskyldt efter anden lovgivning«) bliver aktuel.

LOV

AI-forordningen § 50, stk. 4

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1

Straffeloven § 235, stk. 1, 2

PRAKSIS	Landsretten · Ubetinget fængsel for fremstilling, besiddelse og udbredelse af over 36.000 AI-genererede billeder af børnepornografisk karakter	12.06.2025
	Byretten · Dom for fremstilling og udbredelse af AI-genereret børnepornografi	08.01.2025
	Procesbevillingsnævnet · 3.-instansbevilling: Strafudmåling for besiddelse og udbredelse af ca. 36.000 AI-genererede børnepornografiske billeder (U 2025.3571 V)	21.11.2025

§ 14 Sammenfatning – hvad der er afklaret, og hvad der endnu udestår

Afklaret retstilstand. Danmark har med [lov nr. 467 af 14. maj 2025](#), vedtaget enstemmigt med 109 stemmer ved [L 154](#), etableret den institutionelle og strafferetlige ramme for forordningens første fase. Tilsynet er delt mellem Digitaliseringsstyrelsen, Datatilsynet og Domstolsstyrelsen med en fjerde ordning for domstolenes judicielle AI-brug. Markedsovervågningsbeføjelserne er vidtgående – oplysningskrav, kontrolbesøg uden retskendelse, tekniske undersøgelser på stedet, sagkyndig bistand, politibistand, påbud, midlertidigt forbud og offentliggørelse. Overtrædelser straffes med bøde, juridiske personer kan ifalde ansvar efter straffelovens kapitel 5, og forældelsesfristen er 5 år. Der er ingen administrativ rekurs.

Uafklaret. Fire ting står åbne:

- Bødeniveauet.** Der findes ingen dansk retspraksis om bødeudmåling efter § 10. Den foreslåede bødemodel i det bortfaldne [L 111](#) – statiske grundbeløb på 700.000/150.000/37.500 EUR og dynamiske på 0,14/0,03/0,005 % af global omsætning – er den eneste konkrete indikation, men den er ikke gældende ret.
- Anden fase af gennemførelsen.** Forordningen fandt anvendelse i sit fulde omfang fra 2. august 2026, men det lovforslag, der skulle etablere den fulde nationale tilsyns- og sanktionsramme for højrisiko-systemer, gennemsigtighed og GPAI, bortfaldt. Indtil ny lovgivning vedtages, dækker den gældende lov alene tilsyn med forbudt AI-praksis efter art. 5, stk. 1, litra a-g.
- Grænsen mellem beslutningsstøtte og automatiseret afgørelse.** Digitaliseringsstyrelsen erkender selv i [høringsudkastet af februar 2026](#), at kravet til den menneskelige involverings omfang ikke er fastlagt i retspraksis.
- Samspillet med GDPR.** Datatilsynet er både markedsovervågningsmyndighed for art. 5, stk. 1, litra d og g, og databeskyttelsestilsyn. En og samme AI-anvendelse kan derfor rammes ad to spor, og art. 99, stk. 7,

litra b og c, pålægger netop at tage hensyn til, om andre myndigheder allerede har sanktioneret den samme operatør for samme aktivitet – et ne bis in idem-hensyn, der endnu ikke er prøvet i dansk praksis.

Hvad praksis indtil videre siger. Den retningsgivende praksis findes uden for forordningen selv, men på dens materielle kerneområder: Datatilsynets sondring mellem udvikling og drift i [2023-212-0015](#), afgrænsningen af biometri i [2023-431-0018](#) og [2024-51-0012](#), EU-Domstolens forklaringspligt i [C-203/22](#) og [C-634/21](#), nødvendighedskravet ved biometriske politidata i [C-118/22](#) og [C-80/23](#), Ombudsmandens krav til automatiserede systemer i [FOB 2026-6](#), og Ligebehandlingsnævnets prøvelse af algoritmisk profilering i [20-25601](#). Beslægtede spørgsmål om Datatilsynets bødeindstillinger behandles under [datatilsynsboder-gdpr-overtraedelser](#), AI-systemers persondatabehandling under [ai-systemer-gdpr](#), og AI i ansættelsesforhold under [databeskyttelse-medarbejder](#).

LOV

[AI-forordningen § 99, stk. 7](#)
[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1-4](#)

PRAKSIS	EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	27.02.2025
	EU-Domstolen · Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar	28.11.2024
	EU-Domstolen · Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten	30.01.2024
	EU-Domstolen · Automatisk kreditscoring som en individuel afgørelse efter GDPR	07.12.2023
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	18.12.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023
	Ligebehandlingsnævnet · Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige	12.05.2022

REFERENCE Lovgrundlag

8 paragraffer

AI-forordningen § 5	stk. 1	AI-forordningen § 6	stk. 2, 3
AI-forordningen § 99	stk. 3-7	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2	stk. 1-5
Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3		Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 6	stk. 1
Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 8	stk. 1, 2	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10	stk. 1-4

MATERIALE Citerede afgørelser

22 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		7
20.11.2025	Beskyttelse af personoplysninger: Politiets indsamling og opbevaring af biometriske og genetiske data fra mistænkte	C-57/23
27.02.2025	Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	C-203/22
28.11.2024	Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar	C-80/23
04.10.2024	Politimyndigheders adgang til mobiltelefoner: Krav om retslig kontrol og proportionalitet ved databehandling i straffesager	C-548/21
21.03.2024	Ugyldighed af forordning om biometriske identitetskort pga. forkert retsgrundlag (C-61/22)	C-61/22
30.01.2024	Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten	C-118/22
07.12.2023	Automatisk kredit scoring som en individuel afgørelse efter GDPR	C-634/21
LANDSRETTEEN · ANKEINSTANS		1
12.06.2025	Ubetinget fængsel for fremstilling, besiddelse og udbredelse af over 36.000 AI-genererede billeder af børnepornografisk karakter	S-0141-25
BYRETTEEN · FØRSTE INSTANS		1
08.01.2025	Dom for fremstilling og udbredelse af AI-genereret børnepornografi	6888-8272
DATATILSYNET · NÆVN / KLAGEINSTANS		11
09.10.2025	Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	2025-31-1798
18.12.2024	F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	2024-51-0012
13.09.2024	Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag	2024-32-0482
27.06.2024	IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	2023-431-0018
12.06.2024	Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	2024-212-0371
23.05.2024	Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	2023-423-0005
30.01.2024	Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	2023-211-0004
22.12.2023	Alvorlig kritik og påbud til Hillerød Kommune for utilstrækkelig behandlingssikkerhed og manglende risikovurderinger	2023-423-0009
17.11.2023	Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	2023-212-0015
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676

26.02.2020	Tilsyn med Rejsekort & Rejseplan A/S og overholdelse af retten til indsig	2019-41-0031
------------	---	--------------

LIGEBEHANDLINGSNÆVNET · NÆVN / KLAGEINSTANS	1
---	---

12.05.2022	Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige	20-25601
------------	---	----------

PROCESBEVILLINGSNÆVNET · NÆVN / KLAGEINSTANS	1
--	---

21.11.2025	3.-instansbevilling: Strafmåling for besiddelse og udbredelse af ca. 36.000 AI-genererede børnepornografiske billeder (U 2025.3571 V)	U 2025.3571 V
------------	---	---------------

02

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over AI-systemer og persondata

Datatilsynets praksis om retsgrundlag, automatiske afgørelser og transparens – og samspillet med AI-forordningen

Version 2 · Opdateret 15. jul. 2026 · 23 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

AI-systemer, der behandler personoplysninger, reguleres i dag af to regelsæt på én gang: databeskyttelsesforordningen, der er teknologineutral og har været gældende siden 2018, og AI-forordningen (EU) 2024/1689, der siden august 2024 er trådt trinvis i kraft. Datatilsynets praksis har på få år udviklet en klar keredoktrin: en offentlig myndighed kan som udgangspunkt *udvikle* og *gentræne* en AI-løsning med hjemmel i den lovgivning, der pålægger myndigheden opgaven, men *driften* af løsningen kræver et tilstrækkeligt klart supplerende nationalt retsgrundlag – og kravet til klarhed stiger med indgrebets intensitet. Den doktrin har udløst en hel bølge af danske hjemmelsbekendtgørelser i 2025-2026 og et generelt lovforslag om AI i den offentlige forvaltning, der var i høring i februar 2026. Oversigten samler Datatilsynets afgørelser og udtalelser, EU-Domstolens praksis om GDPR art. 22 og 15 samt Folketingets Ombudsmands praksis om automatiserede sagsskridt.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Udvikling og gentræning af en AI-løsning kan efter Datatilsynets praksis ske på grundlag af den sektorlovgivning, der forpligter myndigheden til opgaven, mens DRIFTEN af løsningen kræver et selvstændigt og tilstrækkeligt klart nationalt retsgrundlag (j.nr. 2023-212-0015).
- 02** Kravet til retsgrundlagets klarhed er glidende: jo mere indgribende behandlingen af personoplysninger i AI-løsningen er for borgeren, desto klarere skal hjemlen være.
- 03** Udvikling af en AI-løsning anses databeskyttelsesretligt som et SELVSTÆNDIGT formål – forskelligt fra myndighedens daglige drift – og skal derfor hjemles og formålsafgrænses særskilt.
- 04** En trænet AI-model udgør som klart udgangspunkt ikke i sig selv personoplysninger; risikoen for genidentifikation ved målrettede angreb ændrer ikke dette (j.nr. 2023-212-0021).
- 05** GDPR art. 22 er ikke et generelt forbud, men en ret for den registrerede – den rammer kun afgørelser, der ALENE er baseret på automatisk behandling uden faktisk og reel menneskelig involvering, og som evaluerer personlige forhold.

- 06** Ren matematisk beregning uden evaluering af personlige forhold falder uden for art. 22; beslutningsstøtte, hvor en sagsbehandler reelt træffer afgørelsen, gør det også – men understøttelsen må ikke være proforma.
- 07** EU-Domstolen har i C-634/21 (SCHUFA) fastslået, at en automatisk fastsat scoringsværdi selv udgør en "afgørelse" efter art. 22, når tredjemand i afgørende grad lægger den til grund for sin beslutning.
- 08** Indsigtsretten i "logikken" bag en automatisk afgørelse, jf. art. 15, stk. 1, litra h, kræver en forståelig forklaring af den procedure og de principper, der konkret er anvendt – ikke udlevering af algoritmen – og forretningshemmeligheder skal i givet fald forelægges tilsynsmyndighed eller domstol til afvejning (C-203/22).
- 09** De danske AI-bekendtgørelser fra 2025-2026 tillader mønstergenkendelse og profilering til sagsUNDERSTØTTELSE, men forbyder udtrykkeligt afgørelser truffet alene på grundlag af automatisk behandling.
- 10** Bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen pålægger en oplysningspligt, der går VIDERE end GDPR art. 13-14: det skal tydeligt fremgå for borgeren, når kunstig intelligens anvendes.
- 11** Ansigtsgenkendelse er behandling af biometriske data og forudsætter enten udtrykkeligt samtykke med reelle alternativer eller – for private – en konkret tilladelse fra Datatilsynet efter databeskyttelseslovens § 7, stk. 4; tilladelser gives snævert og formålsbestemt.
- 12** Datatilsynet er markedsovervågningsmyndighed for AI-forordningens forbud mod prædiktiv kriminalitetsprofilering og biometrisk kategorisering (art. 5, stk. 1, litra d og g), mens Digitaliseringsstyrelsen fører tilsyn med de øvrige forbud.
- 13** AI-forordningen berører ikke databeskyttelsesforordningen (art. 2, stk. 7) – compliance med den ene giver ikke lovlighed efter den anden.
- 14** Folketingets Ombudsmand kræver, at forvaltningsretlige krav – officialprincip, partshøring, begrundelse – tænkes ind fra START ved udvikling af automatiserede systemer; automatisering forudsætter, at sagsskridtet kan foretages efter objektive kriterier uden individuelt skøn.

To regelsæt, ét system: databeskyttelsesforordningen og AI-forordningen side om side

§ 1

AI-systemer, der behandler personoplysninger, er underlagt **begge** regelsæt samtidig. Det er ikke et valg. [AI-forordningens artikel 2, stk. 7](#) fastslår udtrykkeligt, at forordningen ikke berører databeskyttelsesforordningen:

EU-retten om beskyttelse af personoplysninger, privatlivets fred og kommunikationshemmeligheden finder anvendelse på personoplysninger, som behandles i forbindelse med de rettigheder og forpligtelser, der er fastsat i denne forordning. Denne forordning berører ikke forordning (EU) 2016/679 [...]

Det betyder i praksis, at et AI-system godt kan være fuldt ud lovligt efter AI-forordningen (fx fordi det ikke er et højrisikosystem) og alligevel ulovligt, fordi der ikke er et gyldigt behandlingsgrundlag efter [GDPR artikel 6](#). Omvendt gør et gyldigt GDPR-hjemmelsgrundlag ikke en forbudt AI-praksis lovlig.

AI-forordningen trådte i kraft i august 2024 og finder anvendelse **trinvis**. Af forarbejderne til den danske gennemførelseslov fremgår tidsplanen:

Tidspunkt	Hvad finder anvendelse
2. februar 2025	Kapitel I (almindelige bestemmelser) og kapitel II (forbudte former for AI-praksis)
2. august 2025	Bla. kapitel III, afdeling 4, kapitel V (AI-modeller til almen brug), VII (forvaltning) og XII (sanktioner) samt art. 78
2. august 2026	Forordningen i øvrigt
2. august 2027	Artikel 6, stk. 1 (højrisiko-AI i produkter) og de tilsvarende forpligtelser

Danmark har suppleret forordningen ved [lov nr. 467 af 14. maj 2025 om supplerende bestemmelser til forordningen om kunstig intelligens](#), der efter [§ 12](#) trådte i kraft den 2. august 2025. Loven regulerer indtil videre kun tilsynet med de **forbudte** former for AI-praksis. Kompetencefordelingen efter [§ 2](#) er central for denne praksisoversigt:

- **Digitaliseringsstyrelsen** er bemyndigende myndighed, centralt kontaktpunkt og markedsovervågningsmyndighed for [artikel 5, stk. 1, litra a-c](#) og [litra e-f](#) (manipulerende teknikker, udnyttelse af sårbarheder, social scoring, ansigtsgenkendelsesdatabaser skabt ved ikke-målrettet indsamling, følelseggenkendelse på arbejdsplads og uddannelsesinstitution).
- **Datatilsynet** er markedsovervågningsmyndighed for [artikel 5, stk. 1, litra d](#) (prædiktiv kriminalitetsprofilering) og [litra g](#) (biometrisk kategorisering med henblik på at udlede race, politiske anskuelser, seksuel orientering m.v.) – dog kun for de dele, der ikke er omfattet af det danske retsforbehold.
- **Domstolsstyrelsen** fører tilsyn med domstolenes *administrative* brug af AI-systemer.

Af lovforarbejderne fremgår, at de kompetente myndigheder skal virke **funktionelt uafhængigt**:

De nationale kompetente myndigheders eventuelle overordnede myndigheder har således ikke instruktionsbeføjelse i de opgaver og sager, som behandles i medfør af den foreslåede lov, herunder i forbindelse med de nationale kompetente myndigheders udførelse af tilsyn og kontrol.

Efter [§ 3](#) kan myndighedernes afgørelser ikke indbringes for anden administrativ myndighed. Et efterfølgende lovforslag om en samlet dansk "AI-lov" ([L 111, fremsat 18. februar 2026](#)), der ville have ophævet 2025-loven og udbygget tilsynsbeføjelserne, **bortfaldt**. Retsstillingen er derfor fortsat lov nr. 467 af 14. maj 2025.

LOV

[AI-forordningen § 2, stk. 7](#)

[AI-forordningen § 5, stk. 1](#)

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2](#)

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3](#)

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 12](#)

§ 2 Hvornår foreligger der en "afgørelse alene baseret på automatisk behandling"? Afgrænsningen af GDPR art. 22

GDPR artikel 22, stk. 1 giver den registrerede ret til ikke at være genstand for en afgørelse, der **alene** er baseret på automatisk behandling, herunder profilering, og som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende. Bestemmelsen er ikke et generelt forbud. Betænkningsudvalget bag den danske databeskyttelseslov fastslog i [betænkning nr. 1565/2017, s. 371](#):

Det samme ses at være tilfældet med databeskyttelsesforordningen, idet bestemmelsen som anført stort set har samme ordlyd som direktivet, og da der heller ikke ses at fremgå et direkte forbud mod automatiske individuelle afgørelser. Forordningens artikel 22, vil derfor ligesom efter persondatalovens § 39 [...] skulle ses som en indsigelsesret for den registrerede.

Tre afgrænsninger er afgørende i praksis:

1) Der skal evalueres personlige forhold. Betænkningen fremhæver på [s. 373](#), at rene beregninger falder udenfor:

Der vil således ikke være tale om en afgørelse i artikel 22's forstand, såfremt den afgørelse, der træffes, sker ved en rent matematisk udregning ud fra de givne faktuelle forudsætninger, uden at der dermed sker en evaluering af personlige forhold vedrørende vedkommende.

Det er baggrunden for, at fx **automatisk hastighedsmåling og sektionskontrol** ikke er et art. 22-problem, men et almindeligt hjemmels- og proportionalitetsspørgsmål. I [2025-31-1798](#) vurderede Datatilsynet lovligheden af sektionskontrol på Storebæltsbroen efter [artikel 6, stk. 1, litra e](#) og dataminimeringsprincippet – ikke efter art. 22.

2) Afgørelsen skal have retsvirkning eller betydeligt påvirke. Betænkningen nævner som eksempler et forsikringsselskabs automatiske afslag på at tegne en police eller på at dække en skade, en banks automatiske afslag på lån, og et automatiseret frasorteringssystem i rekruttering. Generel markedsføring er derimod ikke omfattet.

3) "Alene" betyder uden reel menneskelig involvering. Den nyeste danske normering findes i [vejledningen til bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen](#) (januar 2026):

Ved automatisk behandling forstås en afgørelse, der alene er baseret på automatisk behandling uden en vis grad af faktisk og reel menneskelig involvering.

Ordet **faktisk og reel** er kernen: et pro forma-klik af en sagsbehandler, der ikke reelt kan tilsidesætte modellens output, gør ikke afgørelsen "menneskelig".

EU-Domstolen har skubbet grænsen udad. I [C-634/21](#) (SCHUFA, 7. december 2023) fastslog Domstolen, at et kreditoplysningsbureaus automatiske fastsættelse af en **scoringsværdi** i sig selv udgør en "afgørelse" i art. 22, stk. 1's forstand, når tredjemand – fx en bank – i afgørende grad lægger værdien til grund for sin beslutning om at indgå eller afvise en aftale. Det er en vigtig præcisering for AI-baserede scoring- og risikomodeller: **den, der leverer scoren, kan ikke gemme sig bag, at det formelt er kunden, der træffer beslutningen.** Samme dag afgjorde Domstolen [C-26/22](#), hvor grænserne for kreditoplysningsbureauers lagring af oplysninger blev fastlagt, og hvor det blev slået fast, at tilsynsmyndighedens afgørelser er undergivet **fuld** domstolsprøvelse.

LOV	Databeskyttelsesforordningen § 6, stk. 1	Databeskyttelsesforordningen § 22, stk. 1
PRAKSIS	EU-Domstolen · Automatisk kredit scoring som en individuel afgørelse efter GDPR	07.12.2023
	EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
	Datatilsynet · Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	09.10.2025

§ 3 Datatilsynets keredoktrin: udvikling kan hjemles i opgavelovgivningen – drift kræver et klart nationalt retsgrundlag

Den vigtigste enkeltafgørelse i dansk AI-databeskyttelsespraksis er Datatilsynets udtalelse af 17. november 2023 til Københavns Kommune, [j.nr. 2023-212-0015](#). Kommunen ville udvikle, idriftsætte og gentræne en AI-løsning, der som **beslutningsstøtte** for sagsbehandlere i sundheds- og omsorgsforvaltningen skulle identificere borgere med behov for vedligeholdende træning og rehabiliterende indsats. Datatilsynets vurdering:

Det er Datatilsynets vurdering, at udvikling, drift og gentræning af en AI-løsning, hvor der behandles personoplysninger og særlige kategorier af personoplysninger med henblik på at forudsige borgeres behov for og gavn af genoptræning for at undgå funktionsnedsættelse generelt kan ske på baggrund af databeskyttelsesforordningens artikel 6, stk. 1, litra e, samt artikel 9, stk. 2, litra g. Begge bestemmelser forudsætter dog et såkaldt supplerende nationalt retsgrundlag.

Og dernæst den afgørende sontring:

Behandling af personoplysninger til udvikling, herunder gentræning, af løsningen kan efter Datatilsynets vurdering ske under henvisning til de eksisterende bestemmelser i serviceloven, der forpligter kommunen til at træffe afgørelse om og levere vedligeholdende træning og rehabiliterende indsats.

Behandling af personoplysninger som led i driften af løsningen kan imidlertid ikke ske inden for rammerne af disse bestemmelser, da der ikke er tale om et tilstrækkeligt klart retsgrundlag i lyset af, hvor indgribende en behandlingsaktivitet der er tale om.

Doktrinen er dermed:

- **Udvikling og gentræning** ⇒ kan bæres af den sektorlov, der pålægger myndigheden opgaven ([art. 6, stk. 1, litra e](#) og [art. 9, stk. 2, litra g](#)).
- **Drift** ⇒ kræver et *særskilt* og *tilstrækkeligt klart* nationalt retsgrundlag.
- **Klarhedskravet er glidende**. Som Beskæftigelsesministeriet gengav doktrinen i bemærkningerne til [lovforslaget om Arbejdstilsynets AI-anvendelse \(L 143, 2024-25\)](#):

Kravet til klarheden af det nationale retsgrundlag afhænger således af, hvor indgribende behandlingen af personoplysninger, der finder sted i den pågældende løsning, vil være for borgeren; jo mere indgribende behandlingen er, desto mere klart skal det nationale retsgrundlag være for behandlingen af personoplysninger i driften af en kunstig intelligens-løsning.

Datatilsynet støtter kravet på EU-Domstolens dom af 24. februar 2022 i **sag C-175/20**, hvorefter lovgivningen bag behandlingen skal fastsætte "klare og præcise regler, der regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning, og som opstiller mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier".

Samme spor ses i den tidligere udtalelse [j.nr. 2022-212-3676](#) om kommunernes brug af **AI-værktøjet Asta**, hvor Datatilsynet vurderede retsgrundlaget med inddragelse af både [art. 6, stk. 1](#), [art. 9, stk. 2](#) og [art. 22, stk. 2](#) samt [databeskyttelseslovens § 7, stk. 4](#), [§ 11, stk. 1](#) og officialprincippet i [retssikkerhedslovens § 10](#). Kombinationen er sigende: spørgsmålet om automatiske afgørelser kan ikke behandles isoleret fra spørgsmålet om, hvorvidt sagen overhovedet er tilstrækkeligt oplyst.

Doktrinen blev anvendt igen i [j.nr. 2024-212-0371](#) om en AI-løsning til sagsbehandling af **SU-ansøgninger**, hvor Datatilsynet udtrykkeligt henviste tilbage til udtalelsen af 17. november 2023 og til tilsynets egen skabelon til konsekvensanalyse ved AI-løsninger, og hvor både [art. 6, stk. 1, litra e](#) og [art. 35, stk. 1](#) indgik i vurderingen.

LOV

[Databeskyttelsesforordningen § 6, stk. 1](#)
[Databeskyttelsesforordningen § 9, stk. 2](#)
[Databeskyttelsesforordningen § 22, stk. 2](#)
[Databeskyttelsesforordningen § 35, stk. 1](#)
[Databeskyttelsesloven § 7, stk. 4](#)
[Databeskyttelsesloven § 11, stk. 1](#)

PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	12.06.2024
	Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023
	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	18.05.2022

Hjemmelsbølgen 2025-2026: bekendtgørelserne som lovgivers svar på Datatilsynets praksis

Datatilsynets krav om et "tilstrækkeligt klart nationalt retsgrundlag" for **driften** af AI-løsninger satte myndighederne skakmat. Digitaliseringsministeriets AI-taskforce konstaterede i [juni 2025](#), at "mange myndigheder støder i dag på juridiske uklarheder", og at taskforcen derfor ville "iværksætte en indsats for at etablere hjemler til brug af kunstig intelligens i den offentlige sektor".

Resultatet er en serie sektorspecifikke hjemmelsbekendtgørelser, der alle følger samme skabelon: bemyndigelse i sektorloven → bekendtgørelse med udtømmende opregning af datakategorier → sikkerhedskrav → forbud mod fuldautomatiske afgørelser.

Bekendtgørelse	Myndighed	Nøgleindhold
Bek. nr. 813 af 26. juni 2025	Uddannelses- og Forskningsstyrelsen	AI til at <i>understøtte</i> SU-sagsbehandling; formålet er at optimere sagsbehandlingsprocesser
Bek. nr. 868 af 28. juni 2025	Arbejdstilsynet	Samkøring og behandling i AI-løsninger til tilsyns- og vejledningsopgaver efter arbejdsmiljølovens § 72; udtømmende liste over 16 datakategorier – inkl. helbred, race, religion og strafbare forhold
Bek. nr. 100 af 20. januar 2026	Styrelsen for Arbejdsmarked og Rekruttering	Udvikling, idriftsættelse og træning af AI-modeller
Bek. nr. 101 af 20. januar 2026	Kommunerne (beskæftigelsesindsatsen)	Mønstergenkendelse og profilering tilladt til sagsunderstøttelse – men forbud mod fuldautomatiske afgørelser

Den kommunale beskæftigelsesbekendtgørelse er den mest gennemarbejdede. § 1 tillader udtrykkeligt mønstergenkendelse og profilering, genanvendelse af data til nye AI-behandlinger og træning af modeller – men slutter med en skarp begrænsning i stk. 6:

Kommunerne kan ikke efter bestemmelserne i denne bekendtgørelse træffe afgørelser, der alene er baseret på automatisk behandling, herunder profilering.

Vejledningen af 23. januar 2026 forklarer, at bestemmelsen "er en gengivelse af databeskyttelsesforordningens artikel 22, stk. 1", og at AI-behandlingen derfor "alene [skal være] sagsunderstøttende". Lovgiver har med andre ord *ikke* villet udnytte det nationale råderum i art. 22, stk. 2, litra b til at hjemle automatiske afgørelser på beskæftigelsesområdet. Samme linje ses i bemærkningerne til [beskæftigelsesreformen](#) (L 66, 2025-26):

Det er ikke hensigten, at bemyndigelsen skal kunne anvendes til at fastsætte regler om anvendelse af løsninger, der anvender kunstig intelligens til f.eks. profilering af borgerne med henblik på at træffe automatiske afgørelser.

Det står i modsætning til fx [L 75 om projektilskud på Kulturministeriets område \(2025-26\)](#), hvor der *netop* skabes hjemmel til automatiseret sagsbehandling – og hvor lovgiver til gengæld udtrykkeligt indbygger art. 22, stk. 3-garantierne: mulighed for at anmode om genoptagelse ved menneskelig indgriben og ret til at fremkomme med sine synspunkter.

Den store brik mangler dog stadig. Digitaliseringsstyrelsen sendte den 12. februar 2026 et [lovforslag om en generel hjemmel til udvikling og anvendelse af AI-systemer og behandling af personoplysninger i den offentlige forvaltning](#) i høring med frist 2. marts 2026. Indtil det vedtages, må hver myndighed fortsat finde sin egen hjemmel – og Datatilsynets doktrin er den gældende målestok.

LOV

[Bekendtgørelse om Arbejdstilsynets anvendelse af kunstig intelligens § 3](#)[Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens eller lignende digitale løsninger i beskæftigelsesindsatsen § 1](#)[Databeskyttelsesforordningen § 22, stk. 1, 2](#)

PRAKSIS

Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor 17.11.2023

§ 5 Træningsdata og modeller: er en AI-model personoplysninger?

Spørgsmålet om træningsdata og modellers retlige status blev afklaret i Datatilsynets udtalelse [j.nr. 2023-212-0021](#) af 19. januar 2024. Sagen udsprang af et tværkommunalt samarbejde (med Sønderborg Kommune), der udviklede sprogmodeller til at identificere fortrolige oplysninger i sagsakter ved besvarelse af **aktindsigtsanmodninger**. Datasættet var dannet ved dataskrab fra danske kommuners hjemmesider.

Datatilsynet nåede frem til tre principielle vurderinger.

Modellen er som udgangspunkt ikke personoplysninger:

Datatilsynet lægger til grund, at en AI-model som et klart udgangspunkt ikke i sig selv udgør personoplysninger, men alene er resultatet af behandlingen af personoplysninger. Det svarer til, at en statistisk rapport ligeledes ikke vil anses som personoplysninger, hvis rapporten alene indeholder konklusioner og aggregerede data, der er resultaterne af den statistiske analyse.

Og videre om memorisering og angreb:

Risikoen for, at en ondsindet aktør genidentificerer borgere ved bevidst at gennemføre et angreb for at udlede data, der har indgået i træningsdata, indebærer efter Datatilsynets opfattelse således ikke, at modellen skal anses som personoplysninger i sig selv.

Udvikling er et selvstændigt formål:

Udviklingen af en AI-løsning skal efter Datatilsynets opfattelse anses som et formål i sig selv i konteksten af databeskyttelsesreglerne. Behandling af personoplysninger med henblik på at udvikle nye teknologiske løsninger tjener i sagens natur et andet formål end behandling af personoplysninger som led i myndighedens daglige drift.

Det er en central pointe for formålsbegrænsningen i [art. 5, stk. 1, litra b](#): man kan ikke uden videre genbruge driftsdata til modeludvikling – det kræver sin egen formåls- og hjemmelsvurdering.

Produktionsdata kan være nødvendige – og fravalg kan i sig selv være usikkert:

Jo tættere du (som virksomhed eller som myndighed) kommer på produktionsfasen, jo mere velbegrundet kan det være, at du anvender (flere) produktionsdata – herunder personoplysninger. Nogle gange vil det endda være et udtryk for manglende sikkerhed at sætte et system i produktion uden at have testet med produktionsdata – herunder personoplysninger – først.

Datatilsynet har i en parallel udtalelse om **etablering og deling af datasæt** (januar 2024, Alexandra Instituttet) taget stilling til lydoptagelser og fastslået, at en stemme kan gøre en person identificerbar, netop fordi "den nuværende teknologi, herunder stemmegenkendelsesværktøjer og kunstig intelligens, gør det muligt at gennemføre analyser og identificering". Datasættet kunne udgøre **biometriske data**, men var ikke omfattet af forbuddet i [art. 9, stk. 1](#), fordi behandlingen ikke skete med det formål entydigt at identificere en fysisk person. Det er den samme sontring, Datatilsynet anvendte i [j.nr. 2023-431-0018](#) (IDA Forsikring), hvor AI-analyse af transskriberede telefonsamtaler ikke faldt under art. 9, stk. 1, fordi systemet ikke anvendte stemmegenkendende teknologi og ikke havde til formål at identificere den, der ringede.

Den skarpe grænse går ved **ikke-målrettet indsamling af ansigtsbilleder**. I [j.nr. 2023-211-0004](#) afviste Datatilsynet webskrabning til opbygning af en biometrisk ansigtsgenkendelsesdatabase. Den praksis er nu kodificeret som en **forbudt AI-praksis** i [AI-forordningens artikel 5, stk. 1, litra e](#).

For højrisiko-AI stiller [AI-forordningens artikel 10](#) selvstændige krav til datastyring: datasæt skal være relevante, tilstrækkeligt repræsentative og i videst muligt omfang fejlfrie, og udbyderen skal undersøge og afbøde bias. [Artikel 10, stk. 5](#) indeholder en snæver, betinget hjemmel til undtagelsesvis at behandle **særlige kategorier af personoplysninger** – netop for at kunne påvise og korrigere bias – men kun når det er strengt nødvendigt, ikke kan opnås med syntetiske eller anonymiserede data, og under skrappe sikkerheds-, adgangs- og sletningsbetingelser.

Endelig et forbehold om data af tvivlsom oprindelse: i [j.nr. 2024-32-0482](#) fastslog Datatilsynet (efter forelæggelse for Datarådet), at rimelighedsprincippet i [art. 5, stk. 1, litra a](#) kræver en konkret vurdering af, **hvordan og af hvem** oplysningerne er tilvejebragt, over for de modsatrettede interesser. Myndigheden måtte i den sag godt anvende ulovligt optagne lydfile, fordi den ikke selv havde medvirket til den ulovlige aflytning, og fordi hensynet til barnets tarv vejede tungest. Overført på AI: **oprindelsen af træningsdata er en selvstændig rimelighedsparameter – ikke kun et hjemmelsspørgsmål**. (Ophavsretligt er billedet et andet: Østre Landsret

ophævede ved kendelse af 11. maj 2026 i sag **BS-55572/2025-OLR** et midlertidigt forbud mod scraping af data fra boligportal.dk, bl.a. under inddragelse af ophavsretslovens regler om tekst- og datamining.)

LOV

AI-forordningen § 5, stk. 1

AI-forordningen § 10, stk. 5

Databeskyttelsesforordningen § 5, stk. 1

Databeskyttelsesforordningen § 9, stk. 1

PRAKSIS	Datatilsynet · Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag	13.09.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	30.01.2024
	Datatilsynet · Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	19.01.2024

§ 6 Biometrisk AI: ansigtsgenkendelse mellem samtykke og tilladelse

Ansigtsgenkendelse er den AI-anvendelse, hvor Datatilsynet har den tætteste og mest konkrete praksis – og hvor koblingen til AI-forordningen er stærkest, fordi Datatilsynet er markedsovervågningsmyndighed for [artikel 5, stk. 1, litra g](#).

Udgangspunktet er, at behandling af ansigtsbilleder med henblik på entydig identifikation er behandling af biometriske data, jf. [art. 4, nr. 14](#), og dermed forbudt efter [art. 9, stk. 1](#), medmindre en undtagelse finder anvendelse. To spor findes i praksis:

Spor 1 – udtrykkeligt samtykke ([art. 9, stk. 2, litra a](#)). I [j.nr. 2023-31-0028](#) om ansigtsgenkendelse som adgangskontrol i fitnesscentre stillede Datatilsynet skarpe krav til frivilligheden:

I en situation som den foreliggende er det Datatilsynets opfattelse, at kravet om, at et samtykke skal være informeret, indebærer, at den registrerede skal oplyses om de alternativer, der er til samtykke til ansigtsgenkendelse.

Datatilsynet fandt, at adgang via reception i bemandet tid **ikke** var et reelt alternativ (det ville begrænse den 24/7-adgang, medlemmet betalte for), mens døgnsupport og engangskoder var det. Da klageren konkret var blevet fejlinformeret af en medarbejder, var hendes samtykke ugyldigt, og der blev udtalt kritik. Samtykket skal desuden **granuleres** – adgangskontrol og statistik kræver hvert sit samtykke. Det samme granuleringskrav slog igennem i [j.nr. 2023-431-0018](#), hvor IDA Forsikring kun indhentede ét samlet samtykke til både dokumentations- og kvalitetssikringsformål:

Datatilsynet kan konstatere, at der i forbindelse med, at en person ringer til IDA forsikring, alene indhentes ét samlet samtykke til både dokumentations- og kvalitetssikringsformål (uddannelse). Vedkommende, som ringer, får således ikke mulighed for at vælge kun at samtykke til et af formålene.

Spor 2 – tilladelse efter [databeskyttelseslovens § 7, stk. 4](#). Private dataansvarlige kan få Datatilsynets tilladelse til at behandle følsomme oplysninger af hensyn til væsentlige samfundsinteresser, jf. [art. 9, stk. 2, litra g](#). Bestemmelsen har efter forarbejderne "karakter af en opsamlingsbestemmelse" og "forudsættes at have et snævert anvendelsesområde". Datatilsynets praksis afspejler netop den snæverhed:

Sag	Formål	Udfald

2024-51-0012 (18. december 2024)	Ansigtsgenkendelse i Parken mod karantæneramte tilskuere	Tilladelse til fodboldkampe – men afslag for "øvrige arrangementer" (koncerter m.v.), da behandlingen dér ikke stod i rimeligt forhold til formålet
2024-51-0014 (16. juli 2025)	Superligaklubbers ansigtsgenkendelse mod karantæneramte	Tilladelse, med vilkår om bl.a. oplysningspligt og behandlingssikkerhed
Danske Shoppingcentre (8. december 2022)	Biometrisk behandling uden hjemmel	Politianmeldelse

FCK-sagen er den mest instruktive: tilladelsen blev **formålsopdelt**. Behandlingen kunne rummes inden for "væsentlige samfundsinteresser" i den kontekst (fodboldkampe, sikkerhed, karantænelister), men ikke automatisk overføres til enhver anden begivenhed på samme stadion. Proportionalitetsvurderingen er **kontekstbunden, ikke stedbunden**.

I ansættelsesforhold gælder en tredje hjemmel. I [j.nr. 2019-31-1650](#) accepterede Datatilsynet (efter behandling i Datarådet, med dissens) fingeraftryksbaseret adgangskontrol på et slagteri med hjemmel i [databeskyttelseslovens § 12, stk. 1](#) sammenholdt med DA/LO-aftalen om kontrolforanstaltninger, fordi entydig identifikation var nødvendig for at opfylde fødevarer sikkerheds- og certificeringskrav, og fordi der kun blev lagret krypterede templates – ikke billeder.

LOV

[AI-forordningen § 5, stk. 1](#)
[Databeskyttelsesforordningen § 9, stk. 1, 2](#)
[Databeskyttelsesloven § 7, stk. 4](#)
[Databeskyttelsesloven § 12, stk. 1](#)

PRAKSIS	Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	16.07.2025
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	18.12.2024
	Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	03.07.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger	08.12.2022
	Datatilsynet · Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	08.07.2020

§ 7 Transparens: oplysningspligt, indsigt og retten til at forstå "logikken"

Transparens er det område, hvor GDPR og AI-forordningen overlapper mest – og hvor de danske bekendtgørelser går videre end begge.

GDPR-sporet. Efter [art. 13, stk. 2, litra f](#) og [art. 15, stk. 1, litra h](#) skal den dataansvarlige oplyse om forekomsten af automatiske afgørelser og give "som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede". Betænkning nr. 1565/2017 forudså allerede spændingen med forretningshemmeligheder, jf. [s. 384](#):

Eksempelvis må det antages, at retten til indsigt efter artikel 22 i selve logikken bag en virksomheds afslag på kredit vil kunne begrænses efter eksempelvis forordningens artikel 23, stk. 1, litra i, om beskyttelse af andres rettigheder og frihedsrettigheder af hensyn til virksomhedens forretningshemmeligheder.

EU-Domstolen har nu afgjort, hvordan den afvejning skal foretages. I [C-203/22](#) (Dun & Bradstreet Austria, 27. februar 2025) fastslog Domstolen, at "meningsfulde oplysninger om logikken" kræver en **kortfattet, gennemsigtig og forståelig** beskrivelse af den procedure og de principper, der **konkret** er anvendt, så den registrerede kan forstå, hvilke af vedkommendes personoplysninger der er indgået, og hvordan de er blevet brugt. Udlevering af selve algoritmen eller den fulde matematiske formel er hverken tilstrækkeligt (det er ikke forståeligt) eller påkrævet. Påberåber den dataansvarlige sig forretningshemmeligheder, kan vedkommende ikke blot afvise indsigt: oplysningerne skal forelægges **tilsynsmyndigheden eller domstolen**, som herefter afvejer de modstående interesser. Sammenholdt med [C-634/21](#) betyder det, at scoringsleverandøren både er ansvarssubjekt for "afgørelsen" og forklaringspligtig for logikken.

Datatilsynets nationale praksis om oplysningspligt er streng, også når AI ikke er indblandet: se [j.nr. 2022-431-0204](#) (Tryk Forsikring, art. 13-14) og [j.nr. 2019-421-0028](#) (kritik af Udbetaling Danmarks håndtering af indsichtsretten). I [j.nr. 2023-431-0018](#) fandt Datatilsynet omvendt IDA Forsikrings information om AI-transskribering og -analyse tilstrækkelig – det indledende speak og persondatapolitikken opfyldte i det væsentlige art. 13.

Den danske skærpelse. [Bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen § 2, stk. 4](#) kræver, at det "tydeligt fremgår for den, hvis personoplysninger behandles, når kunstig intelligens anvendes". [Vejledningen](#) er utvetydig om, at der er tale om en **selvstændig, skærpet pligt**:

Oplysningspligten efter bekendtgørelsens § 2, stk. 4, går således videre end den almindelige oplysningspligt efter databeskyttelsesforordningen, da den indeholder et eksplicit krav om at oplyse om anvendelsen af kunstig intelligens, hvilket ikke altid vil være et krav efter oplysningspligten i artikel 13 og artikel 14.

Vejledningen accepterer, at pligten kan opfyldes fleksibelt – fx ved henvisning til en privatlivspolitik eller ved en oplysning i sagsbehandlerens autosignatur.

AI-forordningens spor. [Artikel 26, stk. 11](#) pålægger idriftsættere af bilag III-højrisikosystemer, der træffer eller bistår med at træffe beslutninger om fysiske personer, at underrette de pågældende om, at de er genstand for systemet. Og [artikel 86](#) giver en **selvstændig ret til forklaring**:

Enhver berørt person, der er omfattet af en afgørelse truffet af idriftsætteren på grundlag af output fra et højrisiko-AI-system opført i bilag III [...] og som har retsvirkninger eller på tilsvarende måde i væsentlig grad påvirker den pågældende person [...] har ret til at få en klar og meningsfuld forklaring fra idriftsætteren om AI-systemets rolle i beslutningsprocessen og hovedelementerne i den trufne afgørelse.

Retten er subsidiær: den finder efter [art. 86, stk. 3](#) kun anvendelse, "for så vidt den [...] omhandlede ret ikke på anden vis er fastsat i EU-retten" – dvs. den udfylder hullerne, hvor GDPR art. 15 ikke rækker (typisk fordi afgørelsen *ikke* er fuldautomatisk og derfor falder uden for art. 22).

LOV

[AI-forordningen § 26, stk. 11](#)[AI-forordningen § 86, stk. 1, 3](#)[Databeskyttelsesforordningen § 13, stk. 2](#)[Databeskyttelsesforordningen § 15, stk. 1](#)[Databeskyttelsesforordningen § 23, stk. 1](#)

PRAKSIS

EU-Domstolen · Indsichtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder 27.02.2025

EU-Domstolen · Automatisk kredit scoring som en individuel afgørelse efter GDPR 07.12.2023

Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne 27.06.2024

Datatilsynet · Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger

02.01.2024

Datatilsynet · Kritik af Udbetaling Danmarks håndtering af de registreredes ret til indsigt

26.02.2020

Konsekvensanalyse og risikostyring: DPIA, FRIA og det dobbelte § 8 spor

Brug af AI til behandling af personoplysninger vil ofte udløse pligt til **konsekvensanalyse** efter [GDPR artikel 35, stk. 1](#). Det er ikke en formalitet. [Vejledningen om digitaliseringsklar lovgivning](#) fremhæver eksplicit AI som en udløsende faktor:

Dette er navnligt tilfældet ved anvendelse af ny teknologi, fx brug af biometriske data, herunder iris-scanning, eller af kunstig intelligens, der skal behandle følsomme oplysninger, eksempelvis helbredsoplysninger.

Datatilsynets AULA-tilsyn viser, hvor hårdt tilsynet slår ned på mangelfulde konsekvensanalyser. I [j.nr. 2023-423-0005](#) udtalte Datatilsynet kritik af Københavns Kommune:

Det er imidlertid Datatilsynets vurdering, at Københavns Kommune ikke har gennemført en fyldestgørende konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35, stk. 1, idet den fremsendte konsekvensanalyse ikke opfylder mindstekravene hertil i forordningens artikel 35, stk. 7, litra a-d.

Analysen manglede en vurdering af nødvendighed og proportionalitet, beskrivelsen af formål, retligt grundlag og datakategorier var utilstrækkelig, og der var ingen entydig sammenhæng mellem konsekvensanalysen og de bagvedliggende risikovurderingsskemaer. Af de seks kommuner i tilsynsrunden fik **samtlig**e kritik eller alvorlig kritik på konsekvensanalysedelen, og to fik påbud om at udarbejde en analyse inden for tre måneder.

Datatilsynet har efterfølgende udgivet en dedikeret **skabelon til konsekvensanalyse ved AI-løsninger**, som tilsynet selv henviste til i SU-sagen [j.nr. 2024-212-0371](#), og som supplerer tilsynets vejledninger "Brug af kunstig intelligens i den offentlige sektor" og "Offentlige myndigheders brug af kunstig intelligens – Inden I går i gang" (begge oktober 2023).

Hertil kommer AI-forordningens **konsekvensanalyse vedrørende grundlæggende rettigheder** (FRIA) i [artikel 27](#), som offentligretlige organer og private, der leverer offentlige tjenester, skal foretage før idriftsættelse af bilag III-højrisikosystemer. De to analyser er **komplementære, ikke alternative** – art. 27, stk. 4 fastslår, at FRIA'en "supplerer" en DPIA foretaget efter GDPR art. 35, og [art. 26, stk. 9](#) pålægger omvendt idriftsætteren at bruge udbyderens oplysninger efter art. 13 til at opfylde sin DPIA-forpligtelse.

En særligt vigtig klassifikationsregel: efter [AI-forordningens artikel 6, stk. 3](#) kan et bilag III-system undtagelsesvis falde ud af højrisikokategorien, hvis det kun udfører en snæver proceduremæssig eller forberedende opgave – **men**:

Uanset første afsnit betragtes et AI-system, der er omhandlet i bilag III, altid som højrisiko, hvis AI-systemet udfører profilering af fysiske personer.

De danske bekendtgørelser tillader netop profilering til sagsunderstøttelse. Kommuner og styrelser, der udnytter den hjemmel på et bilag III-område, vil derfor som udgangspunkt være idriftsættere af et **højrisiko**-AI-system fra 2. august 2026 – med de dertil hørende pligter om menneskeligt tilsyn ([art. 26, stk. 2](#)), inputdatakvalitet, logopbevaring i mindst seks måneder og registrering i EU-databasen.

Størrelsesordenen er ikke trivial: Skatteforvaltningen oplyste i [april 2025](#), at den anvender 29 AI-modeller i kontrolarbejdet.

LOV	AI-forordningen § 6, stk. 3	AI-forordningen § 26, stk. 2, 9	AI-forordningen § 27
	Databeskyttelsesforordningen § 35, stk. 1, 7		
PRAKSIS	Datatilsynet · Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS) 10.07.2024 Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger 12.06.2024 Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024		

§ 9 Den private sektor: profilering, scoring og samtykkets grænser

I den private sektor er behandlingsgrundlaget et andet – men fejlene er de samme.

Forkert behandlingsgrundlag ved profilering. I [j.nr. 2019-32-0709](#) udtalte Datatilsynet **alvorlig kritik** af en privat virksomhed for at have anvendt et forkert behandlingsgrundlag ved profilering, med inddragelse af [art. 5, stk. 1](#), [art. 6, stk. 1](#) og [art. 13](#). Pointen generaliserer: en virksomhed kan ikke først vælge teknologien og bagefter lede efter en hjemmel.

AI-analyse er ikke nødvendigvis et nyt formål. I [j.nr. 2023-431-0018](#) (IDA Forsikring) blev telefonsamtaler optaget, transskriberet af en talegenkender og analyseret af AI-modeller for temaer, opkaldsårsager og indikative kvalitetsscoringer. Datatilsynet fastslog:

Det er i den forbindelse Datatilsynets opfattelse, at analysen af de optagne telefonsamtaler til brug for kvalitetssikring ikke skal anses for et selvstændigt formål. IDA Forsikring kan således basere analysen på samme grundlag som selve optagelsen af samtalen.

Selskabet kunne altså godt optage og AI-analysere samtalerne – men **samtykkeprocessen** holdt ikke, fordi der kun blev indhentet ét samlet samtykke til to formål. Datatilsynet pålagde selskabet fremadrettet at rette op, fx ved at kræve "to tryk" for at opnå den nødvendige granularitet, eller ved at basere optagelsen på et andet grundlag end samtykke.

Bemærk kontrasten til AI-udvikling i det offentlige: i [j.nr. 2023-212-0021](#) er *udvikling* af en model et selvstændigt formål, mens *analyse* som led i den løbende kvalitetssikring i IDA-sagen ikke var det. Sondringen er: **træner du en model, forfølger du et nyt formål; anvender du en model på data, du allerede lovligt behandler til et givet formål, gør du det typisk ikke.**

Samtykke og kontrakt som art. 22-undtagelser. Betænkning nr. 1565/2017 gennemgår på [s. 374-375](#) undtagelserne i [art. 22, stk. 2, litra a og c](#) og fremhæver, at nødvendighedskravet ved kontraktundtagelsen kan rumme ressourcemæssige hensyn – men **kun** hvis art. 22, stk. 3-garantierne er på plads. Betænkningen fastslår på [s. 380](#), at et samtykke efter litra c ikke er nok i sig selv: den dataansvarlige har samtidig ansvaret for at gennemføre passende foranstaltninger – **som minimum ret til menneskelig indgriben, til at fremkomme med synspunkter og til at bestride afgørelsen.**

Erstatning. Endelig har EU-Domstolen i [C-590/22](#) (20. juni 2024) præciseret rammerne for erstatningskrav efter [art. 82](#): en overtrædelse giver ikke i sig selv erstatning – der kræves skade og årsagssammenhæng – men skaden behøver ikke have en vis alvorsgrad, og erstatningen er rent **kompenserende**, ikke afskrækkende:

Den ret til erstatning, der er fastsat i databeskyttelsesforordningens artikel 82, stk. 1, har ikke en afskrækkende eller ligefrem straffende funktion. Erstatningsbeløbet kan således ikke fastsættes på et niveau, der overstiger fuld erstatning for denne skade.

For AI-leverandører betyder det, at den økonomiske risiko primært ligger i bøder og tilsynsindgreb – ikke i civile massekrav med pønalt præg.

LOV

[Databeskyttelsesforordningen § 6, stk. 1](#)

[Databeskyttelsesforordningen § 22, stk. 2, 3](#)

[Databeskyttelsesforordningen § 82, stk. 1](#)

PRAKSIS	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024
	Datatisynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatisynet · Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	19.01.2024
	Datatisynet · Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	03.11.2020

Forvaltningsretten oven på databeskyttelsen: ombudsmandens praksis om automatiserede sagsskridt

Databeskyttelsesretten regulerer *behandlingen* af oplysninger. Forvaltningsretten regulerer *afgørelsen*. En offentlig AI-løsning skal bestå begge prøver – og Folketingets Ombudsmand har i en lang række sager slået fast, at de forvaltningsretlige krav ikke fraviges, fordi sagsbehandlingen digitaliseres.

Allerede i [FOB 2014-34](#) rejste ombudsmanden problemstillingen generelt over for Finansministeriet, og Digitaliseringsstyrelsen og Justitsministeriet erklærede sig enige:

Grundlæggende forvaltningsretlige regler og principper skal naturligvis iagttages af offentlige myndigheder. Dette gælder uanset, om forvaltningen varetages manuelt eller digitalt. Reglerne om blandt andet partshøring, begrundelse af afgørelser, klagevejledning, vejledningspligt, notatpligt, parterets ret til aktindsigt, offentlige myndigheders tavshedspligt mv. fraviges således ikke, når forvaltningen digitaliseres.

I [FOB 2023-3](#) formuleredes kravet skarpt: det er "et grundlæggende krav, at offentlige it-systemer kan understøtte en korrekt anvendelse af den relevante lovgivning" – både formelle regler (partshøring, begrundelse) og materielle regler (udøvelse af skøn i den enkelte sag). Ansvar ligger hos myndigheden, **uanset om systemet er leveret af en ekstern leverandør**.

Den mest direkte AI-relevante udtalelse er [FOB 2026-6](#) om Skatteforvaltningens automatiserede SMV-løsning (marts 2026), hvor ombudsmanden formulerer automatiseringens strukturelle risiko:

Automatiserede afgørelsessystemer forudsætter dermed også, at myndighederne på forhånd kan afgrænse, hvilket faktum der måtte være relevant i fremtidige sager, idet den faktiske del af beslutningsgrundlaget ikke længere bliver genstand for myndighedens konkrete vurdering. Automatiserede systemer indebærer derfor en risiko for, at

myndighederne ikke fanger tilfælde med atypiske fakta eller tilfælde, hvor retsgrundlaget forpligter til at tage hensyn til forhold, der enten normalt ikke opstår eller normalt ikke er relevante.

Og om datakvalitet – direkte overførbart på AI-modellers inputdata:

Med automatiseringen vil systemet samtidig være direkte afhængigt af, at eksempelvis den underliggende sagsoplysning – systemets inddata – er tilstrækkelig og af den fornødne kvalitet.

Ombudsmanden fremhæver samme sted, at myndigheden må overveje, **om regelgrundlaget overhovedet understøtter den påtænkte automatisering**, idet "automatisering forudsætter bl.a., at de pågældende sagsskridt kan foretages uden udøvelse af et individuelt skøn og efter rent objektive kriterier". Det er den forvaltningsretlige pendant til Datatilsynets hjemmelskrav – og præcis den erkendelse, der ligger bag hjemmelsbølgen beskrevet ovenfor.

Hvad der sker, når automatiseringen fejler, viser [FOB 2025-13](#) om Vurderingsstyrelsens robotløsning, hvor samspillet mellem tilbagebetalingssystemet, administrationsgrundlaget og robotens automatiske sagsskridt "ikke fungerede efter hensigten". Og [FOB 2022-11](#) understreger, at ansvars- og rollefordelingen skal afklares, når flere systemer og myndigheder indgår i kæden frem mod en afgørelse – en pointe med stor vægt i AI-værdikæder med eksterne modelleverandører og databehandlere.

Underskriftskravet. Forvaltningsretten er dog ikke blind for automatisering: efter **forvaltningslovens § 32 b, stk. 2** gælder kravet om personlig underskrift ikke for dokumenter, hvor der anvendes automatisk sagsbehandling – dvs. "sagsbehandlingssystemer, der indebærer, at en sag helt eller delvist behandles og afgøres maskinelt på baggrund af faste og entydige kriterier, uden at en fysisk person sagsbehandler", jf. [vejledningen om digitaliseringsklar lovgivning](#).

Diskriminationsrisikoen. Automatiserede processer kan i sig selv være diskriminerende.

Ligebehandlingsnævnet fandt i [sag 21-9890](#), at en kommunes faste, it-understøttede praksis med automatisk at registrere **moderen** som "sagsperson" og betaler for institutionsplads – begrundet i, at børneydelsen typisk udbetales til mødre, og i systemets begrænsninger – udgjorde ulovlig forskelsbehandling på grund af køn. Afgørelsen illustrerer præcis den risiko, [AI-forordningens artikel 10, stk. 2, litra f](#) adresserer: bias, der "føre[r] til forskelsbehandling, som er forbudt i henhold til EU-retten".

Endelig har **Dataetisk Råd** i sit høringssvar til CBAM-lovforslaget ([L 17, 2024-25](#)) formuleret den principielle bekymring ved brede bemyndigelser til automatiseret sagsbehandling: at delegationen "reducerer den parlamentariske kontrol og offentlighedens indsigt", og at der mangler "klarhed om håndtering af klager og indsigt i afgørelsesgrundlaget". Rådet anbefalede klare rammer for åbenhed om algoritmerne og for prøvelse af automatisk trufne afgørelser.

LOV

[AI-forordningen § 10, stk. 2](#)[Databeskyttelsesforordningen § 22, stk. 1](#)

PRAKSIS

Ligebehandlingsnævnet · Kommunal praksis med automatisk valg af moderen som betaler for institutionsplads var kønsdiskriminerende

12.11.2022

§ 11 Håndhævelse og sanktioner: bøder efter to spor

Sanktionerne løber i to parallelle spor, og de kan ramme samme adfærd.

Databeskyttelsessporet. Danmark har ikke administrative bøder efter [GDPR artikel 83](#); i stedet politianmelder Datatilsynet og indstiller til bøde, jf. [databeskyttelseslovens § 41](#). Datatilsynet har gjort netop det på det biometriske område – se [politianmeldelsen af Danske Shoppingcentre](#) (december 2022) for ulovlig behandling af biometriske oplysninger.

Anklagemyndighedens behandling er detaljeret reguleret i [Rigsadvokatmeddelelsen, afsnittet om Databeskyttelse – Straffesager](#). Retningslinjerne indebærer bl.a., at **Datatilsynet skal høres i alle sager, inden der træffes afgørelse om tiltaleespørgsmålet**, at tiltaleespørgsmålet og strafpåstanden skal forelægges statsadvokaten, og at sagerne indtil videre **ikke må afgøres med bødeforelæg**, før sanktionsniveauet er tilstrækkeligt afklaret i retspraksis. Rigsadvokatmeddelelsen fastslår også, at bødeniveauet er markant hævet i forhold til persondataloven:

Reglerne i databeskyttelsesforordningen og databeskyttelsesloven lægger således op til en markant forøgelse af bødeniveauet i forhold til, hvad overtrædelser af persondataloven blev takseret til. Tidligere retspraksis kan derfor kun i meget begrænset omfang tillægges betydning ved afgørelse af sanktionsspørgsmålet efter de nuværende regler, mens såvel doms- som administrativ praksis fra andre EU-lande fremadrettet vil få øget betydning.

De momenter, der efter [art. 83, stk. 2](#) skal indgå i sanktionsvurderingen, gælder også ved bødeudmåling efter databeskyttelseslovens § 41, jf. lovens § 41, stk. 3.

AI-sporet. [AI-forordningens artikel 99, stk. 3](#) fastsætter for overtrædelse af de forbudte AI-praksisser i art. 5 administrative bøder på op til **35 mio. EUR eller 7 % af den samlede globale årlige omsætning** – det højeste beløb i hele EU's digitale regelværk. Danmark har valgt at sanktionere **strafferetligt**. Efter [AI-lovens § 10](#) straffes med bøde den, der bl.a. overtræder [artikel 5, stk. 1, litra a-g](#), afgiver urigtige oplysninger til myndighederne, hindrer kontrolbesøg eller undlader at efterkomme påbud eller midlertidige forbud. Der kan pålægges selskaber strafansvar efter straffelovens 5. kapitel, og **forældelsesfristen er 5 år**. Efter [§ 11](#) kan der fastsættes regler om bødeforelæg.

Af forarbejderne fremgår begrundelsen for valget:

Det er Digitaliseringsministeriets vurdering, at sanktioner for overtrædelser af forordningens bestemmelser efter dansk ret fastsættes som en strafferetlig sanktion i henhold til artikel 99, stk. 9, 1. pkt., jf. artikel 99, stk. 3 og 5.

Markedsovervågningsmyndighederne kan desuden kræve alle nødvendige oplysninger, få adgang til erhvervsmæssige lokaliteter **uden retskendelse**, udstede påbud, nedlægge midlertidige forbud mod et AI-system, der vurderes at kunne udgøre en risiko, og offentliggøre afgørelser i sager om forbudte former for AI-praksis.

Ikke-sanktionerede indgreb. I langt de fleste af Datatilsynets AI-sager er reaktionen dog en udtalelse, kritik eller alvorlig kritik – ikke bøde. Det gælder fx [j.nr. 2023-421-0015](#) (kritik af Udlændinge- og Integrationsministeriets behandling i Visuminformationssystemet efter art. 5, stk. 1, og art. 24, stk. 1) og AULA-sagerne. Praksis er med andre ord **vejledende og opdragende** snarere end pønalt – indtil videre.

LOV

[AI-forordningen § 99, stk. 3](#)[Databeskyttelsesforordningen § 83, stk. 2](#)[Databeskyttelsesloven § 41](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 11](#)

PRAKSIS

Datatilsynet · Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	10.07.2024
Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	23.05.2024
Datatilsynet · Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger	08.12.2022

§ 12 Sammenfatning: den danske AI-databeskyttelsesmodel i seks træk

Praksis tegner nu et forholdsvis klart billede, som kan sammenfattes i seks træk.

- 1. Hjemmelsdoktrinen er den styrende norm.** Datatilsynets udtalelse i [j.nr. 2023-212-0015](#) – udvikling ja, drift kun med klart nationalt retsgrundlag, med et klarhedskrav der skærpes med indgrebs intensitet – er blevet den centrale målestok. Den er gengivet ordret i forarbejderne til flere lovforslag og har fremtvunget en hel serie af hjemmelsbekendtgørelser.
- 2. Danmark har (endnu) ikke udnyttet art. 22-råderummet på de store velfærdsområder.** [Art. 22, stk. 2, litra b](#) tillader fuldautomatiske afgørelser med hjemmel i national ret og passende garantier. Men [bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen § 1, stk. 6](#) forbyder dem udtrykkeligt. AI er sagsUNDERSTØTTENDE – mennesket træffer afgørelsen. Kun på afgrænsede, objektivt regulerede områder (fx tilskudsadministration) har lovgiver skabt hjemmel til egentlig automatiseret sagsbehandling.
- 3. "Reel menneskelig involvering" er det kritiske skøn.** Fordi den danske model bygger på beslutningsstøtte, flytter det retlige tyngdepunkt sig til spørgsmålet om, hvornår sagsbehandlerens involvering er **faktisk og reel** – og ikke bare et gummistempel på modellens output. Her giver [C-634/21](#) et advarselssignal: hvis modellens score i praksis er determinerende, er der tale om en afgørelse i art. 22's forstand – uanset hvem der formelt trykker på knappen.
- 4. Transparens er skærpet, ikke lempet.** [C-203/22](#) kræver en forståelig forklaring af den konkret anvendte logik, og forretningshemmeligheder giver ikke ret til tavshed, men til en afvejning ved tilsynsmyndighed eller domstol. Nationalt kræver AI-bekendtgørelserne, at det **tydeligt fremgår**, når AI anvendes – en pligt, der udtrykkeligt går videre end GDPR art. 13-14. Og fra 2. august 2026 supplerer [AI-forordningens artikel 86](#) med en ret til forklaring, netop hvor GDPR art. 22 ikke rækker.
- 5. Biometri er den skarpeste grænse.** Ansigtsgenkendelse kræver enten et gyldigt, granuleret og reelt frivilligt samtykke ([j.nr. 2023-31-0028](#)) eller en snæver, formålsbestemt tilladelse efter [databeskyttelseslovens § 7, stk. 4](#) ([j.nr. 2024-51-0012](#) og [j.nr. 2024-51-0014](#)). Og ikke-målrettet webskrabning til ansigtsgenkendelsesdatabaser er nu **forbudt** AI-praksis – Datatilsynet nåede dertil allerede i [j.nr. 2023-211-0004](#), før AI-forordningen fik virkning.
- 6. Forvaltningsretten er den anden halvdel af regnestykket.** Ombudsmandens praksis – [FOB 2026-6-](#), [FOB 2025-13](#), [FOB 2023-3](#) og [FOB 2014-34](#) – kræver, at officialprincip, partshøring, begrundelse og notatpligt tænkes ind fra systemudviklingens første fase, og at myndigheden erkender automatiseringens blinde vinkel over for atypiske sager. En AI-løsning kan være databeskyttelsesretligt upåklagelig og alligevel forvaltningsretligt uholdbar.

Det åbne spørgsmål er, om Danmark får den generelle hjemmel, som Digitaliseringsstyrelsen sendte i høring den 12. februar 2026 – og hvor langt den i givet fald går. Så længe den mangler, forbliver Datatilsynets doktrin fra november 2023 den afgørende adgangsbillet til AI i den offentlige forvaltning.

LOV

AI-forordningen § 86

Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens eller lignende digitale løsninger i beskæftigelsesindsatsen § 1, stk. 6

Databeskyttelsesforordningen § 22, stk. 2

Databeskyttelsesloven § 7, stk. 4

PRAKSIS	EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	27.02.2025
	EU-Domstolen · Automatisk kredit scoring som en individuel afgørelse efter GDPR	07.12.2023
	Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	16.07.2025
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	18.12.2024
	Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	03.07.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	30.01.2024
	Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023

REFERENCE Lovgrundlag

10 paragraffer

AI-forordningen § 5	stk. 1	AI-forordningen § 26	stk. 11
AI-forordningen § 86	stk. 1	Databeskyttelsesforordningen § 6	stk. 1
Databeskyttelsesforordningen § 9	stk. 2	Databeskyttelsesforordningen § 15	stk. 1
Databeskyttelsesforordningen § 22	stk. 1-3	Databeskyttelsesforordningen § 35	stk. 1
Databeskyttelsesloven § 7	stk. 4	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2	

MATERIALE Citerede afgørelser

23 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		4
27.02.2025	Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	C-203/22
20.06.2024	Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	C-590/22
07.12.2023	Automatisk kredit scoring som en individuel afgørelse efter GDPR	C-634/21
07.12.2023	Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	C-26/22

DATATILSYNET · NÆVN / KLAGEINSTANS		18
09.10.2025	Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	2025-31-1798
16.07.2025	Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	2024-51-0014
18.12.2024	F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	2024-51-0012
13.09.2024	Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag	2024-32-0482
10.07.2024	Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	2023-421-0015
03.07.2024	Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	2023-31-0028
27.06.2024	IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	2023-431-0018
12.06.2024	Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	2024-212-0371
23.05.2024	Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	2023-423-0005
30.01.2024	Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	2023-211-0004
19.01.2024	Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	2023-212-0021
02.01.2024	Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	2022-431-0204
17.11.2023	Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	2023-212-0015
08.12.2022	Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger	
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676
03.11.2020	Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	2019-32-0709
08.07.2020	Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	2019-31-1650
26.02.2020	Kritik af Udbetaling Danmarks håndtering af de registreredes ret til indsigt	2019-421-0028
LIGEBEHANDLINGSNÆVNET · NÆVN / KLAGEINSTANS		1
12.11.2022	Kommunal praksis med automatisk valg af moderen som betaler for institutionsplads var kønsdiskriminerende	21-9890

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 1)
nr. 1565 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 2)
nr. 1565 · 2017 · Justitsministeriet

03

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over cookies og samtykke

Datatilsynets og EU-Domstolens praksis om gyldigt samtykke, dark patterns, cookie walls og fælles dataansvar

Version 2 · Opdateret 26. jun. 2026 · 14 afgørelser · 2019-2024

[Læs online](#)

INTRODUKTION

Cookies og online-tracking er reguleret i et samspil mellem ePrivacy-direktivet (direktiv 2002/58/EF, artikel 5, stk. 3), den danske cookiebekendtgørelse og GDPR. Datatilsynet har siden 2020 opbygget en omfattende praksis om gyldigt samtykke til cookies, der bl.a. omfatter krav om aktiv accept (forbud mod forudafkrydsede felter og "gå videre"-samtykke), forbud mod nudging via vildledende cookiebanner-design, betingelserne for "pay-or-track"-modeller og cookie walls samt krav om granulært og informeret samtykke. EU-Domstolen har med Planet49-dommen, Fashion ID-dommen og IAB Europe TCF-dommen fastlagt de grundlæggende EU-retlige rammer for cookie-samtykke og fælles dataansvar ved online-annoncering.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Cookies til statistik og markedsføring kræver et forudgående, aktivt samtykke – tavshed, forudafkrydsede felter, inaktivitet eller videre browsing udgør ikke et gyldigt samtykke.
- 02 Samtykkekravet i ePrivacy-direktivets artikel 5, stk. 3, gælder uafhængigt af, om de lagrede oplysninger er personoplysninger – beskyttelsen retter sig mod ethvert indgreb i terminaludstyret.
- 03 Cookies må aldrig placeres før brugeren har afgivet samtykke (pre-consent loading er ulovligt).
- 04 Et cookiebanner skal oplyse om alle behandlingsformål allerede i første lag – information gemt i et andet lag opfylder ikke informationskravet, når flertallet klikker 'Acceptér alle'.
- 05 Brug af farver og visuelle virkemidler i cookiebannere, der nudger brugeren mod at acceptere (fx trafiklys-systemer med rød/grå/grøn), er i strid med gennemsigtighedsprincippet i GDPR artikel 5, stk. 1, litra a.
- 06 Det skal være lige let at afvise cookies som at acceptere dem – asymmetri i klikantal eller visuelt design undergraver samtykkets frivillighed.
- 07 En 'pay-or-track'-model kan opfylde samtykkets frivillighedskrav, men kun hvis betalingsalternativet giver adgang til i vidt omfang tilsvarende indhold som samtykke-alternativet, og prisen ikke er urimelig høj.

- 08 En cookie wall, hvor indholdet ved betaling er væsentligt udvidet i forhold til gratis adgang med samtykke, opfylder ikke kravet om tilsvarende ydelser og gør samtykket ufrivilligt.
- 09 Samtykke til behandling til statistiske formål kan kun indgå som del af en pay-or-track-model, hvis virksomheden kan påvise, at statistisk behandling er nødvendig – ellers skal statistik-samtykke kunne gives særskilt.
- 10 Hjemmesideoperatøren er fælles dataansvarlig med tredjeparter (fx Google, Facebook) for indsamling og transmission af personoplysninger via integrerede tredjepartcookies, sociale plugins og annonce-tags.
- 11 Samtykke til tredjepartcookies skal indhentes af hjemmesideoperatøren – ikke af tredjeparten – og oplysningspligten over for brugeren påhviler ligeledes operatøren.
- 12 Oplysningspligten ved cookie-samtykke omfatter cookiernes funktionsvarighed, formål og oplysninger om tredjemands adgang.
- 13 En TC String (Transparency and Consent String) i IAB Europes TCF udgør en personoplysning, når den kan kobles til en IP-adresse, og IAB Europe er fælles dataansvarlig for registreringen af brugernes samtykkepræferencer.
- 14 Offentlige myndigheder kan ikke påberåbe sig legitim interesse som behandlingsgrundlag og skal derfor have gyldigt samtykke for ikke-nødvendige cookies.
- 15 Teknisk nødvendige cookies (session-cookies, login-funktionalitet mv.) er undtaget fra samtykkekravet efter cookiebekendtgørelsens § 4, men må ikke viderebehandles til andre formål.

Retsgrundlaget: ePrivacy-direktivet, cookiebekendtgørelsen og GDPR

§ 1

Reglerne om cookies og online-tracking hviler på et samspil mellem tre regelsæt:

ePrivacy-direktivet (direktiv 2002/58/EF) regulerer i artikel 5, stk. 3, lagring af og adgang til oplysninger i brugeres terminaludstyr. Bestemmelsen kræver forudgående samtykke fra brugeren, medmindre lagringen er teknisk nødvendig for at levere en tjeneste, som brugeren har anmodet om. Direktivet er gennemført i dansk ret via [cookiebekendtgørelsen](#).

[Cookiebekendtgørelsens § 3](#) fastsætter hovedreglen: Fysiske eller juridiske personer må ikke lagre oplysninger i eller opnå adgang til oplysninger i en slutbrugers terminaludstyr uden samtykke. Samtykket skal være baseret på fyldestgørende information, der bl.a. skal:

- Fremstå i et klart, præcist og letforståeligt sprog
- Indeholde oplysning om formålet med lagringen
- Identificere enhver person, der foranstalter lagringen
- Give brugeren umiddelbart tilgængelig adgang til at afslå eller tilbagekalde samtykke

[Cookiebekendtgørelsens § 4](#) undtager teknisk nødvendige cookies fra samtykkekravet. Undtagelsen dækker cookies, der alene tjener til at overføre kommunikation, eller som er en teknisk forudsætning for at levere den tjeneste, slutbrugeren har anmodet om.

Da ePrivacy-direktivets samtykkedefinition henviser til GDPR (efter 2018), skal samtykkekravene for cookies nu opfylde [GDPR artikel 4, nr. 11](#), som kræver en **frivillig, specifik, informeret og utvetydig viljestilkendegivelse**. GDPR's 32. betragtning præciserer udtrykkeligt, at tavshed, forudafkrydsede felter og inaktivitet ikke udgør samtykke. Erhvervsstyrelsen tilpasser tilsynskompetencen i forhold til selve lagringen (cookiebekendtgørelsen), mens Datatilsynet har kompetence over den personoplysningsbehandling, der følger af cookies.

Den officielle [Cookievejledning](#) fra 2019 ændrede Erhvervsstyrelsens praksis, så "gå videre"-samtykke (hvor brug af hjemmesiden anses som samtykke) ikke længere accepteres. Vejledningen fastslog, at EU-Domstolens dom i Planet49-sagen medfører, at videre brug af en hjemmeside kan sidestilles med et forudafkrydset felt og derfor ikke udgør et aktivt, specifikt samtykke.

LOV

[Cookiebekendtgørelsen § 3, stk. 1](#)[Cookiebekendtgørelsen § 4, stk. 1](#)[Databeskyttelsesforordningen \(GDPR\) § 4](#)[Databeskyttelsesforordningen \(GDPR\) § 6, stk. 1](#)

§ 2 EU-Domstolens krav til cookie-samtykke: Planet49-dommen

EU-Domstolens dom i [C-673/17 \(Planet49\)](#) af 1. oktober 2019 er den grundlæggende EU-retlige præcedens for cookie-samtykke. Dommen (Store Afdeling) fastslog tre principper, der alle har direkte virkning for dansk ret:

1. Forudafkrydsede felter er utilstrækkelige. Et samtykke til lagring af cookies er ikke gyldigt, når det baseres på et forudafkrydset felt, som brugeren aktivt skal fjerne for at nægte. Domstolen udtalte:

«Kun en aktiv adfærd fra denne person med henblik på at tilkendegive sit samtykke kan opfylde dette krav.» (præmis 54)

En generel "deltag"-knap i forbindelse med en online-konkurrence kan ikke i sig selv udgøre et specifikt samtykke til en anden behandling.

2. Samtykkekravet gælder uanset datatype. ePrivacy-direktivets artikel 5, stk. 3, beskytter brugerens terminaludstyr – og dermed privatsfæren – mod ethvert indgreb, uanset om de berørte oplysninger er personoplysninger. Spørgsmålet om datatype er irrelevant for samtykkekravets anvendelse.

3. Oplysningspligten omfatter funktionsvarighed og tredjemandsadgang. Brugeren skal oplyses om cookiernes levetid og om, hvorvidt tredjemand får adgang til oplysningerne. Disse informationer er nødvendige for, at brugeren kan bedømme konsekvenserne af et eventuelt samtykke.

Planet49-dommen førte direkte til, at Erhvervsstyrelsen ændrede sin praksis og ikke længere accepterer "gå videre"-samtykke. Datatilsynet har efterfølgende gentaget kravene i en række konkrete afgørelser.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 4](#)[Databeskyttelsesforordningen \(GDPR\) § 6, stk. 1](#)

PRAKSIS

EU-Domstolen · Krav om aktivt samtykke til cookies og rækkevidden af oplysningspligten (Planet49-sagen)

01.10.2019

§ 3 Krav om cookies-før-samtykke-forbud: pre-consent loading

Datatilsynet har i flere sager slået fast, at cookies aldrig må placeres på brugerens enhed, før samtykke er indhentet. Denne tekniske fejl – pre-consent loading – udgør i sig selv en selvstændig overtrædelse af GDPR.

I sagen om **Leadwise ApS** (2021-31-5282) blev der placeret cookies fra Google og Facebook på letfinans.dk, inden brugeren overhovedet havde interageret med samtykkebanneret. Virksomheden hævdede, at der blot var tale om "anonym besøgstatistik", men Datatilsynet fastslog, at cookies med onlineidentifikatorer som IP-adresser og cookie-ID'er udgør personoplysninger. Tilsynet udtalte **alvorlig kritik**.

I sagen om **Alstrøm – Din Isenkræmmer ApS** (2021-431-0125) blev 18 tredjepartscookies placeret ved sideindlæsning under en overgangsperiode til en ny samtykkeløsning. Datatilsynet udtalte **alvorlig kritik** og understregede, at en teknisk implementeringsfejl ikke fritager for ansvar.

I sagen om **DMI** (2018-32-0357) blev personoplysninger transmitteret til Google via annonce-tags, før brugeren havde givet samtykke. DMI anerkendte fejlen og ændrede kildekoden, men Datatilsynet udtalte alligevel **alvorlig kritik** og fastslog, at:

«Under alle omstændigheder skal samtykke altid opnås, inden den dataansvarlige indleder den behandling af personoplysninger, hvortil samtykket skal bruge.»

LOV	Databeskyttelsesforordningen (GDPR) § 6, stk. 1	
PRAKSIS	Datatilsynet · Alvorlig kritik af Leadwise ApS for utilstrækkeligt samtykke til markedsføring på letfinans.dk	23.12.2022
	Datatilsynet · Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies	20.10.2021
	Datatilsynet · Alvorlig kritik af DMI's behandling af personoplysninger om besøgende på dmi.dk	11.02.2020

§ 4 Dark patterns og nudging: krav til cookiebannerets design

Datatilsynets afgørelse om **JP/Politikens Hus (eb.dk)** (2021-41-0149) er den principielle danske afgørelse om dark patterns i cookiebannere. Datatilsynet udtalte **alvorlig kritik** på to selvstændige grundlag:

Trafiklys-nudging. Cookiebanneret anvendte tre knapper: "Kun nødvendige" (rød), "Tilpas Indstillinger" (grå) og "Acceptér alle" (grøn). Datatilsynet fandt, at dette udgjorde et trafiklys-lignende system, der pressede brugeren mod at klikke grøn:

«Det er Datatilsynets opfattelse, at brugen af farver ved valg af responsknapper – alt efter omstændighederne – kan påvirke besøgende til at foretage bestemte valg. Særligt er det tilsynets opfattelse, at brugen af et trafiklys lignende system kan udgøre en form for 'føring' (nudging), der ikke er forenelig med princippet i databeskyttelsesforordningens artikel 5, stk. 1, litra a.»

Manglende information i første lag. 72-75 % af brugerne valgte "Acceptér alle", men denne knap dækkede bl.a. præference-cookies, som først blev omtalt i andet lag. Datatilsynet fastslog, at alle behandlingsformål skal oplyses allerede i første lag af samtykkeløsningen.

I sagen om **Alstrøm** (2021-431-0125) fandt Datatilsynet tilsvarende, at knapperne "Acceptér" (orange tekst, hvid baggrund) og "ACCEPTÉR ALLE" (hvid tekst, orange baggrund) skabte en visuel skævhed, der skubbede brugeren mod "Acceptér alle".

I sagen om **DGU Erhverv (golf.dk)** (2020-31-3354) var der slet ingen mulighed for at afvise cookies – brugeren kunne kun klikke "Tillad alle cookies" eller "Vis detaljer". Samtykket opfyldte dermed hverken kravet om frivillighed eller granularitet.

På tværs af denne praksis kan følgende designprincipper udledes:

- Accept- og afvis-knapperne skal være visuelt ligestillede (samme størrelse, farvemæssig ligestillethed)
- Alle behandlingsformål skal fremgå af første lag
- Brugeren skal i første lag have mulighed for at afvise alle ikke-nødvendige cookies med ét klik
- Granularitet kræves – det skal være muligt at til- og fravælge de enkelte formål separat

LOV	Databeskyttelsesforordningen (GDPR) § 4	Databeskyttelsesforordningen (GDPR) § 5, stk. 1
PRAKSIS	Datatilsynet · Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	27.10.2022
	Datatilsynet · Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies	20.10.2021
	Datatilsynet · Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	13.11.2020

§ 5 Cookie walls og pay-or-track: Datatilsynets tre principielle afgørelser

Datatilsynets tre principielle Dataråds-afgørelser fra 2023-2024 om cookie walls og pay-or-track-modeller tegner de danske rammer for, hvornår adgang til en hjemmeside kan betinges af samtykke til cookies:

Gul og Gratis – godkendt pay-or-track (29 kr./md.)

I sagen 2021-31-4871 fandt Datatilsynet, at Gul og Gratis' pay-or-track-model *principielt* kan opfylde kravet om frivilligt samtykke, da:

- Brugeren tilbød et reelt valg (samtykke eller 29 kr./md.)
- Betaling gav adgang til en tjeneste, der i vidt omfang var tilsvarende
- Prisen ikke var urimelig høj

«Undladelse af at give samtykke indebærer derfor efter Datatilsynets opfattelse ikke negative konsekvenser for de besøgende.»

Tilsynet udstedte dog et påbud, fordi virksomheden ikke havde påvist, at samtykke til *statistiske formål* var en nødvendig del af alternativet.

Jysk Fynske Medier – underkendt cookie wall (99 kr./md.)

I sagen 2021-31-5553 underkendte Datatilsynet modellen, fordi de to alternativer ikke var tilsvarende: gratis adgang med samtykke gav kun adgang til "ulåste artikler", mens betaling (99 kr./md.) gav adgang til alle artikler. Denne forskel betød, at brugeren ikke havde et reelt frit valg.

Kriterium	Gul og Gratis (godkendt)	JFM (underkendt)
Tilsvarende indhold	Ja – identisk adgang	Nej – ulåste vs. alle artikler
Pris	29 kr./md.	99 kr./md.
Statistik-samtykke særskilt	Nej (påbud om ændring)	Nej (påbud om ændring)

Berlingske Media – underkendt delvis cookie wall

I sagen [2023-431-0010](#) blokerede Berlingske kun delindhold (videoafspillere, liveblogs) bag et samtykkekrav. Datatilsynet fastslog, at det er uden betydning, om det er hele hjemmesiden eller kun delindhold, der spærres – principperne om frivillighed og koppelingsforbudet i [GDPR artikel 7, stk. 4](#) gælder tilsvarende.

Forbrugerombudsmanden har indtaget en tilsvarende linje: I sagen om en elhandelsvirksomhed ([fom-80111-](#)) udtalte ombudsmanden, at det er i strid med god skik efter [markedsføringslovens § 3](#) at kræve accept af ikke-nødvendige cookies for at få adgang til nødvendige forbrugsoplysninger. Virksomheder skal give forbrugere adgang til nødvendige oplysninger "uden at forbrugerne skal betale for det, hverken i form af penge eller data."

LOV

[Databeskyttelsesforordningen \(GDPR\) § 4](#)
[Databeskyttelsesforordningen \(GDPR\) § 7, stk. 4](#)
[Markedsføringsloven § 3](#)

PRAKSIS	Datatilsynet · Ugyldigt samtykke ved brug af "cookie walls" hos Berlingske Media	14.02.2024
	Datatilsynet · Lovligheden af "Pay-or-track"-model hos Gul og Gratis	08.02.2023
	Datatilsynet · Lovligheden af cookie walls: Datatilsynets afgørelse i sagen om Jysk Fynske Medier	08.02.2023
	Forbrugerombudsmanden · Elhandelsvirksomhed krævede accept af unødvendige cookies for adgang til kundekonto: Tilsidesættelse af god skik	18.01.2022

§ 6 Fælles dataansvar ved tredjepartscookies: Fashion ID og DMI

Spørgsmålet om fælles dataansvar ved tredjepartscookies er afklaret gennem EU-Domstolens praksis og Datatilsynets konkrete afgørelser.

Fashion ID-dommen (C-40/17)

EU-Domstolen fastslog i [C-40/17 \(Fashion ID\)](#), at en hjemmesideoperatør, der integrerer Facebooks "synes godt om"-knap, er **fælles dataansvarlig** med Facebook for indsamling og transmission af besøgendes personoplysninger. Ansvarer er begrænset til de operationer, operatøren har reel indflydelse på (indsamling og overførsel), men omfatter ikke Facebooks efterfølgende behandling.

Domstolen fastslog tre centrale pligter for hjemmesideoperatøren:

- **Samtykke** skal indhentes af operatøren inden overførslen
- **Oplysningspligten** påhviler operatøren for indsamlingsfasen
- Både operatørens og plugin-udbyderens **legitime interesse** skal vurderes for behandlingen

DMI-sagen (Datatilsynet)

I afgørelsen om [DMI](#) (j.nr. 2018-32-0357) anvendte Datatilsynet Fashion ID-principperne og fastslog, at DMI og Google er fælles dataansvarlige for indsamling og videregivelse af personoplysninger via

Google-annonce-tags på dmi.dk. Da DMI er en offentlig myndighed, kan [GDPR artikel 6, stk. 1, litra f](#) (legitim interesse) ikke påberåbes, og samtykke er dermed det eneste mulige behandlingsgrundlag.

JP/Politikens eb.dk-sagen

I tilsynet med [JP/Politikens Hus](#) indskærpede Datatilsynet, at fælles dataansvar efter [GDPR artikel 26](#) kræver en klar aftale mellem parterne om deres respektive ansvar, og at væsentlige dele heraf skal gøres tilgængelige for de registrerede.

LOV	Databeskyttelsesforordningen (GDPR) § 6, stk. 1	Databeskyttelsesforordningen (GDPR) § 26
PRAKSIS	EU-Domstolen · Websideoperatørers ansvar ved brug af sociale plugins: Fælles dataansvar og forbrugerorganisationers søgsmålskompetence (Fashion ID-sagen)	29.07.2019
	Datatilsynet · Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	27.10.2022
	Datatilsynet · Alvorlig kritik af DMI's behandling af personoplysninger om besøgende på dmi.dk	11.02.2020

§ 7 IAB Europe TCF: samtykkestrengere som personoplysninger

EU-Domstolens dom i [C-604/22 \(IAB Europe\)](#) af 7. marts 2024 har vidtrækkende konsekvenser for den digitale annonceindustri og de danske medier, der bruger IAB Europes Transparency & Consent Framework (TCF) til at håndtere cookie-samtykke.

TCF er en branchestandard, der koder brugernes samtykkepræferencer i en **TC String** – en bogstav- og tegnække, som deles med datamæglere og reklameplatforme i forbindelse med Real-Time Bidding (RTB). Samtykkeplatforme (CMP'er) placerer en cookie (*eukonsent-v2*) på brugerens enhed, der kobler TC String til IP-adressen.

TC String er en personoplysning. Domstolen fastslog, at en TC String udgør en personoplysning efter [GDPR artikel 4, nr. 1](#), fordi den ved rimelige midler kan forbindes med en IP-adresse, som gør det muligt at identificere den registrerede. Det er irrelevant, at IAB Europe ikke selv kan foretage koblingen – medlemmerne har adgang til identifikatorerne.

IAB Europe er fælles dataansvarlig. Brancheorganisationen fastsætter de bindende tekniske og kontraktlige regler for, hvordan samtykke indsamles, kodes og distribueres. Da overholdelse af TCF er en betingelse for medlemskab, og IAB Europe har et eget formål med databehandlingen (fremme af reklamemarkedet), er organisationen fælles dataansvarlig med sine medlemmer for *registreringen* af brugerpræferencer. Ansvar et strækker sig dog ikke automatisk til tredjeparters efterfølgende målrettede annoncering.

Dommen har direkte betydning for danske medier og annoncører, der anvender TCF-baserede samtykkeløsninger (herunder CMP'er som OneTrust, Cookiebot og Quantcast Choice), da TCF-infrastrukturen nu indebærer fælles dataansvar med IAB Europe.

LOV	Databeskyttelsesforordningen (GDPR) § 4	Databeskyttelsesforordningen (GDPR) § 26
PRAKSIS	EU-Domstolen · Klassificering af samtykkestrengere som personoplysninger og brancheorganisationers status som fælles dataansvarlige under GDPR	07.03.2024

§ 8 Offentlige myndigheders særlige pligter ved cookies

Offentlige myndigheder er underlagt skærpede krav ved brug af cookies. Datatilsynets DMI-afgørelse (- [2018-32-0357](#)) fastslog, at offentlige myndigheder **ikke kan påberåbe sig legitim interesse** (GDPR artikel 6, stk. 1, litra f) som behandlingsgrundlag for personoplysninger indsamlet via cookies. Da DMI's vejrtjeneste let kunne drives uden persondatasporing, kunne heller ikke offentlig opgave/samfundsinteresse (litra e) begrunde behandlingen. Samtykke er dermed det eneste mulige grundlag.

Regulatorisk er området yderligere skærpet af [Vejledning om brug af tredjepartcookies på statslige, obligatoriske digitale selvbetjeningsløsninger](#) fra 2022. Vejledningen fastsætter krav om, at tredjeparter ikke må indsamle oplysninger om borgere på obligatoriske selvbetjeningsløsninger og nationale portaler til egne formål. Formålet er at styrke borgernes tillid til den offentlige sektors datahåndtering.

Dette indebærer, at offentlige myndigheder bør undgå tredjepartcookies til statistik og markedsføring på deres hjemmesider, medmindre de kan sikre et gyldigt samtykke, der opfylder alle GDPR-krav. Alternativer som serverside-analyse uden cookies bør foretrækkes.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 6, stk. 1](#)

PRAKSIS

Datatilsynet · Alvorlig kritik af DMI's behandling af personoplysninger om besøgende på dmi.dk

11.02.2020

§ 9 Vildledende samtykkeflows: Forbrugerombudsmandens og Datatilsynets parallelle håndhævelse

Cookies og samtykke reguleres ikke kun af Datatilsynet – Forbrugerombudsmanden har en selvstændig håndhævelsesrolle efter markedsføringsloven, og de to myndigheders praksis understøtter hinanden.

I sagen om et forsikringsselskab ([fom-100407](#)) indskærpede Forbrugerombudsmanden, at et samtykkeflow, der viste en advarsel om "manglende optimal rådgivning" ved afslag på markedsføringssamtykke, var **vildledende og aggressivt**. Flowet var i strid med [markedsføringslovens §§ 5-7](#), og samtykker indhentet på denne måde var ugyldige.

Forbrugerombudsmandens elhandelsvirksomhed-sag ([fom-80111](#)) fastslog, at accept af 54 ikke-nødvendige cookies som betingelse for kontoadgang er i strid med god skik. Virksomheder har pligt til at give forbrugere adgang til nødvendige oplysninger "uden at forbrugere skal betale for det, hverken i form af penge eller data."

Denne parallelle håndhævelse understreger, at cookies og samtykke ikke alene er et databeskyttelsesretligt spørgsmål, men også et forbrugerretligt. Virksomheder, der designer vildledende samtykkeflows, risikerer sanktioner fra begge myndigheder.

LOV

[Markedsføringsloven § 3](#)[Markedsføringsloven § 5](#)

PRAKSIS

Forbrugerombudsmanden · Vildledende samtykkeflow: Forsikringsselskab indskræpes for aggressiv markedsføringspraksis

19.02.2024

Forbrugerombudsmanden · Elhandelsvirksomhed krævede accept af unødvendige cookies for adgang til kundekonto: Tilsidesættelse af god skik

18.01.2022

§ 10 Sammenfatning: den samlede retsstilling i 2024-2026

Praksis fra Datatilsynet, EU-Domstolen og Forbrugerombudsmanden tegner nu et klart billede af kravene til cookie-samtykke i Danmark:

Samtykkeindhentning:

- Samtykke skal gives ved en aktiv handling – forudafkrydsede felter, inaktivitet og "gå videre"-samtykke er ugyldige
- Cookies må ikke placeres før samtykke er givet
- Alle behandlingsformål skal oplyses i første lag
- Brugeren skal let og i ét klik kunne afvise ikke-nødvendige cookies
- Farver, størrelser og visuelt design må ikke nudge brugeren mod accept

Cookie walls og pay-or-track:

- En ren cookie wall uden alternativ er som udgangspunkt ulovlig
- Pay-or-track kan være lovligt, hvis betalingsalternativet giver i vidt omfang tilsvarende indhold og prisen ikke er urimelig
- Statistik-samtykke skal kunne gives særskilt eller dokumenteres som nødvendigt

Fælles dataansvar:

- Hjemmesideoperatøren er medansvarlig for indsamling og transmission via tredjepartcookies og sociale plugins
- IAB Europas TCF-samtykkestreng er en personoplysning, og IAB Europe er fælles dataansvarlig
- En klar aftale om ansvarsfordeling efter GDPR artikel 26 er påkrævet

Sanktioner:

- Datatilsynet har hidtil primært reageret med kritik (herunder alvorlig kritik) og påbud
- Manglende efterlevelse af påbud kan straffes med bøde eller fængsel i op til 6 måneder
- Overtrædelse af cookiebekendtgørelsens § 3 kan straffes med bøde, jf. § 5
- Forbrugerombudsmanden kan indskærpe og politianmelde efter markedsføringsloven

Et kommende ePrivacy-forordning (der har været under forhandling i EU siden 2017) vil potentielt erstatte ePrivacy-direktivet og den danske cookiebekendtgørelse, men indtil da hviler den danske retsstilling på det beskrevne samspil mellem cookiebekendtgørelsen, GDPR og den nationale og EU-retlige praksis.

LOV

[Cookiebekendtgørelsen § 3](#)
[Cookiebekendtgørelsen § 5](#)
[Databeskyttelsesforordningen \(GDPR\) § 26](#)

PRAKSIS	EU-Domstolen · Klassificering af samtykkestrengs som personoplysninger og brancheorganisationers status som fælles dataansvarlige under GDPR	07.03.2024
	EU-Domstolen · Krav om aktivt samtykke til cookies og rækkevidden af oplysningspligten (Planet49-sagen)	01.10.2019
	EU-Domstolen · Websideoperatørers ansvar ved brug af sociale plugins: Fælles dataansvar og forbrugerorganisationers søgsmålskompetence (Fashion ID-sagen)	29.07.2019
	Datatilsynet · Ugyldigt samtykke ved brug af "cookie walls" hos Berlingske Media	14.02.2024
	Datatilsynet · Lovligheden af "Pay-or-track"-model hos Gul og Gratis	08.02.2023
	Datatilsynet · Lovligheden af cookie walls: Datatilsynets afgørelse i sagen om Jysk Fynske Medier	08.02.2023

Datatilsynet · Alvorlig kritik af Leadwise ApS for utilstrækkeligt samtykke til markedsføring på letfinans.dk	23.12.2022
Datatilsynet · Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	27.10.2022
Datatilsynet · Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies	20.10.2021
Datatilsynet · Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	13.11.2020
Datatilsynet · Alvorlig kritik af DMI's behandling af personoplysninger om besøgende på dmi.dk	11.02.2020

REFERENCE Lovgrundlag

6 paragraffer

Cookiebekendtgørelsen § 3 stk. 1	Cookiebekendtgørelsen § 4 stk. 1
Databeskyttelsesforordningen (GDPR) § 4	Databeskyttelsesforordningen (GDPR) § 5 stk. 1
Databeskyttelsesforordningen (GDPR) § 6 stk. 1	Databeskyttelsesforordningen (GDPR) § 7 stk. 4

MATERIALE Citerede afgørelser

14 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		4
07.03.2024	Klassificering af samtykkestrengs som personoplysninger og brancheorganisationers status som fælles dataansvarlige under GDPR	C-604/22
04.07.2023	Konkurrencemyndighedens adgang til at efterprøve databeskyttelsesregler og kravene til lovlig behandling af personoplysninger på sociale netværk	C-252/21
01.10.2019	Krav om aktivt samtykke til cookies og rækkevidden af oplysningspligten (Planet49-sagen)	C-673/17
29.07.2019	Websideoperatørers ansvar ved brug af sociale plugins: Fælles dataansvar og forbrugerorganisationers søgsmålskompetence (Fashion ID-sagen)	C-40/17
DATATILSYNET · NÆVN / KLAGEINSTANS		8
14.02.2024	Ugyldigt samtykke ved brug af "cookie walls" hos Berlingske Media	2023-431-0010
08.02.2023	Lovligheden af "Pay-or-track"-model hos Gul og Gratis	2021-31-4871
08.02.2023	Lovligheden af cookie walls: Datatilsynets afgørelse i sagen om Jysk Fynske Medier	2021-31-5553
23.12.2022	Alvorlig kritik af Leadwise ApS for utilstrækkeligt samtykke til markedsføring på letfinans.dk	2021-31-5282
27.10.2022	Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	2021-41-0149
20.10.2021	Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies	2021-431-0125

13.11.2020	Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	2020-31-3354
------------	--	--------------

11.02.2020	Alvorlig kritik af DMI's behandling af personoplysninger om besøgende på dmi.dk	2018-32-0357
------------	---	--------------

FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS	2
---	---

19.02.2024	Vildledende samtykkeflow: Forsikringsselskab indskærpes for aggressiv markedsføringspraksis	
------------	---	--

18.01.2022	Elhandelsvirksomhed krævede accept af unødvendige cookies for adgang til kundekonto: Tilsidesættelse af god skik	
------------	--	--

04

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over databedrageri (§ 279 a) – doktrin og afgrænsning

Doktrin, gerningsindhold og afgrænsning til klassisk bedrageri og hacking

Version 2 · Opdateret 24. jun. 2026 · 7 afgørelser · 2013-2026

[Læs online](#)

INTRODUKTION

Straffelovens § 279 a om databedrageri kriminaliserer retsstridigt indgreb i elektronisk databehandling med vindings hensigt – en bestemmelse indført i 1985 for at ramme bedragerilignende handlinger, hvor ingen fysisk person er blevet vildledt, men hvor en datamaskins resultat påvirkes retsstridigt. Bestemmelsen adskiller sig fra det klassiske bedrageri i § 279 ved, at kravet om menneskelig vildfarelse erstattes af et krav om påvirkning af en automatisk databehandling. I praksis anvendes § 279 a navnlig ved organiserede telefonsvindel-modeller ("callcenter-bedrageri"), misbrug af andres digitale login til netbanker og låneudbydere samt manipulation af betalingsterminaler. Ved særlig grov beskaffenhed – typisk professionel organisering, mange forurettede eller store beløb – henføres forholdet under § 286, stk. 2, med strafferamme op til 8 års fængsel.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Databedrageri efter § 279 a kræver ikke, at en fysisk person er blevet vildledt; det er tilstrækkeligt, at gerningsmanden retsstridigt har påvirket resultatet af en automatisk databehandling.
- 02 Den afgørende forskel mellem § 279 (bedrageri) og § 279 a (databedrageri) er, at § 279 forudsætter en handlingsbestemmende vildfarelse hos en person, mens § 279 a erstatter dette krav med et indgreb i den elektroniske databehandling.
- 03 Bestemmelsens gerningsindhold rummer to led: (1) retsstridigt at ændre, tilføje eller slette oplysninger eller programmer til elektronisk databehandling, eller (2) i øvrigt retsstridigt at søge at påvirke resultatet af sådan databehandling.
- 04 Vindingsforsæt er et krav – gerningsmanden skal handle for derigennem at skaffe sig eller andre uberettiget vinding. Uden berigelsesforsæt henføres forholdet under andre bestemmelser, fx § 263 a om ulovlig adgang til datasystemer.
- 05 Bestemmelsens andet led ('i øvrigt retsstridigt søger at påvirke') er en opsamlingsbestemmelse, der bl.a. dækker tilfælde, hvor gerningsmanden ændrer oplysninger bestemt til senere indtastning af en underordnet medarbejder, som ikke udøver reel prøvelse.

- 06** § 279 a er fuldbyrdet allerede ved den retstridige påvirkning af databehandlingen med vindingsforsæt – der kræves ikke, at vinding faktisk er opnået (forsøg er selvstændigt strafbart efter § 21).
- 07** Databedrageri af særlig grov beskaffenhed henføres under § 286, stk. 2, med strafferamme op til 8 års fængsel, navnlig ved professionel organisering, mange forurettede eller store beløb.
- 08** Databedrageri og bedrageri kan begge foreligge i samme sagskompleks – fx hvor forurettede narres til at udlevere login-oplysninger (bedrageri) og oplysningerne derefter bruges til uberettigede digitale transaktioner (databedrageri).
- 09** § 279 a finder anvendelse ved brug af andres digitale identifikationsmidler (NemID/MitID) til at oprette lån eller overføre midler online, da indtastningen påvirker resultatet af kreditinstituttets automatiske databehandling.
- 10** Misbrug af betalingsterminaers offline-funktion til at gennemføre transaktioner med stjålne eller spærrede kort er databedrageri, idet gerningsmanden retsstridigt tilføjer data til betalingssystemets elektroniske databehandling.

§ 1 Lovgrundlaget: § 279 a og dens tilblivelse

Bestemmelsen om databedrageri i [straffelovens § 279 a](#) lyder:

For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling.

Bestemmelsen blev indført ved **lov nr. 229 af 6. juni 1985** og byggede på [Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet](#). Straffelovrådet konstaterede, at den klassiske bedrageribestemmelse i [§ 279](#) ikke var anvendelig i situationer, hvor en forretningsmæssig arbejdsgang var så automatiseret, at der ikke i forløbet optrådte en enkeltperson, der handlede på grundlag af urigtige dataoplysninger. Rådet foreslog derfor en ny selvstændig bestemmelse, som indholdsmæssigt har tilknytning til § 279, men fraviger kravet om menneskelig vildfarelse:

"Den vigtigste forskel mellem de to bestemmelser er, at § 279 a fraviger kravet i § 279 om, at en person som følge af gerningsmandens forhold skal være blevet vildledt til at foretage en disposition. I stedet for denne vildledelse træder ved databedrageri et indgreb i grundlaget for den elektroniske databehandling."

– [Betænkning nr. 1032/1985, s. 79](#)

Normalstrafferammen for databedrageri er den samme som for bedrageri, dvs. fængsel indtil 1 år og 6 måneder, jf. [§ 285](#). For forhold af særlig grov beskaffenhed gælder [§ 286, stk. 2](#), der hæver strafferammen til fængsel indtil 8 år. For forhold af mindre strafværdighed kan § 279 a straffes med bøde efter [§ 287, stk. 1](#). Der er ingen vedtagne, men endnu ikke konsoliderede ændringer af § 279 a pr. juni 2026.

LOV

[Straffeloven § 279a](#)

[Straffeloven § 279](#)

[Straffeloven § 286, stk. 2](#)

[Straffeloven § 287, stk. 1](#)

§ 2 Gerningsindholdet: de to led i § 279 a

Bestemmelsen har to led, som tilsammen dækker et bredt spektrum af indgreb i elektronisk databehandling.

Første led – direkte indgreb i data eller programmer:

Gerningsmanden retsstridigt *ændrer, tilføjer eller sletter* oplysninger eller programmer til elektronisk databehandling. Straffelovrådet fremhævede i [betænkning nr. 1032/1985, s. 80](#), at det er uden betydning, *hvorledes* indgrebet foretages – det kan ske ved brug af en terminal, men også ved fysisk ødelæggelse af et magnetbånd, der indgår i en databehandling. Det er berigelsesforsættet, der i sidstnævnte tilfælde adskiller forholdet fra tingsødelæggelse efter § 291.

Andet led – opsamlingsbestemmelsen:

Gerningsmanden "i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling". Dette led rammer bl.a. tilfælde, hvor gerningsmanden ikke selv griber direkte ind i den elektroniske databehandling, men ændrer de oplysninger, som en person – typisk en underordnet medarbejder – senere skal indtaste. Straffelovrådet bemærkede, at den pågældende person i visse situationer ikke kan siges at udøve nogen reel prøvelse af oplysningernes rigtighed og derfor ikke bliver bragt i "bestemmende vildfarelse" som krævet i § 279. Forholdet har da en betydelig lighed med det i bestemmelsens første led omtalte direkte indgreb.

Vindingsforsæt:

Begge led forudsætter, at gerningsmanden handler "for derigennem at skaffe sig eller andre uberettiget vinding". Uden berigelsesforsæt – dvs. hvor indgrebet alene har til formål at ødelægge, genere eller skaffe sig information – henføres forholdet under andre bestemmelser som [§ 263, stk. 1](#) (hacking), [§ 263 a](#) (ulovlig adgang til datasystem) eller [§ 193](#) (forstyrrelse af driften af samfundsvigtige datasystemer).

Bestemmelsen er et forsøgsdelikt i den forstand, at det allerede er strafbart at "søge" at påvirke resultatet – det kræves ikke, at vinding faktisk er opnået. Ufuldbyrdet forsøg er herudover strafbart efter [§ 21](#).

LOV

[Straffeloven § 193](#)[Straffeloven § 263, stk. 1](#)[Straffeloven § 263a](#)[Straffeloven § 279a](#)

§ 3 Afgrænsningen til klassisk bedrageri (§ 279) og andre formueforbrydelser

Den principielle afgrænsning mellem databedrageri og bedrageri beror på, om den tabsvoldende disposition fremkommer ved en *menneskelig vildfarelse* (§ 279) eller ved *påvirkning af en automatisk databehandling* (§ 279 a).

§ 279 – klassisk bedrageri:

Kræver at gerningsmanden retsstridigt fremkalder, bestyrker eller udnytter en *vildfarelse* hos en person, som derved bestemmes til en handling eller undladelse, der medfører et formuetab. Hvis en person handler ud fra urigtige dataoplysninger og har en reel prøvelsesadgang, foreligger der bedrageri.

§ 279 a – databedrageri:

Kræver *ikke* menneskelig vildfarelse. Bestemmelsen anvendes, hvor beløb krediteres eller debiteres en person

ved indtastning i et dataanlæg uden yderligere mellemkommende handlinger, der opfylder § 279's krav om, at nogen er blevet vildledt. Som [betænkning nr. 1581/2023 om strafudmåling, s. 236](#) sammenfatter:

"Straffelovens § 279 om bedrageri ikke omfatter tilfælde, hvor en forretningsmæssig arbejdsgang er så automatiseret, at der ikke i forløbet optræder en enkeltperson, der handler på grundlag af de urigtige dataoplysninger."

I praksis forekommer begge bestemmelser ofte i sammenstød. I sager om telefonsvindel mod ældre foreligger der typisk bedrageri, når forurettede narres til at udlevere kortoplysninger (vildfarelse), og databedrageri, når oplysningerne derefter bruges til automatiserede betalinger. Retten i Aarhus præciserede i [SS-10613/2022-ARH](#):

"Forholdene alene skulle henføres under straffelovens § 279 a om databedrageri (og ikke § 279 om bedrageri), idet den tabsvoldende disposition – overførsel eller køb – først skete ved en automatiseret handling, efter at de personlige oplysninger var indtastet retsstridigt."

Afgrænsning til § 301:

[Straffelovens § 301](#) kriminaliserer med forsæt til uberettiget anvendelse at fremstille, skaffe sig, besidde eller videregive oplysninger, der identificerer et betalingsmiddel. Bestemmelsen rammer således *besiddelsen* af betalingsoplysninger, mens § 279 a rammer den faktiske *brug* heraf til at påvirke en databehandling. For en nærmere behandling af betalings-app-misbrug, se [praksisoversigten om MobilePay og betalingstjenestesvindel](#).

Afgrænsning til § 263 a og hacking:

[Straffelovens § 263 a](#) kriminaliserer erhvervmæssig udbredelse eller videregivelse af adgangsmidler til datasystemer. Bestemmelsen rammer den *uberettigede adgang* til systemet, mens § 279 a rammer den *berigelsesmotiverede påvirkning* af systemets resultat. For nærmere om hacking og uberettiget systemadgang, se [praksisoversigten herom](#).

LOV

[Straffeloven § 263a](#)[Straffeloven § 279](#)[Straffeloven § 279a](#)[Straffeloven § 301](#)

PRAKSIS

Byretten · Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe

15.12.2023

§ 4 Typiske gerningsformer i retspraksis

Retspraksis illustrerer en række karakteristiske gerningsformer, der henføres under § 279 a:

- **Organiseret telefonsvindel ("callcenter-bedrageri"):** Gerningsmænd ringer systematisk til typisk ældre personer, udgiver sig for bank, Nets eller politi, og franarrer dem NemID-oplysninger, kortdata eller pinkoder. Oplysningerne bruges straks til at foretage overførsler eller køb. Denne model blev eksempelvis anvendt i [SS-10613/2022-ARH](#), hvor 436 opkald til ældre forurettede medførte et samlet tab/risiko på ca. 15 mio. kr.
- **Misbrug af NemID/MitID til lånoptagelse:** Gerningsmanden anvender forurettedes digitale login til at ansøge om lån hos online-kreditinstitutter. Låneprovenuene overføres til forurettedes konto og videreføres til gerningsmanden. I [SS-5306/2018-VIB](#) optog tiltalte fire lån på samlet 29.500 kr. via forurettedes NemID og overførte yderligere 47.108 kr. fra dennes konto. En detaljeret behandling af NemID/MitID-specifikke forhold findes i [praksisoversigten om MitID/NemID-misbrug](#).
- **Misbrug af betalingsterminalers offline-funktion:** Gerningsmænd opretter fiktive virksomheder, anskaffer dankortterminaler og gennemfører transaktioner med stjålne eller spærrede kort i offline-tilstand, hvor bankens autorisationstjek omgås. Beløbene overføres straks videre. I [SS-962/2013-ALB](#) blev fire mænd dømt

for databedrageri i millionklassen via denne metode, herunder forsøg på at hvidvaske provenuet gennem guldkøb.

- **Identitetsudnyttelse og fiktive konti:** En systemoperatør opretter fiktive konti for ikke-eksisterende personer (leverandører, lønmodtagere, pensionister) og opnår udbetaling via konti, som vedkommende selv eller andre råder over. Denne form – der var central i Straffelovrådets overvejelser i 1985 – er fortsat relevant i moderne sagskomplekser.
- **Fysisk opsøgende bedrageri kombineret med digitale transaktioner:** Gerningsmænd opsøger ældre på bopælen under påskud af at være fra banken og franarrer dem betalingskort med pinkode. Kortene bruges derefter til hævnninger i automater. I [S-1703-25](#) (Vestre Landsret 2026) blev ni ældre ofre i alderen 68-93 år udsat for denne metode med et samlet tab på ca. 170.000 kr.

For phishing- og smishing-specifikke forhold, se [praksisoversigten om SMS-phishing/smishing](#).

LOV	Straffeloven § 279a	Straffeloven § 286, stk. 2	
PRAKSIS	Landsretten · Systematisk bankudgiver-bedrageri mod 9 ældre ofre: 9 måneders betinget fængsel med psykiatrisk behandling (Vestre Landsret 2026)		18.02.2026
	Byretten · Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe		15.12.2023
	Byretten · Databedrageri og udvisning - Strafferetlig dom mod udenlandsk statsborger		15.01.2020
	Byretten · Omfattende svindel med betalingskort og fiktive virksomheder: Fire mænd dømt for databedrageri i millionklassen		21.05.2013

§ 5 Strafudmåling og skærpelesmomenter

Strafudmålingen i databedrageri-sager følger de samme principper som for de øvrige formueforbrydelser, og [Rigsadvokatmeddelelsen om formueforbrydelser](#) anfører, at forbrydelser efter §§ 278-280 og 283 (herunder § 279 a) af særlig grov beskaffenhed henføres under [§ 286, stk. 2](#) med strafferamme op til 8 år:

"Disse forbrydelser vil navnlig være af særlig grov beskaffenhed på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i forening, eller som følge af omfanget af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået."

For mindre strafværdige forhold (§ 287) gælder en værdigrænse på ca. 8.000 kr., og straffen er bøde.

Praksis viser følgende strafniveauer ved groft databedrageri:

Sag	Instans	Tab/risiko	Straf	Skærpelesfaktorer
SS-10613/2022-ARH	Byretten	~15 mio. kr.	5½-6 års fængsel	Organiseret callcenter, 436 opkald, sårbare ofre
S-1149-22	Landsretten	~6,3 mio. kr.	3 års fængsel	8 års systematik, 112 forhold, gentagelse
SS-962/2013-ALB	Byretten	~4,5 mio. kr.	1½-3 års fængsel	Fiktive virksomheder, offline-terminaler, guldhandel
S-1703-25	Landsretten	~170.000 kr.	9 mdr. betinget	Psykiatrisk lidelse, tilståelse, 25% rabat
SS-5306/2018-VIB	Byretten	~77.000 kr.	60 dages fængsel	20 forhold, tilståelse

De strengeste straffe ses ved professionelt organiseret kriminalitet med mange sårbare ofre og store beløb. Callcenter-modellen med systematisk svigtende tillid til det digitale betalingssystem har medført straffe i niveauet 5-6 års fængsel, hvilket retten i Aarhus bl.a. begrundede med at kriminaliteten var "samfundsundergravende, idet den svækkede tilliden til digitale betalingsløsninger".

LOV	Straffeloven § 286, stk. 2	Straffeloven § 287, stk. 1	
PRAKSIS	Landsretten · Systematisk bankudgiver-bedrageri mod 9 ældre ofre: 9 måneders betinget fængsel med psykiatrisk behandling (Vestre Landsret 2026)		18.02.2026
	Landsretten · Stadfæstelse af 3 års ubetinget fængsel for systematisk bedrageri, databedrageri og dokumentfalsk for over 6,3 mio. kr.		16.05.2023
	Byretten · Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe		15.12.2023
	Byretten · Databedrageri og udvisning - Strafferetlig dom mod udenlandsk statsborger		15.01.2020
	Byretten · Omfattende svindel med betalingskort og fiktive virksomheder: Fire mænd dømt for databedrageri i millionklassen		21.05.2013

§ 6 Højesterets praksis: Hvepsebo-sagen om menneskehandel og databedrageri

Den mest principielle Højesteretsdom, der involverer § 279 a, er sag 70/2017 – den såkaldte "Hvepsebo-sag" – afgjort den 29. maj 2017. [Sag 70/2017](#) vedrørte tre rumænske søskende, der i perioden 2012-2015 systematisk rekrutterede fattige rumænske statsborgere, fik dem registreret med CPR-nummer, NemID og bankkonti i Danmark og udnyttede deres identitet til at optage lån og foretage internetkøb.

De tiltalte blev dømt for menneskehandel efter [§ 262 a](#) og for databedrageri efter § 279 a med straffe på 3-3½ års fængsel samt udvisning for bestandig. Det samlede tab af bedrageri og databedrageri androg ca. 900.000 kr.

Højesteret fastslog et principielt punkt om menneskehandelsparagraffens rækkevidde, men sagen illustrerer også en vigtig doktrinær pointe om databedrageri: identitetsmisbruget bestod i, at de tiltalte *ikke selv* foretog transaktionerne direkte, men udnyttede ofrenes digitale legitimation til at igangsætte automatiserede processer hos kreditinstitutter. Det er netop den type handlinger – retsstridigt at tilføje oplysninger i et dataanlæg (her: kreditansøgninger med andres identitet), hvorved kreditinstitutternes automatiske systemer afgav lån – som § 279 a blev indført for at ramme.

LOV	Straffeloven § 262a, stk. 1	Straffeloven § 279a	
PRAKSIS	Højesteret · Højesteret stadfæster dom for organiseret menneskehandel og databedrageri: Udnyttelse af identitet kræver ikke kendskab fra ofret		29.05.2017

§ 7 Doktrinær indplacering: Straffelovrådets betænkning nr. 1032/1985 og betænkning nr. 1581/2023

To betænkninger er centrale for forståelsen af § 279 a's doktrinære fundament.

Betænkning nr. 1032/1985 om datakriminalitet

[Straffelovrådets betænkning nr. 1032/1985](#) er den grundlæggende kilde til § 279 a's formål og rækkevidde. Rådet analyserede straffelovens daværende bestemmelser om bedrageri, underslæb og mandatsvig i forhold til den fremvoksende datakriminalitet og konstaterede tre centrale huller:

1. [§ 279](#) (bedrageri) var uanvendelig, hvor ingen fysisk person var vildledt, fordi den automatiserede arbejdsgang gjorde menneskelig prøvelse overflødig.
2. [§ 278](#) (underslæb) krævede, at pengene var "betroe", hvilket sjældent var tilfældet.
3. [§ 280](#) (mandatsvig) var ikke udformet med datakriminalitet for øje, og det var "mindre naturligt" at henhøre de nye kriminalitetsformer under den.

Rådet fremhævede, at problemet var af *international* karakter – tilsvarende lovændringer var under forberedelse i Sverige, Norge og Finland – og foreslog den bestemmelse, der med uændret ordlyd gælder i dag.

Betænkning nr. 1581/2023 om strafudmåling (Bind III)

[Betænkning nr. 1581/2023, s. 235-236](#) gennemgår § 279 a i konteksten af Straffelovrådets aktuelle strafudmålingsovervejelser for formueforbrydelser. Betænkningen sammenfatter lovhistorikken og bekræfter, at bestemmelsens ordlyd og gerningsindhold er uændret siden 1985, men at den har fået fornyet praktisk betydning i takt med digitaliseringen af betalingssystemer og identifikationsløsninger.

LOV

[Straffeloven § 278](#)[Straffeloven § 279a](#)[Straffeloven § 279](#)[Straffeloven § 280](#)

§ 8 Sammenfatning og praksisoverblik

Databedrageri efter [§ 279 a](#) er en central bestemmelse i det moderne strafferetlige værn mod digital formuekriminalitet. Bestemmelsen er uændret siden sin indførelse i 1985, men har fået stadigt større praktisk betydning i takt med digitaliseringen.

De væsentligste takeaways fra praksis er:

- **Afgrænsningsprincippet:** Den tabsvoldende disposition skal bero på en *automatiseret* handling – sker den som følge af menneskelig vildfarelse, anvendes i stedet [§ 279](#). I praksis forekommer begge bestemmelser hyppigt i samme sagskompleks.
- **Strafniveauet:** Ved organiseret databedrageri med professionel infrastruktur (callcentre, fiktive virksomheder) og mange sårbare forurettede ses straffe i niveauet 3-6 års fængsel under [§ 286](#), stk. 2. Enkeltstående forhold med mindre beløb afgøres med korte frihedsstraffe eller bøde.
- **Erstatningsansvar:** Tiltalte dømmes konsekvent til solidarisk erstatning for de forurettedes tab, typisk til pengeinstitutter (Nets, banker) eller direkte til forurettede. Konfiskation af udbytte sker regelmæssigt.
- **Udvisning:** Ved alvorligt databedrageri er udvisning med indrejseforbud en fast bestanddel af sanktionspakken for ikke-danske statsborgere.
- **Beslægtede emner:** Konkrete gerningstyper som [phishing/smishing](#), [MitID/NemID-misbrug](#), [betalings-app-svindel](#) og [hacking](#) behandles i selvstændige praksisoversigter.

Bestemmelsens fortolkningsmæssige kerne – kravet om påvirkning af resultatet af en *automatisk* databehandling, som erstatning for bedrageriets krav om menneskelig vildfarelse – har stået fast siden Straffelovrådets formulering i 1985 og er ikke blevet udfordret doktrinært.

LOV	Straffeloven § 279a	Straffeloven § 286, stk. 2	
PRAKSIS	Højesteret · Højesteret stadfæster dom for organiseret menneskehandel og databedrageri: Udnyttelse af identitet kræver ikke kendskab fra ofret 29.05.2017		
	Landsretten · Systematisk bankudgiver-bedrageri mod 9 ældre ofre: 9 måneders betinget fængsel med psykiatrisk behandling (Vestre Landsret 2026) 18.02.2026		
	Landsretten · Stadfæstelse af 3 års ubetinget fængsel for systematisk bedrageri, databedrageri og dokumentfalsk for over 6,3 mio. kr. 16.05.2023		
	Byretten · Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe 15.12.2023		
	Byretten · Databedrageri og udvisning - Strafferetlig dom mod udenlandsk statsborger 15.01.2020		
	Byretten · Omfattende svindel med betalingskort og fiktive virksomheder: Fire mænd dømt for databedrageri i millionklassen 21.05.2013		

REFERENCE Lovgrundlag

6 paragraffer

Straffeloven § 263a	Straffeloven § 279a
Straffeloven § 279	Straffeloven § 286 stk. 2
Straffeloven § 287 stk. 1	Straffeloven § 301

MATERIALE Citerede afgørelser

7 afgørelser

HØJESTERET · ØVERSTE INSTANS		1
29.05.2017	Højesteret stadfæster dom for organiseret menneskehandel og databedrageri: Udnyttelse af identitet kræver ikke kendskab fra ofret	Sag 70/2017
LANDSRETTEEN · ANKEINSTANS		2
18.02.2026	Systematisk bankudgiver-bedrageri mod 9 ældre ofre: 9 måneders betinget fængsel med psykiatrisk behandling (Vestre Landsret 2026)	S-1703-25
16.05.2023	Stadfæstelse af 3 års ubetinget fængsel for systematisk bedrageri, databedrageri og dokumentfalsk for over 6,3 mio. kr.	S-1149-22
BYRETTEEN · FØRSTE INSTANS		4
15.12.2023	Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe	6497-7797
15.01.2020	Databedrageri og udvisning - Strafferetlig dom mod udenlandsk statsborger	1067-1287
21.05.2013	Omfattende svindel med betalingskort og fiktive virksomheder: Fire mænd dømt for databedrageri i millionklassen	6689-8035
25.04.2013	Omfattende sag om systematisk databedrageri via betalingsterminaler og hvidvask gennem guldhandel	6689-8033

FORARBEJDE Betænkninger

2 referencer

Straffelovrådets betænkning om datakriminalitet

nr. 1032 · 1985 · Justitsministeriet

Betænkning om strafudmåling – Bind III

nr. 1581 · 2023 · Justitsministeriet

05

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over Datatilsynets afgørelser

Kritik, påbud og bødeindstilling efter GDPR art. 58 og databeskyttelseslovens § 41

Version 2 Opdateret 16. jul. 2026 86 afgørelser · 2019-2026

[Læs online](#)

INTRODUKTION

Datatilsynet udøver sine beføjelser efter databeskyttelsesforordningens artikel 58 og råder over en gradueret sanktionstrappe fra ingen kritik over kritik og alvorlig kritik til påbud, forbud og – i de groveste sager – politianmeldelse med indstilling til bøde. Danmark har som en af få medlemsstater valgt en strafferetlig sanktionsmodel, hvor bøder ikke pålægges administrativt af tilsynet, men udmåles af domstolene efter databeskyttelseslovens § 41, jf. forordningens artikel 83, stk. 2. Praksis viser, at manglende sletning og utilstrækkelig behandlingssikkerhed er de to dominerende bødegrunde, mens kritik og påbud typisk retter sig mod behandlingsgrundlag, risikovurdering og de registreredes rettigheder. Med EU-Domstolens dom i C-383/23 og Vestre Landsrets efterfølgende dom er bødeloftet nu forankret i hele koncernens samlede omsætning.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Datatilsynet kan ikke selv pålægge bøder til private – Danmark har valgt en strafferetlig sanktionsmodel, hvor tilsynet politianmelder og indstiller til bøde, og domstolene udmåler straffen efter databeskyttelseslovens § 41.
- 02 Sanktionstrappen er gradueret: ingen kritik → kritik → alvorlig kritik → påbud med frist → politianmeldelse. Alvorlig kritik reserveres til overtrædelser af grundlæggende principper eller sager med mange berørte registrerede.
- 03 Den dataansvarlige skal kunne påvise en konkret hjemmel – det er ikke tilstrækkeligt at henvise generelt til gældende lovgivning eller til at behandlingen er "nødvendig".
- 04 En dataansvarlig bør som altovervejende udgangspunkt ikke skifte behandlingsgrundlag efter behandlingen er påbegyndt, og skift væk fra samtykke er særligt problematisk, fordi samtykket giver den registrerede et reelt valg.
- 05 Samtykke skal være frivilligt, granulært og udtryk for en aktiv handling – fortsat brug af en hjemmeside, tavshed eller forudafkrydsede felter udgør ikke samtykke.
- 06 Manglende systemteknisk understøttelse fritager ikke for opbevaringsbegrænsningen – tekniske begrænsninger hos leverandøren kan ikke retfærdiggøre en flerårig tilsidesættelse af slettepligten.

-
- 07** En slettepolitik på papiret er ikke nok; den dataansvarlige skal kunne dokumentere, at sletning rent faktisk sker i de tekniske systemer.
-
- 08** Flerfaktoraumentifikation ved fjernadgang til beskyttelsesværdige oplysninger har længe været et krav – undladelse anses for væsentlig uagtsomhed og udløser rutinemæssigt bødeindstilling.
-
- 09** Kryptering af udtagelige lagringsmedier med personoplysninger anses for en nødvendig og påkrævet sikkerhedsforanstaltning, der er relativt let at gennemføre.
-
- 10** Passende sikkerhed indebærer normalt løbende stikprøvekontrol af logs, hyppig kontrol af adgangsrettigheder og at medarbejdere ikke selv kan installere programmer på enheder med adgang til produktionsdata.
-
- 11** Brud på persondatasikkerheden skal anmeldes inden 72 timer, medmindre det er usandsynligt, at bruddet indebærer en risiko – men alle brud skal dokumenteres internt efter art. 33, stk. 5, uanset anmeldelsespligt.
-
- 12** Uden en risikovurdering kan den dataansvarlige ikke vide, om de implementerede sikkerhedsforanstaltninger er tilstrækkelige – risikovurderingen er en grundlæggende forudsætning for et passende sikkerhedsniveau.
-
- 13** En konsekvensanalyse (DPIA) skal foreligge FØR behandlingen igangsættes; udarbejdelse først efter tilsynets anmodning udløser alvorlig kritik, og analysen skal opfylde mindstekravene i art. 35, stk. 7.
-
- 14** Ved AI-løsninger sondres mellem udvikling og drift: eksisterende opgavehjemler kan bære udviklingsfasen, mens indgribende drift kræver et klarere supplerende nationalt retsgrundlag.
-
- 15** Et databrud beviser ikke i sig selv, at sikkerhedsforanstaltningerne var utilstrækkelige – men bevisbyrden for, at de var passende, påhviler den dataansvarlige (C-340/21).
-
- 16** Bødeloftet efter art. 83 beregnes på grundlag af hele den økonomiske enheds (koncernens) samlede globale årlige omsætning, jf. C-383/23 og Vestre Landsrets dom af 2. september 2025.
-
- 17** Bøder forudsætter skyld – forsæt eller uagtsomhed – men den juridiske person hæfter direkte uden at overtrædelsen skal føres tilbage til en identificeret fysisk person (C-807/21).
-
- 18** Tilsynsmyndigheden har et skøn og er ikke forpligtet til at udøve en korrigerende beføjelse i ethvert tilfælde af konstateret brud (C-768/21).
-
- 19** Ansvarssubjektet i databeskyttelsesretlige straffesager er altid den dataansvarlige eller databehandleren – ikke den enkelte medarbejder, medmindre denne bliver selvstændig dataansvarlig.
-
- 20** Offentlige myndigheder kan straffes uanset straffelovens § 27, stk. 2, når overtrædelsen begås ved udøvelse af virksomhed, der ikke kan sidestilles med privat virksomhed, jf. databeskyttelseslovens § 41, stk. 6.
-

Retsgrundlaget: artikel 58-beføjelserne og den danske strafferetlige sanktionsmodel

§ 1

Datatilsynets myndighedsudøvelse hviler på [databeskyttelsesforordningens artikel 58](#), der tildeler tilsynsmyndigheden tre grupper af beføjelser: undersøgelsesbeføjelser (stk. 1), korrigerende beføjelser (stk. 2) og godkendelses- og rådgivningsbeføjelser (stk. 3).

De korrigerende beføjelser i [artikel 58, stk. 2](#) udgør sanktionstrappens retlige ryggrad:

Litra	Beføjelse	Anvendes i praksis ved
a	Advarsel om planlagte behandlinger	Forudgående høring, sjælden
b	Udtale kritik	Kernen i dansk tilsynspraksis
c	Påbud om at imødekomme registreredes anmodninger	Indsigt, sletning
d	Påbud om at bringe behandling i overensstemmelse	Sikkerheds- og systemmangler
e	Påbud om underretning af registrerede	Databrud med høj risiko
f	Midlertidig eller definitiv begrænsning, herunder forbud	Chromebook-/skysager
g	Påbud om berigtigelse eller sletning	Opbevaringsbegrænsning
i	Administrativ bøde	Ikke anvendt i Danmark
j	Suspension af tredjelandsoverførsel	Kapitel V-sager

Den danske særegenhed ligger i litra i. Efter [artikel 83, stk. 9](#) kan medlemsstater, hvis retssystem ikke kender administrative bøder, i stedet anvende straffesager. Danmark har valgt denne model: Datatilsynet **politianmelder** og **indstiller** til bøde, hvorefter anklagemyndigheden rejser tiltale og domstolene udmåler straffen efter [databeskyttelseslovens § 41](#).

Straffebestemmelsen kriminaliserer bl.a. overtrædelse af de grundlæggende principper i art. 5-7 og 9, de registreredes rettigheder i art. 12-22, den dataansvarliges pligter i art. 25-39 samt tredjelandsoverførsler i art. 44-49, jf. [§ 41, stk. 1](#). Manglende efterkommelse af et påbud er selvstændigt strafbart efter [§ 41, stk. 2, nr. 5](#) – en henvisning Datatilsynet konsekvent indsætter i sine påbudsafgørelser.

Broen til EU-retten slås i [§ 41, stk. 3](#):

Databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålæggelse af straf efter stk. 1 og 2.

Hermed gælder forordningens bødeudmålingskriterier – overtrædelsens karakter, grovhed, varighed, forsæt/uagtsomhed, antal berørte, samarbejdsvilje mv. – direkte i danske straffesager. Offentlige myndigheder kan straffes uanset straffelovens § 27, stk. 2, når overtrædelsen sker ved udøvelse af virksomhed, der ikke kan sidestilles med privat virksomhed, jf. [§ 41, stk. 6](#) – den bestemmelse Datatilsynet påberåber sig i kommune- og regionssagerne. Forældelsesfristen er fem år, jf. [§ 41, stk. 7](#).

Lovens anvendelsesområde afgrænses i [databeskyttelseslovens § 3](#), der bl.a. undtager efterretningstjenesterne, Folketingets parlamentariske arbejde og – for de fleste kapitlers vedkommende – behandling i journalistisk, kunstnerisk eller litterært øjemed. Det forklarer, hvorfor Datatilsynet i sager om politiets straffesagsbehandling

henviser til retshåndhævelsesloven i stedet; se [2018-813-0001](#), hvor tilsynet udtalte kritik af Den Uafhængige Politiklagemyndighed efter retshåndhævelseslovens § 13, men samtidig fastslog, at underretning af anmeldte polititjenestemænd med sigtet lignende rettigheder skal ske efter retsplejelovens regler, som tilsynet ikke fører tilsyn med.

Det dogmatiske fundament er lagt i Justitsministeriets [betænkning nr. 1565/2017 om databeskyttelsesforordningen](#), hvis konklusion på [s. 11](#) er, at forordningen i vidt omfang viderefører retstilstanden efter persondataloven – hvilket er forklaringen på, at Datatilsynets praksis fra før 2018 fortsat har vejledende værdi. Straffelovrådet noterede parallelt i [betænkning nr. 1563/2017](#), at artikel 84 viderefører medlemsstaternes adgang til at fastsætte strafferetlige sanktioner, men at der navnlig ikke bør fastsættes sanktioner for overtrædelser, der er underlagt administrative bøder efter artikel 83.

LOV

[Databeskyttelsesforordningen § 58, stk. 2](#)[Databeskyttelsesforordningen § 83, stk. 9](#)[Databeskyttelsesloven § 3](#)[Databeskyttelsesloven § 41, stk. 1-7](#)

PRAKSIS

Datatilsynet · Kritik af Politiklagemyndighedens håndtering af de registreredes rettigheder ved efterforskning

12.07.2019

§ 2 Sanktionstrappen i praksis: fra "ingen kritik" til politianmeldelse

Datatilsynets afgørelser fordeler sig på en genkendelig trappe, hvor placeringen styres af overtrædelsens karakter, antallet af berørte og oplysningernes følsomhed.

Ingen kritik gives, når tilsynet vurderer, at organisationens "modenhed" svarer til risikoen. I den tværgående spørgeskemaundersøgelse fra 2020 slap både [2020-41-0063](#) (Codan Forsikring), [2020-421-0078](#) (Udviklings- og Forenklingsstyrelsen) og [2020-423-0231](#) (Odense Kommune) for kritik. Karakteristisk er, at tilsynet alligevel udtaler en *bemærkning* om dokumentationssvagheder:

Det er tilsynets umiddelbare vurdering, at Odense Kommune efter omstændighederne vil kunne have svært ved – inden for rimelig tid – at påvise (dokumentere), at personoplysninger i forhold til beredskabsområdet behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, jf. databeskyttelsesforordningens artikel 5, stk. 2, jf. artikel 5, stk. 1, litra f.

Samme mønster ses i [2019-41-0035](#) (DJØF), [2019-421-0029](#) (Ankestyrelsen) og [2021-423-0241](#) (Hedensted Kommune), hvor kommunens konkrete afhjælpning efter konstaterede brud – screeningsgruppe før aktindsigt, indkøb af sløringsværktøj – førte til, at tilsynet fandt sikkerheden passende.

Kritik anvendes ved konstaterede, men mindre graverende overtrædelser. I [2021-31-5737](#) fik en arbejdsgiver kritik for at orientere en bred medarbejderkreds om årsagen til en afskedigelse:

Datatilsynet finder, at en arbejdsgiver skal udvise stor tilbageholdenhed med at videregive oplysninger om årsagen til en medarbejders ophør. Det er tilsynets opfattelse, at en arbejdsgiver som udgangspunkt kun må informere kolleger om, at en medarbejder er fratrådt, og hvem man eventuelt skal rette henvendelse til i stedet.

Alvorlig kritik reserveres til overtrædelser af grundlæggende principper, sager med mange registrerede eller følsomme oplysninger, samt tilfælde hvor den dataansvarlige har handlet mod bedre vidende. Eksempler: [2019-32-0709](#) (Rejsekort – princippet om lovlighed), [2023-423-0004](#) (DPIA tre år for sent) og [2025-431-0053](#) (51 kommuner i Chromebook-sagen).

Et særligt kuriosum er [2020-442-8866](#), hvor Datatilsynet udtalte alvorlig kritik af **sig selv** for manglende behandlingssikkerhed og underretning ved et brud – en påmindelse om, at tilsynet også er dataansvarlig.

Påbud meddeles efter [artikel 58, stk. 2, litra d og g](#) med konkret frist. I [2022-423-0261](#) fik Mariagerfjord Kommune to påbud med forskellige frister – systemliste og sletning inden 15. november 2022, fjernelse af installationsrettigheder allerede inden 15. august 2022.

Politianmeldelse med bødeindstilling er trappens top og forudsætter en konkret grovhedsvurdering efter [artikel 83, stk. 2](#).

EU-Domstolen har bekræftet, at trappen indebærer et **skøn**. I [C-768/21](#) fastslog Domstolen, at tilsynsmyndigheden ikke er forpligtet til at udøve en korrigerende beføjelse i ethvert tilfælde af konstateret brud – hvilket er den EU-retlige forankring af "ingen kritik"-kategorien.

LOV	Databeskyttelsesforordningen § 5, stk. 2	Databeskyttelsesforordningen § 58, stk. 2
	Databeskyttelsesforordningen § 83, stk. 2	
PRAKSIS	EU-Domstolen · Tilsynsmyndigheders skønsebeføjelse ved brud på persondatasikkerheden under GDPR	26.09.2024
	Datatilsynet · Alvorlig kritik af 51 kommuner for manglende beskyttelse af skoleelevers data i Chromebook-sagen	29.01.2026
	Datatilsynet · Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	22.12.2023
	Datatilsynet · Tilsyn med offentlig myndigheds håndtering og anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Kritik af arbejdsgiver for at orientere bredere kreds om baggrund for afskedigelse	19.12.2022
	Datatilsynet · Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	15.07.2022
	Datatilsynet · Ingen kritik af Codan Forsikrings behandlingssikkerhed efter Datatilsynets planlagte tilsyn	15.01.2021
	Datatilsynet · Tilsyn med Udviklings- og Forenklingsstyrelsens behandlingssikkerhed fører ikke til kritik	15.01.2021
	Datatilsynet · Datatilsynets kontrol af informationssikkerhed og risikostyring i Odense Kommune	15.01.2021
	Datatilsynet · Ingen kritik af DJØF efter tilsyn med anmeldelse af brud på persondatasikkerheden	08.12.2020
	Datatilsynet · Ingen kritik af Ankestyrelsens procedurer for anmeldelse af brud på persondatasikkerheden	08.12.2020
	Datatilsynet · Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	03.11.2020
	Datatilsynet · Alvorlig kritik af Datatilsynet for manglende behandlingssikkerhed og underretning ved brud på persondatasikkerheden	11.09.2020

§ 3 Behandlingsgrundlag: kravet om at kunne påvise konkret hjemmel

Det gennemgående krav i Datatilsynets praksis er, at den dataansvarlige skal kunne **pege på en konkret bestemmelse** – ikke blot henvise til lovgivningen i almindelighed.

I det landsdækkende tilsyn med 25 frie grundskoler, [2024-41-0093](#), konstaterede tilsynet, at flere skoler enten ikke præciserede hjemlen eller blot anførte, at behandlingen var "nødvendig". Tilsynet præciserede, at det ikke er tilstrækkeligt at henvise generelt til gældende lovgivning, og at [art. 6, stk. 1, litra c](#) og [litra e](#) altid kræver et

identificeret supplerende retsgrundlag i dansk ret eller EU-ret. Sagerne blev afsluttet uden kritik, men med et generelt vejledningsbehov.

For **offentlige myndigheder** er litra e-sporet det praktisk vigtigste. I [2021-32-2645](#) fandt tilsynet Skatteforvaltningens interne deling mellem Skattestyrelsen og Gældsstyrelsen lovlig, fordi begge styrelser havde national hjemmel (skattekontrolloven og gældsinddrivelsesloven), og formålene var forenelige:

Der er endvidere en betydelig sammenhæng mellem de to forvaltningers opgaver (formål), idet de for begges vedkommende angår statens "provenu". Hertil bemærkes det, at den registrerede – i dette tilfælde klager – med rimelighed bør forvente, at oplysninger om indtægter i form af (kommende) arv holdes op imod oplysninger om gæld til det offentlige.

Samme resultat i [2025-31-1798](#), hvor strækningsbaseret hastighedsmåling på Storebæltsbroen kunne støttes på §§ 3 og 17 i lov om Sund og Bælt Holding A/S, jf. art. 6, stk. 3, jf. art. 6, stk. 1, litra e. Tilsynet lagde vægt på, at målingerne primært tjente trafiksikkerheden, ikke politimæssig håndhævelse, og at videregivelse til politiet ved mistanke om strafbare forhold var dækket af [databeskyttelseslovens § 8, stk. 3-4](#).

Den mest principielle udtalelse er [2023-212-0015](#) om **AI-løsninger**. Datatilsynet sondrede skarpt mellem udvikling og drift:

Kravene til klarheden af det retsgrundlag, som skal danne baggrund for jeres behandling af personoplysninger ved drift af en AI-løsning, afhænger af, hvor indgribende behandlingen er for borgerne. [...] Konsekvenserne for borgerne er dermed ofte større, når AI-løsningen er i drift, og der stilles derfor højere krav til klarheden af det retsgrundlag, der danner baggrund for at anvende løsningen i drift.

Resultatet blev, at serviceloven §§ 86 og 112 var tilstrækkeligt grundlag for **udvikling og gentræning**, men ikke for **drift** af et beslutningsstøtteværktøj rettet mod sårbare borgere. Tilsynet lagde vægt på risikoen for automation bias og på, at AI kan drage konklusioner ud over hvad en menneskelig sagsbehandler kan – og henviste til EU-Domstolens krav om klare og præcise regler i [C-175/20](#) (Valsts ienpēmumu dienests) samt til Justitsministeriets [betænkning nr. 1565/2017](#), hvor det anføres, at nødvendighedskravet i art. 6, stk. 3, kan udledes af den nationale lov med dens forarbejder.

For **private** er interesseafvejningen i [art. 6, stk. 1, litra f](#) hovedsporet, og den kræver en konkret afvejning. To sager illustrerer udfaldsrummet:

- [2021-31-5439](#): DBA's afslag på sletning var berettiget, fordi svindelforebyggelse udgjorde en vægtig legitim grund – men tilsynet **korrigerede** virksomhedens egen hjemmelsangivelse fra litra d (vitale interesser) til litra f.
- [2021-31-5654](#): Videregivelse til virksomhedens advokat var lovlig efter litra f.

EU-Domstolen har i [C-638/23](#) præciseret, at også administrative organer uden selvstændig juridisk personlighed kan udpeges som dataansvarlige, og i [C-683/21](#) fastlagt betingelserne for fælles dataansvar efter art. 26.

LOV	Databeskyttelsesforordningen § 6, stk. 1, 3	Databeskyttelsesloven § 8, stk. 3-4	
PRAKSIS	EU-Domstolen · Udpegelse af administrative organer uden juridisk personlighed som dataansvarlige i medfør af GDPR		27.02.2025
	EU-Domstolen · Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR (C-683/21)		05.12.2023

Datatilsynet · Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	09.10.2025
Datatilsynet · Datatilsynets landsdækkende tilsyn med de frie grundskolers håndtering af personoplysninger	30.09.2024
Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023
Datatilsynet · Skatteforvaltningens interne deling af personoplysninger var lovlig og nødvendig for myndighedsudøvelse	14.03.2023
Datatilsynet · Privat virksomheds videregivelse af personoplysninger til advokat var i overensstemmelse med reglerne	22.12.2022
Datatilsynet · DBA's afslag på sletning af brugeroplysninger var berettiget af hensyn til bekæmpelse af svindel	31.01.2022

§ 4 Samtykkets grænser: frivillighed, granularitet og forbuddet mod at skifte grundlag

Samtykke er i Datatilsynets praksis et **skrøbeligt** behandlingsgrundlag, og tilsynet advarer aktivt mod at vælge det.

Den ledende afgørelse er [2019-32-0709](#) om Rejsekort A/S. Kunden havde trukket sit samtykke tilbage, hvorefter selskabet forsøgte at fortsætte opbevaringen på kontrakt- og retskravshjemler. Tilsynet fandt, at samtykke aldrig burde have været valgt:

På grundlag af sagens oplysninger, er det Datatilsynets opfattelse, at Rejsekort under hele aftaleforholdet med klager kunne have behandlet personoplysninger om klager på baggrund af henholdsvis forordningens artikel 6, stk. 1, litra b, om behandling af oplysninger i forbindelse med kontraktforhold (i forhold til selve aftalen om et rejsekort), og artikel 6, stk. 1, litra c, om behandling af oplysninger til opfyldelse af en retlige forpligtelse, (i forhold til overholdelse af bogføringsloven).

Og videre om skiftet:

Datatilsynet har herved lagt væsentlig betydning, at en dataansvarlig som altovervejende udgangspunkt ikke bør skifte behandlingsgrundlag, efter behandlingen af personoplysninger er påbegyndt. I den henseende må et skift af behandlingsgrundlag anses som særlig problematisk, når behandlingen sker på baggrund af et samtykke, da et samtykke efter databeskyttelsesforordningen er et udtryk for, at de registrerede gives et reelt valg og kontrol over, hvordan deres oplysninger behandles.

Resultatet blev dobbelt **alvorlig kritik** – dels for tilsidesættelse af lovlighedsprincippet i [art. 5, stk. 1, litra a](#), dels for den fortsatte behandling efter tilbagekaldelsen – samt påbud om sletning efter [art. 58, stk. 2, litra g](#) med frist 1. december 2020 og krav om fornyet vurdering for øvrige kunder inden 1. februar 2021. Kun de økonomiske data kunne fortsat opbevares – i højst fem år efter [bogføringsloven § 10](#).

Gyldighedskravene er udfoldet i [2020-31-3354](#) om golf.dk, hvor tilsynet opstillede tre kernekrav og fandt alle tre brudt:

- **Frivillighed** – det var ikke muligt at afvise cookies.
- **Granularitet** – statistik og markedsføring kunne ikke vælges hver for sig.
- **Utvetydig viljestilkendegivelse** – fortsat brug af hjemmesiden udgør ikke samtykke.

Tilsynet citerede præambelbetragtning 32 ("Tavshed, forudafkrydsede felter eller inaktivitet bør derfor ikke udgøre samtykke") og henviste til EU-Domstolens **C-673/17** (Planet49). Virksomhedens indsigelse om undskyldelig retsvildfarelse blev afvist. Resultatet: **alvorlig kritik**.

Samme linje i [2021-431-0125](#) (Alstrøm – Din Isenkræmmer) og i [2020-431-0085](#), hvor DBA fik alvorlig kritik for en besværlig tilbagetrækningsmekanisme i strid med [art. 7, stk. 3](#). I [2023-31-0211](#) udvidedes praksis til **cookie-walls**: et betalingsalternativ, der alligevel krævede statistik-cookies, var i strid med frivillighedskravet.

At samtykke *kan* bruges korrekt viser [2021-31-5080](#), hvor indmeldelse i en kundeklub opfyldte kravene.

I **ansættelsesforhold** er samtykke særligt problematisk. Datatilsynet gav alvorlig kritik i [2019-32-0639](#) (Arbejdsmarkedets Feriefond) for både mangelfuld oplysningspligt og ugyldigt samtykke, jf. [art. 7, stk. 4](#). Ved rekruttering – se [2019-421-0033](#) (Fødevarestyrelsen) og [2023-431-0025](#) (Parken Services) – er det kombinationen af art. 5, 6, 9 og 13 sammen med [databeskyttelseslovens § 12](#) om ansættelsesforhold, der sætter rammen.

LOV	Databeskyttelsesforordningen § 5, stk. 1		Databeskyttelsesforordningen § 6, stk. 1	
	Databeskyttelsesforordningen § 7, stk. 3, 4		Databeskyttelsesloven § 12	
PRAKSIS	Datatilsynet · Parken Services A/S' behandling af personoplysninger i forbindelse med rekruttering			05.09.2024
	Datatilsynet · Cookie-walls: Krav om statistik-cookies i betalingsalternativ var i strid med reglerne om frit samtykke			18.03.2024
	Datatilsynet · Indhentelse af samtykke ved indmeldelse i kundeklub var i overensstemmelse med GDPR			26.04.2022
	Datatilsynet · Alvorlig kritik af DBA for mangelfuld samtykkeløsning og besværlig tilbagetrækning			26.01.2022
	Datatilsynet · Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies			20.10.2021
	Datatilsynet · Fødevarestyrelsens overholdelse af databeskyttelsesreglerne i forbindelse med rekrutteringsprocesser			02.03.2021
	Datatilsynet · Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside			13.11.2020
	Datatilsynet · Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering			03.11.2020
	Datatilsynet · Alvorlig kritik af Arbejdsmarkedets Feriefond for mangelfuld oplysningspligt og ugyldigt samtykke			20.12.2019

§ 5 Særlige kategorier og oplysninger om strafbare forhold: den skærpede hjemmelskontrol

Ved følsomme oplysninger efter [artikel 9](#) og oplysninger om strafbare forhold efter [databeskyttelseslovens § 8](#) skærpes Datatilsynets kontrol markant – og det er her, bødeindstillingerne mod private oftest opstår.

Videregivelse af oplysninger om strafbare forhold til en videre kreds er den klassiske fejl. I [Nordbornholms Byggeforretning-sagen](#) havde en virksomhed skrevet til to kunder, at en tidligere medarbejder havde erkendt svindel ved politiafhøring, med angivelse af beløbet. Datatilsynet anerkendte den legitime kerne, men fandt udformningen uproportional:

Det må anses for legitimt at oplyse sine kunder om, at en medarbejder, der tidligere har tegnet virksomheden, ikke længere er ansat, og dermed ikke længere kan indgå aftaler på virksomhedens vegne, men detaljerede beskrivelser

af anklagerne mod den tidligere medarbejder, herunder oplysninger om, at den tidligere medarbejder skulle have erkendt forholdet ved en afhøring hos politiet, og hvor stort et beløb den tidligere medarbejder havde svindlet for, mener vi ikke er nødvendige for at varetage den legitime interesse.

Skærpende var, at Bornholm er et afgrænset område, hvor den pågældende fortsat bor og arbejder – hvilket øgede indgrebet i hans private og arbejdsmæssige forhold. Bødeindstilling: **400.000 kr.** Samme mønster i [sagen om manglende sletning af kundedata](#), hvor videregivelse af strafbare forhold kombineret med systematisk manglende sletning af ~385.000 kunders data førte til bødeindstilling på **150.000 kr.**, jf. [databeskyttelseslovens § 41, stk. 2](#).

Se også [2019-31-2250](#), hvor håndtering af følsomme oplysninger efter en afskedigelse udløste alvorlig kritik efter art. 6, 9 og 13.

Forskningsvideregivelse kræver tilladelse. I [2023-421-0013](#) fik Aarhus Universitet alvorlig kritik for videregivelse uden den fornødne tilladelse efter [databeskyttelseslovens § 10](#), og i [2020-422-0026](#) fik Region Syddanmark kritik for mangelfuld kontrol med personoplysninger anvendt til forskning.

Sundhedsdata udløser tilsynets skarpeste reaktioner. [Privathospitalet Capio A/S](#) blev indstillet til **1,5 mio. kr.** efter en IDOR-sårbarhed, hvor uvedkommende kunne tilgå tredjemands helbredsoplysninger ved blot at ændre URL-adressen efter log-ind – kombineret med at hospitalet ikke havde ført tilsyn med sine databehandlere i adskillige år. Skærpende var sårbarhedens fundamentale karakter ("burde være opdaget i forbindelse med test"), antallet af registrerede og datatypen.

At art. 9 ikke automatisk fører til kritik viser [2020-31-3840](#), hvor Tryg Forsikrings behandling af helbredsoplysninger blev fundet lovlig efter art. 9, stk. 2, sammenholdt med [databeskyttelseslovens § 7](#). Tilsvarende i [2025-31-1972](#), hvor videregivelse af fagforeningstilhørsforhold til en rådgiver under en arbejdsretlig tvist var lovlig – behandlingen var nødvendig for at retskrav kunne fastlægges, gøres gældende eller forsvares.

Det nationale råderum for følsomme oplysninger er beskrevet i [betænkning nr. 1565/2017, s. 222](#), hvor det antages, at eksisterende særlovgivning fastsat i overensstemmelse med databeskyttelsesdirektivet allerede opfylder art. 9, stk. 2, litra b, g, h, i og j – og at der navnlig er adgang til at opretholde konkrete lovregler om behandling af følsomme oplysninger i sundhedssektoren.

LOV	Databeskyttelsesforordningen § 9, stk. 2	Databeskyttelsesloven § 7
	Databeskyttelsesloven § 8, stk. 3, 4	Databeskyttelsesloven § 10
PRAKSIS	Datatilsynet · Lovlig videregivelse af personoplysninger og fagforeningstilhørsforhold til rådgiver under arbejdsretlig tvist	09.04.2026
	Datatilsynet · Aarhus Universitet får alvorlig kritik for manglende tilladelse til videregivelse af personoplysninger	11.06.2024
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Politianmeldelse af privat virksomhed for manglende sletning af kundedata	02.12.2022
	Datatilsynet · Kritik af Region Syddanmark for mangelfuld kontrol med personoplysninger til forskning	20.07.2022
	Datatilsynet · Tryg Forsikring frifundet for kritik i sag om behandling af helbredsoplysninger	08.12.2021
	Datatilsynet · Politianmeldelse og bødeindstilling af virksomhed for ulovlig behandling af oplysninger om strafbare forhold	07.07.2021
	Datatilsynet · Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse	18.06.2020

§ 6 Opbevaringsbegrænsning: den dominerende bodegrund

Ingen enkelt bestemmelse har genereret flere og større bodeindstillinger end [artikel 5, stk. 1, litra e](#) om opbevaringsbegrænsning. Mønsteret er karakteristisk: store organisationer med komplekse it-landskaber, hvor slettepolitikken findes på papir men ikke er eksekveret teknisk.

Danske Bank blev indstillet til **10 mio. kr.** – den hidtil største danske bodeindstilling – efter at tilsynet af egen drift undersøgte ca. 400 systemer med oplysninger om millioner af nuværende og tidligere kunder, jf. [afgørelsen af 5. april 2022](#). Bankens indsigelse om kompleks it-arkitektur blev afvist:

Ét af grundprincipperne i GDPR er, at man kun må behandle oplysninger, man har brug for - og når man ikke har brug for dem længere, skal de slettes. Når det handler om en organisation af Danske Banks størrelse, der har mange og komplekse systemer, er det særlig afgørende, at man samtidig kan dokumentere, at sletningen rent faktisk sker.

Formildende vægt fik bankens løbende dokumentationsarbejde og samarbejdsvilje; skærpende var, at overtrædelsen ramte et grundlæggende princip, havde varet i årevis og berørte meget mange registrerede.

Det Kongelige Teater blev indstillet til **500.000 kr.** for at opbevare oplysninger om ca. 520.000 kunder i op til 25 år uden fastsatte slettefrister, jf. [afgørelsen af 9. januar 2024](#). Data gik tilbage til 1999; 104.000 kunder havde været inaktive i over fem år, 45.000 i over ti. Tilsynet afviste både de tekniske og de statistiske begrundelser:

Opbevaring af kundedata i 10, 15 eller endda 25 år langt overstiger, hvad der er nødvendigt for at administrere et kundeforhold eller sende markedsføring.

Afgørende var, at statistiske formål forudsætter **anonymisering** – opbevaring af identifikationsegenskaber uden konkret behov er et direkte brud. Overtrædelsen blev anset for forsætlig, fordi ledelsen var bekendt med manglen.

I den kommunale kontekst fastslog [2022-423-0261](#) den centrale retsregel:

Datatilsynet bemærker, at en manglende systemteknisk understøttelse ikke kan føre til, at princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e, tilsidesættes.

Mariagerfjord Kommune havde ca. 300 systemer, hvoraf mange ikke understøttede automatisk sletning – men kommunen havde heller ikke foretaget manuel sletning, hvor det var teknisk muligt, og manglede overblik over hvilke systemer der indeholdt overskredne oplysninger. Resultatet blev alvorlig kritik plus påbud om systemliste, sletning og en leverandørplan.

Samme princip i [sagen om manglende sletning af kundedata](#):

Det er ikke tilstrækkeligt blot at have en slettepolitik på papiret; den skal også efterleves i de tekniske systemer, der anvendes i den daglige drift. Tekniske vanskeligheder kan ikke retfærdiggøre en flerårig tilsidesættelse af de registreredes rettigheder.

Opbevaringsbegrænsningen skal holdes adskilt fra **sletteretten** efter [art. 17](#), som er en rettighed for den registrerede og ikke ubetinget. Datatilsynet præciserede i [2024-41-0093](#), at der ikke automatisk består slettepligt alene på baggrund af en anmodning – mindst ét af de seks kriterier i art. 17, stk. 1, skal være opfyldt. Sletteretten over for søgemaskiner behandles særskilt under [ret til at blive glemt](#), og kreditoplysningsbureauernes registreringer under [sletning hos RKI/Experian](#).

LOV	Databeskyttelsesforordningen § 5, stk. 1	Databeskyttelsesforordningen § 17, stk. 1
	Databeskyttelsesforordningen § 83, stk. 2	
PRAKSIS	Datatilsynet · Datatilsynets landsdækkende tilsyn med de frie grundskolers håndtering af personoplysninger	30.09.2024
	Datatilsynet · Det Kongelige Teater indstilles til bøde på 500.000 kr. for manglende sletning af kundedata	09.01.2024
	Datatilsynet · Politianmeldelse af privat virksomhed for manglende sletning af kundedata	02.12.2022
	Datatilsynet · Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	15.07.2022
	Datatilsynet · Danske Bank indstilles til bøde for manglende sletning af personoplysninger	05.04.2022

§ 7 Behandlingssikkerhed efter artikel 32: flerfaktorautentifikation, kryptering og adgangsstyring

[Artikel 32, stk. 1](#) er den hyppigst påberåbte bestemmelse i Datatilsynets tilsynspraksis, og tilsynet har gennem en række afgørelser opbygget et konkret **minimumskatalog**.

Flerfaktorautentifikation (MFA) ved fjernadgang er det klareste krav. [SIRIUS advokater](#) blev indstillet til **500.000 kr.** efter et ransomware-angreb via en medarbejderkonto beskyttet alene med brugernavn og adgangskode:

Advokatfirmaer behandler i sagens natur mange oplysninger, som kræver en særlig beskyttelse. I dette tilfælde har SIRIUS advokater manglet basale sikkerhedsforanstaltninger, og det betød desværre, at bl.a. klienternes oplysninger blev kompromitteret. Man kan ikke gardere sig 100 % mod hackerangreb, men reglerne i GDPR kræver, at man gør en indsats for at undgå det, der svarer til risikoen.

Skærpende var, at firmaet var i gang med at implementere MFA, men ikke havde gennemført det – undladelsen blev anset for **væsentlig uagtsomhed**.

[Lyngby-Taarbæk Kommune](#) blev indstillet til **350.000–400.000 kr.** efter to hændelser: mindst 1.000 tidligere medarbejdere havde bevaret adgang til KMD Nexus med oplysninger om ca. 30.000 borgere, og en uvedkommende misbrugte loginoplysninger til Microsoft-tjenester med adgang til ca. 5.000 personers data. Tilsynet formulerede kravet kategorisk:

Når man giver medarbejderne adgang til it-systemer med personoplysninger direkte fra internettet, øges risikoen for, at uvedkommende – f.eks. hackere – får adgang til oplysningerne og kan misbruge dem. Hvis der gives adgang til beskyttelsesværdige oplysninger, har det længe været et krav, at der skal være implementeret flerfaktorautentifikation for at sikre et passende beskyttelsesniveau.

Kryptering af udtagelige medier er ligeledes obligatorisk. [Civilstyrelsen](#) blev indstillet til **100.000 kr.**, efter at et ukrypteret USB-stik med over 800 siders følsomme oplysninger bortkom – og bruddet oven i købet ikke blev anmeldt:

Kryptering af udtagelige lagringsmidler, der indeholder personoplysninger (herunder USB-stik) må anses for at være en nødvendig og påkrævet sikkerhedsforanstaltning.

Samme princip i [kommunesagen af 14. august 2024](#), hvor tyveri af fem bærbare computere afdækkede, at op til 300 kommunale computere manglede kryptering – bødeindstilling **200.000 kr.**, jf. [databeskyttelseslovens § 41, stk. 6](#). Tilsynet understregede, at problemet er gentaget, og at offentlige myndigheder skal udvise særlig påpasselighed.

Logning og adgangsstyring blev konkretiseret i [2022-423-0261](#):

Det er Datatilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at den dataansvarlige løbende foretager stikprøver af loggen for at kontrollere, at brugerne kun tilgår oplysninger, de har et arbejdsbetinget behov for.

Og om lokale installationsrettigheder:

Det er endvidere Datatilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at medarbejdere ikke har rettigheder til at installere programmer på egne mobile enheder og computere, der har adgang til det netværk hvor produktionsdata tilgås, da muligheden for lokal eksekvering kan give et unødigt angrebspunkt for uautoriseret adgang, ransomwareangreb og installation af bagdøre eller anden skadelig kode.

Halvårlig kontrol af adgangsrettigheder blev anset for **utilstrækkelig**.

Regionerne er gengangere. [Region Syddanmark](#) blev indstillet til **500.000 kr.** for to parallelle svigt: et netværksdrev med for bred adgangsprofil (ca. 4.000 registrerede, ca. 25.000 medarbejdere med potentiel adgang, eksponeret i 3 år og 4 måneder) og en forskningsdatabase med URL-manipulationssårbarhed (over 30.000 registrerede, over 1,5 år). Mange berørte var børn i børne- og ungdomspsykiatrien. Skærpende var, at regionen tidligere havde fået alvorlig kritik for et lignende brud. Se også [Region Midtjylland](#), [Region Sjælland](#) (Klinisk Logistik) og [2021-422-0033](#) (Region Nordjylland, adgangskort). [Udlændingestyrelsen](#) blev tilsvarende politianmeldt for grove sikkerhedsbrister, og [2021-431-0126](#) angik utilstrækkelig sikkerhed om børns oplysninger.

EU-Domstolen har i [C-340/21](#) sat den principielle ramme: art. 24 og 32 er ikke en absolut garanti mod ethvert brud.

Databeskyttelsesforordningens artikel 24 og 32 kan derfor ikke forstås således, at en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af tredjemand er tilstrækkelig til at konkludere, at de foranstaltninger, som den pågældende dataansvarlige har truffet, ikke var passende som omhandlet i disse bestemmelser, uden at det overhovedet gøres muligt for sidstnævnte at føre bevis for det modsatte.

Men **bevisbyrden** vender:

Det fremgår utvetydigt af ordlyden af databeskyttelsesforordningens artikel 5, stk. 2, artikel 24, stk. 1, og artikel 32, stk. 1, at bevisbyrden for, at personoplysningerne behandles på en måde, der sikrer tilstrækkelig sikkerhed for disse oplysninger som omhandlet i denne forordnings artikel 5, stk. 1, litra f), og artikel 32, påhviler den pågældende dataansvarlige.

LOV

Databeskyttelsesforordningen § 24, stk. 1

Databeskyttelsesforordningen § 32, stk. 1

Databeskyttelsesloven § 41, stk. 6

PRAKSIS	EU-Domstolen · Databeskyttelse og erstatningsansvar: Cyberangreb, bevisbyrde og immateriel skade ved frygt for datamisbrug	14.12.2023
	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024
	Datatilsynet · Kommune indstillet til politianmeldelse og bøde for manglende kryptering af følsomme e-mails	14.08.2024
	Datatilsynet · Alvorlig kritik af Region Sjælland for manglende sikkerhed og adgangskontrol i Klinisk Logistik	13.09.2023
	Datatilsynet · Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	25.08.2022
	Datatilsynet · Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	15.07.2022
	Datatilsynet · SIRIUS advokater politianmeldt og indstillet til bøde for manglende behandlingssikkerhed	14.07.2022
	Datatilsynet · Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	12.05.2022
	Datatilsynet · Datatilsynets tilsyn med Region Nordjyllands administration af adgangskort	18.01.2022
	Datatilsynet · Region Midtjylland indstillet til bøde for manglende adgangsstyring af følsomme personoplysninger	08.09.2021
	Datatilsynet · Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	17.08.2021
	Datatilsynet · Region Syddanmark politianmeldes og indstilles til bøde på 500.000 kr. for alvorligt sikkerhedsbrud	16.07.2021

Brud på persondatasikkerheden: 72-timersfristen, dokumentation og underretning

§ 8

Artikel 33, stk. 1 pålægger anmeldelse uden unødigt forsinkelse og om muligt senest 72 timer – **medmindre** det er usandsynligt, at bruddet indebærer en risiko for de registreredes rettigheder.

Denne undtagelse er reel. I 2019-41-0035 havde DJØF registreret 15 hændelser, som foreningen havde klassificeret som brud, men ikke anmeldt. Datatilsynet tilsluttede sig vurderingen:

Datatilsynet har i den forbindelse vurderet, at det må betegnes som usandsynligt, at de pågældende brud indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder, jf. artikel 33, stk. 1.

Afgørende var, at DJØF kunne fremlægge **dokumentation** for hver enkelt vurdering. Det peger på den ofte oversete pligt i artikel 33, stk. 5: alle brud skal dokumenteres internt, uanset om de anmeldes.

Ifølge databeskyttelsesforordningens artikel 33, stk. 5, skal den dataansvarlige dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden (Datatilsynet) i stand til at kontrollere, at bestemmelsen er overholdt.

Betænkning nr. 1565/2017 uddyber på [s. 495](#), at tilsynsmyndigheden ikke har pligt til at indhente dokumentationen, men at den dataansvarlige har pligt til at stille den til rådighed på anmodning – og at dokumentationen bør omfatte, om og hvordan underretning efter art. 34 er sket.

Datatilsynet har gennemført systematiske temaundersøgelser af anmeldelsespraksis. Runden i december 2020 omfattede bl.a. [2019-421-0029](#) (Ankestyrelsen), [2019-421-0030](#) (Styrelsen for Patientklager), [2019-423-0204](#) (Bornholms Regionskommune) og [2019-41-0036](#) (Ase Lønmodtager). Runden i august 2023 dækkede både private og offentlige dataansvarlige: [2021-41-0133](#), [2021-41-0134](#), [2021-41-0135](#), [2021-41-0137](#) og [2021-423-0243](#).

Manglende anmeldelse vejer selvstændigt ved sanktionsvalget. I [Civilstyrelsen-sagen](#) blev styrelsen bekendt med bruddet 26. august 2020, men anmeldte det ikke – hvilket sammen med den manglende kryptering og de manglende retningslinjer bar bødeindstillingen på 100.000 kr. Også Datatilsynets egen sag [2020-442-8866](#) angik både art. 33 og [art. 34](#) om underretning af de registrerede ved høj risiko.

At et brud ikke automatisk er ansvarspådragende følger af [C-340/21](#), hvor Domstolen fortolkede fritagelsen i art. 82, stk. 3, strengt:

Når et brud på persondatasikkerheden ... er blevet begået af cyberkriminelle og dermed af »tredjemand« ... kan denne tilsidesættelse ikke tilregnes den dataansvarlige, medmindre denne har muliggjort det nævnte brud ved at tilsidesætte en forpligtelse, der er fastsat i databeskyttelsesforordningen, og navnlig den forpligtelse til at beskytte oplysninger, som påhviler den dataansvarlige i henhold til samme forordnings artikel 5, stk. 1, litra f), og artikel 24 og 32.

Dommen fastslog samtidig, at velbegrundet **frygt** for fremtidigt misbrug i sig selv kan udgøre immateriel skade efter art. 82 – et erstatningsretligt spor, der ligger uden for Datatilsynets kompetence, men som ofte følger i kølvandet på tilsynets afgørelser. Kollektiv håndhævelse er muliggjort ved [C-319/20](#) om forbrugersammenslutningers gruppesøgsmål efter art. 80.

LOV	Databeskyttelsesforordningen § 33, stk. 1, 5	Databeskyttelsesforordningen § 34, stk. 1
	Databeskyttelsesforordningen § 82, stk. 1, 3	
PRAKSIS	EU-Domstolen · Databeskyttelse og erstatningsansvar: Cyberangreb, bevisbyrde og immateriel skade ved frygt for datamisbrug 14.12.2023 EU-Domstolen · Forbrugersammenslutningers ret til at anlægge gruppesøgsmål for overtrædelser af databeskyttelsesforordningen (GDPR) 28.04.2022 Datatilsynet · Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden 31.08.2023 Datatilsynet · Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden 31.08.2023 Datatilsynet · Tilsyn med procedurer for anmeldelse af brud på persondatasikkerheden hos privat virksomhed 31.08.2023 Datatilsynet · Rettidig anmeldelse af brud på persondatasikkerheden hos en privat virksomhed 31.08.2023 Datatilsynet · Tilsyn med offentlig myndigheds overholdelse af regler om anmeldelse af brud på persondatasikkerheden 31.08.2023 Datatilsynet · Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden 12.05.2022 Datatilsynet · Ingen kritik af DJØF efter tilsyn med anmeldelse af brud på persondatasikkerheden 08.12.2020 Datatilsynet · Ingen kritik af Ankestyrelsens procedurer for anmeldelse af brud på persondatasikkerheden 08.12.2020 Datatilsynet · Datatilsynets tilsyn med Styrelsen for Patientklagers anmeldelse af brud på persondatasikkerheden 08.12.2020	

Datatilsynet · Datatilsynets tilsyn med Bornholms Regionskommunes håndtering af brud på persondatasikkerheden	08.12.2020
Datatilsynet · Datatilsynets tilsyn med Ase Lønmodtager efter anmeldelse af brud på persondatasikkerheden	08.12.2020
Datatilsynet · Alvorlig kritik af Datatilsynet for manglende behandlingssikkerhed og underretning ved brud på persondatasikkerheden	11.09.2020

§ 9 Risikovurdering og konsekvensanalyse: AULA-sagerne og kommunernes dataansvar

Datatilsynets tilsyn med **AULA** udgør den mest systematiske praksis om [artikel 35](#). Forhistorien er, at tilsynet i december 2019 ved et tilsyn hos KOMBIT fastslog, at det er **de enkelte kommuner** – ikke leverandøren – der er dataansvarlige for behandlingen i AULA. Herefter varsledes i oktober 2021 tilsyn med seks udvalgte kommuner.

Den grundlæggende præmis blev formuleret i [2023-423-0008](#) om Randers Kommune:

Det er en grundlæggende forudsætning for at kunne sikre et passende sikkerhedsniveau, at den dataansvarlige har identificeret og vurderet de risici, som behandlingen af personoplysninger indebærer. Uden en risikovurdering kan en dataansvarlig ikke vide, om de implementerede sikkerhedsforanstaltninger er tilstrækkelige.

Randers havde nedskrevet flere af KOMBIT's høje risici til medium eller lav uden at redegøre for fravigelsen – og tilsynet modtog fortsat løbende anmeldelser om fejlfremsendte beskeder, hvilket modbeviste kommunens egen vurdering. Resultat: **kritik** for art. 5, stk. 2, jf. stk. 1, litra f, og art. 24, stk. 1, jf. art. 32, stk. 1, samt **alvorlig kritik** for art. 35, stk. 1.

[2023-423-0004](#) om Frederikshavn Kommune skærper timingkravet. Kommunen havde identificeret 27 høje og 195 mellemrisici, men havde primært organisatoriske foranstaltninger (undervisning, onboarding):

Datatilsynet finder derudover, at Frederikshavn Kommune ved først at have udarbejdet en konsekvensanalyse for behandlingen af personoplysninger i AULA næsten tre år efter, at det har stået klart, at kommunen er dataansvarlig for behandling af personoplysninger i en løsning, der indebærer en høj risiko for de registrerede, har handlet i strid med databeskyttelsesforordningens artikel 35, stk. 1. Datatilsynet finder det i den forbindelse alvorligt, at konsekvensanalysen først ses at være udarbejdet efter, at Datatilsynet har anmodet om materialet som led i det skriftlige tilsyn på området.

Pointen er dobbelt: DPIA'en skal foreligge **før** behandlingen, og generel GDPR-undervisning kompenserer ikke for manglende tekniske foranstaltninger mod fejlfremsendelse.

[2023-423-0005](#) om Københavns Kommune nuancerer. Her fandt tilsynet, at DPIA'en var udarbejdet rettidigt – fordi dataansvaret først blev afklaret i december 2019 – men at **indholdet** ikke opfyldte mindstekravene:

Det er imidlertid Datatilsynets vurdering, at Københavns Kommune ikke har gennemført en fyldestgørende konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35, stk. 1, idet den fremsendte konsekvensanalyse ikke opfylder mindstekravene hertil i forordningens artikel 35, stk. 7, litra a-d.

Analysen manglede vurdering af nødvendighed og proportionalitet, sammenhæng til de bagvedliggende risikoskemaer og dokumentation for, at DPO'en var hørt, jf. [art. 35, stk. 2](#). Udrulningen til dagtilbud udløste derimod ikke fornyet analysepligt efter [art. 35, stk. 11](#).

Chromebook- og Google Workspace-sagerne følger samme logik. [2020-431-0061](#) mod Helsingør Kommune blev startskuddet – alvorlig kritik og påbud efter art. 5, 6, 28, stk. 3, og 35. [2021-432-0056](#) mod Aarhus Kommune udvidede til art. 24, 32 og 58, stk. 2. Kulminationen er [2025-431-0053](#), hvor **51 kommuner** fik alvorlig kritik for manglende beskyttelse af skoleelevers data efter art. 5, 24, 28, stk. 3, og 32.

Tilsynet har gennemgående anbefalet kommunerne at overveje **fælles** konsekvensanalyser eller et adfærdskodeks efter art. 40 i samarbejde med KL og KOMBIT – en erkendelse af, at 98 parallelle DPIA'er for samme system er ineffektivt.

Betænkning nr. 1565/2017 behandler på [s. 415](#) den beslægtede pligt i [art. 25](#) om databeskyttelse gennem design og bemærker, at et it-system, der ikke understøtter fx indsigt eller dataportabilitet, efter omstændighederne kan udgøre en overtrædelse – men at manglen delvis kan afhjælpes organisatorisk. Betænkningen fremhæver også, at kravene bør indarbejdes allerede i **udbudsfasen**, jf. præambelbetragtning 78.

LOV	Databeskyttelsesforordningen § 24, stk. 1	Databeskyttelsesforordningen § 25, stk. 1
	Databeskyttelsesforordningen § 32, stk. 1	Databeskyttelsesforordningen § 35, stk. 1, 2, 7, 11
PRAKSIS	Datatilsynet · Alvorlig kritik af 51 kommuner for manglende beskyttelse af skoleelevers data i Chromebook-sagen	29.01.2026
	Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	23.05.2024
	Datatilsynet · Alvorlig kritik af Randers Kommunes manglende risikovurderinger og utilstrækkelige behandlingssikkerhed	22.12.2023
	Datatilsynet · Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	22.12.2023
	Datatilsynet · Alvorlig kritik og påbud til Aarhus Kommune for behandling af elevoplysninger i Google Workspace	08.09.2022
	Datatilsynet · Alvorlig kritik og påbud til Helsingør Kommune i sag om Chromebooks og Google Workspace	10.09.2021

§ 10 Databehandlere, instruks og tredjelandsoverførsler

[Artikel 28](#) genererer en selvstændig praksisgren, hvor databehandleren har et **eget** ansvar.

Den principielle afgørelse er [2019-431-0045](#) om MaCom A/S (Lectio), der uden instruks fra de dataansvarlige gymnasier havde videregivet uddrag af elevopgaver til forskere ved DIKU. To spørgsmål blev afklaret:

- Er en opgavebesvarelse en personoplysning?** Ja – tilsynet henviste til **C-434/16** (Nowak): besvarelsen afspejler elevens "viden og kompetence inden for et givent område samt i givet fald hans tankegang, dømmekraft og kritiske sans".
- Er pseudonymiserede uddrag personoplysninger?** Ja – efter **C-582/14** (Breyer) kræver identificering ikke, at alle oplysninger findes hos én aktør; da MaCom fortsat havde de fulde besvarelser, var uddragene pseudonymiserede personoplysninger, jf. art. 4, nr. 5.

Skærpende var, at virksomheden slettede data løbende og derfor **ikke kunne opgøre omfanget** af videregivelsen – en mangel i den organisatoriske styring, der forhindrede påvisning af dataminimering og ansvarlighed. Formildende var det videnskabelige formål, den fysiske adgang uden udlevering og pseudonymiseringen. Resultat: **alvorlig kritik** for art. 28, stk. 3.

Se også [2019-442-3996](#) (alvorlig kritik for behandling uden for instruks, art. 28, stk. 3 og 10) og [2022-431-0167](#), hvor en **underdatabehandler** fik alvorlig kritik for at nægte at udlevere oplysninger til den dataansvarlige.

Tilsynspligten med databehandlere er skærpet. I [Capio-sagen](#) vejede det tungt, at hospitalet ikke havde ført tilsyn med tre stikprøvevis udvalgte databehandlere i adskillige år – det første tilsyn kom først, da Datatilsynet selv indledte undersøgelse. Pligten er beskrevet i [vejledning til bekendtgørelse om andre aktører](#), der udleder af ansvarlighedsprincippet i art. 5, stk. 2, at den dataansvarlige må føre et større eller mindre tilsyn med, at databehandleraftalen overholdes, og at de aftalte foranstaltninger faktisk er gennemført.

Tredjelandsoverførsler efter kapitel V behandles i [2025-211-3556](#), hvor tilsynet vurderede generelle tilladelser til tredjelandsoverførsler i databehandleraftaler efter art. 28, stk. 3, jf. art. 44 og 46. I [2022-212-3529](#) afklarede tilsynet den praktisk vigtige sondring mellem tilsigtede overførsler og **utilsigtet teknisk routing** gennem tredjelande – et spørgsmål, der er blevet aktualiseret efter EU-Domstolens dom i [C-311/18](#) (Schrems II), som gjorde overførsler til USA vanskelige uden supplerende foranstaltninger.

At databehandlerrelationen også har en strafferetlig side fremgår af [Rigsadvokatmeddelelsen om databeskyttelse i straffesager](#):

Både den dataansvarlige og eventuelle databehandlere kan ifalde strafansvar for overtrædelse af databeskyttelsesreglerne.

EU-Domstolen har i [C-683/21](#) præciseret grænsedragningen mellem dataansvarlig, fælles dataansvarlig og databehandler i bødesammenhæng.

LOV	Databeskyttelsesforordningen § 5, stk. 2	Databeskyttelsesforordningen § 28, stk. 3
	Databeskyttelsesforordningen § 44	Databeskyttelsesforordningen § 46, stk. 2
PRAKSIS	EU-Domstolen · Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR (C-683/21)	05.12.2023
	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	23.01.2026
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	29.03.2022
	Datatilsynet · Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	07.02.2022
	Datatilsynet · Alvorlig kritik af testvirksomhed for brud på persondatasikkerheden ved videregivelse af opgavebesvarelser	18.06.2020
	Datatilsynet · Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	19.12.2019

De registreredes rettigheder: oplysningspligt, indsigt og gebyrforbuddet

§ 11

Rettighedskapitlet genererer flest **klagesager** – og dermed den mest borgernære del af Datatilsynets praksis.

Oplysningspligten efter [art. 13](#) og [art. 14](#) er hyppig kritikgrund. [2021-432-0070](#) mod Statens Serum Institut angik mangelfuld oplysning om behandling af helbredsoplysninger, herunder rækkevidden af undtagelsen i art. 14, stk. 5, sammenholdt med [sundhedslovens § 222](#). [2021-432-0059](#) mod Region Hovedstaden angik mangelfuld information om databehandling og rettigheder efter art. 12-14. Se også [2022-431-0204](#) om Tryk

Forsikring og [2025-41-0139](#), hvor et tematisk tilsyn med ejendomsadministratorer dækkede art. 13-15 og 17 samlet.

Indsigtsretten efter [art. 15](#) er ikke absolut. I [2021-32-2438](#) kunne en tidligere arbejdsgiver afvise indsigt under henvisning til undtagelserne i [databeskyttelseslovens § 22](#). Omvendt fik Skatteforvaltningen **alvorlig kritik** i [2024-432-0039](#) for håndteringen af indsigtsanmodninger, navnlig fristerne i art. 12, stk. 3 og 4. Og i [2021-32-2463](#) fik Københavns Kommune kritik for både manglende oplysningspligt og indsigtsbehandling i forbindelse med en advokatundersøgelse.

Gebyrforbuddet er en udbredt misforståelse. I [2024-41-0093](#) fandt tilsynet, at flere frie grundskoler anvendte en forældet skabelon, hvorefter skolen kunne kræve 10 kr. pr. påbegyndt side, maksimalt 200 kr. Tilsynet fastslog, at teksten stammer fra bekendtgørelser udstedt i medfør af den **ophævede** persondatalov og ikke længere er gældende ret. Hovedreglen følger af [art. 12, stk. 5](#):

[...] enhver meddelelse og enhver foranstaltning, der træffes i henhold til artikel 15-22 og 34, er gratis. Hvis anmodninger fra en registreret er åbenbart grundløse eller overdrevne, især fordi de gentages, kan den dataansvarlige enten: a) opkræve et rimeligt gebyr ... eller b) afvise at efterkomme anmodningen. Bevisbyrden for, at anmodningen er åbenbart grundløs eller overdreven, påhviler den dataansvarlige.

Databeskyttelsesrådgiveren (DPO) understøtter rettighedsopfyldelsen. EU-Domstolen har i [C-453/21](#) fastslået, at medlemsstaterne må give DPO'en stærkere afskedigelsesbeskyttelse end art. 38, stk. 3, forudsat det ikke bringer forordningens formål i fare, og at interessekonflikt efter art. 38, stk. 6, foreligger, når DPO'en selv kan fastlægge formål og hjælpemidler:

Det følger navnlig heraf, at en databeskyttelsesrådgiver ikke kan overdrages opgaver eller pligter, der ville medføre, at vedkommende kan fastlægge formålene med og hjælpemidlerne til behandlingen af personoplysninger hos den dataansvarlige eller databehandleren.

I [2023-423-0005](#) indgik det som kritikpunkt, at det ikke fremgik, om DPO'en var hørt om konsekvensanalysen.

Endelig viser [2020-432-0047](#) om Gladsaxe Kommune, at gennemsigtighedsprincippet i art. 5, stk. 1, litra a, også gælder for behandling af oplysninger om hjemmesidebesøgende.

LOV

[Databeskyttelsesforordningen § 12, stk. 3-5](#)
[Databeskyttelsesforordningen § 13, stk. 1](#)
[Databeskyttelsesforordningen § 14, stk. 1, 5](#)
[Databeskyttelsesforordningen § 15, stk. 1](#)
[Databeskyttelsesloven § 22](#)

PRAKSIS	EU-Domstolen · Beskyttelse af databeskyttelsesrådgivere mod afskedigelse og vurdering af interessekonflikter under GDPR	09.02.2023
	Datatilsynet · Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	12.12.2025
	Datatilsynet · Datatilsynet udtaler alvorlig kritik af Skatteforvaltningens håndtering af indsigtsanmodninger	30.09.2025
	Datatilsynet · Datatilsynets landsdækkende tilsyn med de frie grundskolers håndtering af personoplysninger	30.09.2024
	Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	23.05.2024
	Datatilsynet · Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	02.01.2024

Datatilsynet · Kritik af Statens Serum Instituts mangelfulde oplysning af borgere om behandling af helbredsoplysninger	02.02.2023
Datatilsynet · Kritik af Københavns Kommunes manglende oplysningspligt og indsigtsbehandling i advokatundersøgelse	29.11.2022
Datatilsynet · Kritik af Region Hovedstaden for mangelfuld information til borgerne om databehandling og rettigheder	21.10.2022
Datatilsynet · Tidligere arbejdsgiver kunne afvise at efterkomme anmodning om indsigt	31.03.2022
Datatilsynet · Kritik af Gladsaxe Kommunes behandling af personoplysninger om hjemmesidebesøgende	17.11.2021

§ 12 Bødeindstillingerne: niveau, kriterier og Datatilsynets bødevejledning

Datatilsynets bødeindstillinger tegner et niveau, der er markant lavere end i mange andre medlemsstater – en direkte konsekvens af, at bøden skal passere anklagemyndighed og domstole.

Sag	År	Overtrædelse	Indstillet bøde
Danske Bank	2022	Art. 5, stk. 1, litra e – sletning i ~400 systemer	10.000.000 kr.
Privathospitalet Capio	2024	Art. 32 – IDOR-sårbarhed, manglende databehandlertilsyn	1.500.000 kr.
Det Kongelige Teater	2024	Art. 5, stk. 1, litra e – 520.000 kunder i op til 25 år	500.000 kr.
SIRIUS advokater	2022	Art. 32 – manglende MFA, ransomware	500.000 kr.
Region Syddanmark	2021	Art. 32 – netværksdrev + forskningsdatabase	500.000 kr.
Nordbornholms Byggeforretning	2021	DBL § 8 – strafbare forhold videregivet til kunder	400.000 kr.
Lyngby-Taarbæk Kommune	2024	Art. 32 – MFA, brugerstyring, ~42.000 berørte	350.000–400.000 kr.
Kommune (kryptering)	2024	Art. 32 – op til 300 ukrypterede computere	200.000 kr.
Privat virksomhed	2022	Art. 5, stk. 1, litra e + DBL § 8 – ~385.000 kunder	150.000 kr.
Civilstyrelsen	2022	Art. 32 + 33 – ukrypteret USB, manglende anmeldelse	100.000 kr.

Hertil kommer bødeindstillinger mod [Udlændingestyrelsen](#), [Region Midtjylland](#) og [Texas Andreas Petersen A/S](#) (cookies).

Mønstre i udmålingen:

- To overtrædelsestyper dominerer fuldstændigt: **manglende sletning** (art. 5, stk. 1, litra e) og **utilstrækkelig behandlingssikkerhed** (art. 32).
- Overtrædelser af **grundlæggende principper** vægter tungest – det er begrundelsen for Danske Banks 10 mio. kr.

- **Varighed og systematik** skærper: "gentagne", "over en længere periode", "systemisk karakter".
- **Antal registrerede og oplysningernes karakter** er gennemgående – særligt børn og sårbare grupper.
- **Forsæt** skærper markant; Det Kongelige Teaters overtrædelse blev anset for forsætlig, fordi ledelsen kendte manglen.
- **Samarbejdsvilje** og efterfølgende afhjælpning formilder – men ophæver ikke ansvaret.
- **Gentagelse** skærper: Region Syddanmark havde tidligere fået alvorlig kritik for et lignende brud.
- For offentlige myndigheder inddrages **indbyggertal og driftsbevilling** for at sikre afskrækkende virkning, jf. [databeskyttelseslovens § 41, stk. 6](#).

Den metodiske ramme er Datatilsynets **bødevejledning**, hvis status fastlægges i [Rigsadvokatmeddelelsen om databeskyttelse i straffesager](#):

Datatilsynets bødevejledning skal være normerende for både Datatilsynets indstilling til bødepåstanden og for anklagemyndighedens påstand i retten. Det er i den forbindelse vigtigt at være opmærksom på, at strafudmålingsprincipperne i straffelovens kapitel 10 også finder anvendelse på sager om overtrædelse af de databeskyttelsesretlige regler.

Beregningsmodellen er trinvis: **grundbeløb** (overtrædelsens kategori × virksomhedens globale årlige omsætning) → justering for karakter, alvor og varighed → skærpene og formildende omstændigheder → loft efter [art. 83, stk. 4-6](#) → eventuel hensyntagen til betalingsevne.

RM fastlægger også de processuelle rammer: Datatilsynet **skal høres** i alle sager, politikredsen skal forelægge tiltalepørgsmålet for **statsadvokaten**, statsadvokaten skal drøfte bødepåstanden med Datatilsynet, og sagerne må **ikke afgøres med bødeforelæg**, før bødeniveauet er tilstrækkelig afklaret i retspraksis. Om ansvarssubjektet er RM utvetydig:

Det bemærkes dog, at det i sager om overtrædelse af de databeskyttelsesretlige regler og i sager om overtrædelser med databeskyttelsesretlige elementer altid er den dataansvarlige eller databehandleren, der er ansvarssubjekt.

Endelig rækker bødeniveauet ud over GDPR selv. Efter RM's [pkt. 3.10.9](#) er Danmark EU-retligt forpligtet til at sikre, at bøder for overtrædelser af **straffeloven med databeskyttelsesretlige elementer** ikke er lavere, end de ville have været efter databeskyttelsesreglerne – en regel, der siden 27. september 2021 har smittet af på fx [Rigsadvokatmeddelelsen om freds- og ærekrænkelser](#) og digitale sexkrænkelser.

LOV	Databeskyttelsesforordningen § 5, stk. 1	Databeskyttelsesforordningen § 32, stk. 1
	Databeskyttelsesforordningen § 83, stk. 2	Databeskyttelsesloven § 41, stk. 3, 6
PRAKSIS	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024
	Datatilsynet · Kommune indstillet til politianmeldelse og bøde for manglende kryptering af følsomme e-mails	14.08.2024
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Det Kongelige Teater indstilles til bøde på 500.000 kr. for manglende sletning af kundedata	09.01.2024
	Datatilsynet · Texas Andreas Petersen A/S politianmeldt og indstillet til bøde for ulovlig cookie-behandling	06.10.2023
	Datatilsynet · Politianmeldelse af privat virksomhed for manglende sletning af kundedata	02.12.2022

Datatilsynet · SIRIUS advokater politianmeldt og indstillet til bøde for manglende behandlingssikkerhed	14.07.2022
Datatilsynet · Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	12.05.2022
Datatilsynet · Danske Bank indstilles til bøde for manglende sletning af personoplysninger	05.04.2022
Datatilsynet · Region Midtjylland indstillet til bøde for manglende adgangsstyring af følsomme personoplysninger	08.09.2021
Datatilsynet · Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	17.08.2021
Datatilsynet · Region Syddanmark politianmeldes og indstilles til bøde på 500.000 kr. for alvorligt sikkerhedsbrud	16.07.2021
Datatilsynet · Politianmeldelse og bødeindstilling af virksomhed for ulovlig behandling af oplysninger om strafbare forhold	07.07.2021

§ 13 Fra tilsynets indstilling til domstolenes dom: koncernomsætning, skyld og sagsbehandlingstid

Den strafferetlige model betyder, at Datatilsynets indstilling kun er **udgangspunktet**. Domstolene træffer den endelige afgørelse – og har i de seneste år afklaret tre centrale spørgsmål.

Bødeloftet beregnes på koncernniveau. Vestre Landsret forelagde spørgsmålet præjudicielt, og EU-Domstolen svarede i [C-383/23](#) af 13. februar 2025, at begrebet "virksomhed" i [art. 83](#) skal forstås i overensstemmelse med EU's **konkurrenceret**: når et selskab i en økonomisk enhed straffes, beregnes maksimumsbøden på koncernens samlede globale årlige omsætning.

Vestre Landsret udmøntede dommen i [SS-364/2021-VLR](#) af 2. september 2025. Sagen angik manglende sletning af oplysninger om ca. 350.000 tidligere kunder i et ældre it-system (AX 2.5). Landsretten:

- **ændrede skyldsformen fra uagtsomhed til forsæt**, fordi vidneforklaringer viste, at ledelsen kendte til systemets fortsatte eksistens og lejlighedsvis brug uden slette- eller anonymiseringsprocedurer;
- lagde koncernens nettoomsætning i 2018 på ca. **6,9 mia. kr.** til grund, hvilket gav et bødeloft på **278 mio. kr.** (4 %);
- fastsatte bøden til **1,5 mio. kr.** i overensstemmelse med Datatilsynets indstilling – med den bemærkning, at bøden trods koncernstørrelsen måtte betragtes som relativt lille;
- afviste at nedsætte bøden for lang sagsbehandlingstid, fordi kompleksiteten og den præjudicielle forelæggelse retfærdiggjorde forløbet.

Formildende vægt fik, at oplysningerne ikke blev anvendt aktivt kommercielt.

Skyld er en betingelse – men den juridiske person hæfter direkte. EU-Domstolen fastslog i [C-807/21](#), at en bøde forudsætter forsæt eller uagtsomhed, men at overtrædelsen ikke skal kunne føres tilbage til en identificeret fysisk person i ledelsen. Det harmonerer med [databeskyttelseslovens § 41, stk. 6](#) og med Rigsadvokatmeddelelsens regel om, at ansvarssubjektet altid er den dataansvarlige eller databehandleren.

Sagsbehandlingstid kan formilde. I [S-185-23](#) af 28. april 2025 nedsatte landsretten bøden under henvisning til lang sagsbehandlingstid, jf. [straffelovens § 83](#) – en påmindelse om, at almindelige strafudmålingsprincipper gælder fuldt ud, jf. Rigsadvokatmeddelelsens henvisning til straffelovens kapitel 10.

Bøder kan også forhøjes. I [SS-715/2024-VLR](#) af 27. marts 2025 blev Vejle Kommune dømt for brud på databeskyttelsesforordningen, og bøden blev forhøjet til **100.000 kr.**, jf. [straffelovens § 80](#).

Den samlede lære er, at den danske model indebærer en **dobbelt filtrering**: Datatilsynets faglige vurdering møder domstolens strafferetlige prøvelse af både skyld og udmåling. Resultatet har hidtil været, at domstolene i vidt omfang følger tilsynets indstilling – men prøver skyldsspørgsmålet selvstændigt og kan skærpe det.

LOV	Databeskyttelsesforordningen § 83, stk. 4-6	Databeskyttelsesloven § 41, stk. 6
	Straffeloven § 80	Straffeloven § 83
PRAKSIS	EU-Domstolen · Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	13.02.2025
	EU-Domstolen · Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	05.12.2023
	Landsretten · Bøde for GDPR-overtrædelse fastsat på baggrund af hele koncernens omsætning efter afgørelse fra EU-Domstolen	02.09.2025
	Landsretten · Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid	28.04.2025
	Landsretten · Vejle Kommune dømt for brud på databeskyttelsesforordningen – bøde forhøjet til 100.000 kr.	27.03.2025

§ 14 Sammenfatning: hvad praksis kræver af den dataansvarlige

Datatilsynets afgørelsespraksis siden 2018 tegner et konsistent billede, der kan sammenfattes i seks punkter.

1. Sanktionen er gradueret, og skønnet er reelt. Tilsynet afslutter et betydeligt antal sager uden kritik, når organisationens modenhed svarer til risikoen – men følger ofte op med bemærkninger om dokumentationssvagheder. EU-Domstolen har i [C-768/21](#) bekræftet, at tilsynsmyndigheden ikke skal reagere med en korrigerende beføjelse i ethvert tilfælde.

2. Hjemmel skal kunne påvises konkret. Generelle henvisninger til lovgivningen eller til at behandlingen er "nødvendig" er utilstrækkelige, jf. [2024-41-0093](#). Samtykke bør vælges med varsomhed – og aldrig forlades undervejs, jf. [2019-32-0709](#).

3. Sletning skal ske i praksis, ikke kun på papir. Det er den største enkeltstående bøderisiko. Hverken it-kompleksitet, leverandørbegrænsninger eller statistiske formål bærer en flerårig tilsidesættelse, jf. [Danske Bank](#), [Det Kongelige Teater](#) og [2022-423-0261](#).

4. Sikkerhedsminimum er konkretiseret. Praksis har gjort følgende til udtrykkelige krav ved beskyttelsesværdige oplysninger: flerfaktorautentifikation ved fjernadgang, kryptering af bærbar enheder og udtagelige medier, løbende stikprøvekontrol af logs, hyppig gennemgang af adgangsrettigheder, rettidig nedlæggelse af brugeradgange ved fratræden, og begrænsning af medarbejderes installationsrettigheder.

5. Risikovurdering og DPIA er forudsætninger, ikke formaliteter. Uden risikovurdering kan sikkerhedsniveauet ikke fastlægges, og en DPIA udarbejdet efter tilsynets anmodning er per definition for sen. AULA-sagerne – [2023-423-0004](#), [2023-423-0005](#) og [2023-423-0008](#) – viser, at leverandørens risikovurdering ikke kan overtages ukritisk, og at afvigelser skal begrundes.

6. Bøderisikoen er blevet reel. Med [C-383/23](#) og [SS-364/2021-VLR](#) er koncernomsætningen forankret som beregningsgrundlag, og landsretten viste vilje til at skærpe skyldsformen fra uagtsomhed til forsæt. Selvom det danske bødeniveau fortsat ligger under den europæiske middelværdi, er de retlige rammer nu på plads for højere bøder.

Afgrænsning. Denne oversigt dækker Datatilsynets myndighedsudøvelse. Sletning i søgemaskiner behandles under [ret til at blive glemt](#), kreditoplysningsbureauernes registreringer under [sletning hos RKI/Experian](#), og civilretlig GDPR-erstatning efter art. 82 behandles særskilt – selvom [C-340/21](#) viser, at de to spor hænger tæt sammen: bevisbyrden for passende sikkerhed påhviler den dataansvarlige i begge.

Aktualitet. Databeskyttelsesloven er senest konsolideret ved lovbekendtgørelse af 22. marts 2024, og der er ikke vedtagne, endnu ikke konsoliderede ændringer.

LOV	Databeskyttelsesforordningen § 5, stk. 1	Databeskyttelsesforordningen § 32, stk. 1
	Databeskyttelsesforordningen § 35, stk. 1	Databeskyttelsesforordningen § 58, stk. 2
	Databeskyttelsesloven § 41	
PRAKSIS	EU-Domstolen · Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	13.02.2025
	EU-Domstolen · Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	26.09.2024
	EU-Domstolen · Databeskyttelse og erstatningsansvar: Cyberangreb, bevisbyrde og immateriel skade ved frygt for datamisbrug	14.12.2023
	Landsretten · Bøde for GDPR-overtrædelse fastsat på baggrund af hele koncernens omsætning efter afgørelse fra EU-Domstolen	02.09.2025
	Datatilsynet · Datatilsynets landsdækkende tilsyn med de frie grundskolers håndtering af personoplysninger	30.09.2024
	Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	23.05.2024
	Datatilsynet · Det Kongelige Teater indstilles til bøde på 500.000 kr. for manglende sletning af kundedata	09.01.2024
	Datatilsynet · Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	22.12.2023
	Datatilsynet · Alvorlig kritik af Randers Kommunes manglende risikovurderinger og utilstrækkelige behandlingssikkerhed	22.12.2023
	Datatilsynet · Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	15.07.2022
	Datatilsynet · Danske Bank indstilles til bøde for manglende sletning af personoplysninger	05.04.2022
	Datatilsynet · Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	03.11.2020

REFERENCE

Lovgrundlag

9 paragraffer

Databeskyttelsesforordningen § 5	stk. 1
Databeskyttelsesforordningen § 32	stk. 1
Databeskyttelsesforordningen § 35	stk. 1
Databeskyttelsesforordningen § 83	stk. 2
Databeskyttelsesloven § 41	

Databeskyttelsesforordningen § 6	stk. 1
Databeskyttelsesforordningen § 33	stk. 1
Databeskyttelsesforordningen § 58	stk. 2
Databeskyttelsesloven § 3	

MATERIALE Citerede afgørelser	86 afgørelser
--------------------------------------	---------------

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		8
27.02.2025	Udpegelse af administrative organer uden juridisk personlighed som dataansvarlige i medfør af GDPR	C-638/23
13.02.2025	Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	C-383/23
26.09.2024	Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	C-768/21
14.12.2023	Databeskyttelse og erstatningsansvar: Cyberangreb, bevisbyrde og immateriel skade ved frygt for datamisbrug	C-340/21
05.12.2023	Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR (C-683/21)	C-683/21
05.12.2023	Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	C-807/21
09.02.2023	Beskyttelse af databeskyttelsesrådgivere mod afskedigelse og vurdering af interessekonflikter under GDPR	C-453/21
28.04.2022	Forbrugersammenslutningers ret til at anlægge gruppesøgsmål for overtrædelser af databeskyttelsesforordningen (GDPR)	C-319/20
LANDSRETTE · ANKEINSTANS		3
02.09.2025	Bøde for GDPR-overtrædelse fastsat på baggrund af hele koncernens omsætning efter afgørelse fra EU-Domstolen	9975-11672
28.04.2025	Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid	9601-11193
27.03.2025	Vejle Kommune dømt for brud på databeskyttelsesforordningen – bøde forhøjet til 100.000 kr.	9568-11151
DATATILSYNET · NÆVN / KLAGEINSTANS		75
09.04.2026	Lovlig videregivelse af personoplysninger og fagforeningstilhørsforhold til rådgiver under arbejdsretlig tvist	2025-31-1972
29.01.2026	Alvorlig kritik af 51 kommuner for manglende beskyttelse af skoleelevers data i Chromebook-sagen	2025-431-0053
23.01.2026	Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	2025-211-3556
12.12.2025	Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	2025-41-0139
09.10.2025	Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	2025-31-1798
30.09.2025	Datatilsynet udtaler alvorlig kritik af Skatteforvaltningens håndtering af indsigtsanmodninger	2024-432-0039

27.11.2024	Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	
30.09.2024	Datatilsynets landsdækkende tilsyn med de frie grundskolers håndtering af personoplysninger	2024-41-0093
05.09.2024	Parken Services A/S' behandling af personoplysninger i forbindelse med rekruttering	2023-431-0025
14.08.2024	Kommune indstillet til politianmeldelse og bøde for manglende kryptering af følsomme e-mails	
11.06.2024	Aarhus Universitet får alvorlig kritik for manglende tilladelse til videregivelse af personoplysninger	2023-421-0013
23.05.2024	Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	2023-423-0005
18.03.2024	Cookie-walls: Krav om statistik-cookies i betalingsalternativ var i strid med reglerne om frit samtykke	2023-31-0211
01.02.2024	Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	
09.01.2024	Det Kongelige Teater indstilles til bøde på 500.000 kr. for manglende sletning af kundedata	
02.01.2024	Tryg Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	2022-431-0204
22.12.2023	Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	2023-423-0004
22.12.2023	Alvorlig kritik af Randers Kommunes manglende risikovurderinger og utilstrækkelige behandlingssikkerhed	2023-423-0008
17.11.2023	Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	2023-212-0015
06.10.2023	Texas Andreas Petersen A/S politianmeldt og indstillet til bøde for ulovlig cookie-behandling	
13.09.2023	Alvorlig kritik af Region Sjælland for manglende sikkerhed og adgangskontrol i Klinisk Logistik	
31.08.2023	Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden	2021-41-0133
31.08.2023	Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden	2021-41-0134
31.08.2023	Tilsyn med procedurer for anmeldelse af brud på persondatasikkerheden hos privat virksomhed	2021-41-0135
31.08.2023	Rettidig anmeldelse af brud på persondatasikkerheden hos en privat virksomhed	2021-41-0137
31.08.2023	Tilsyn med offentlig myndigheds håndtering og anmeldelse af brud på persondatasikkerheden	2021-423-0241

31.08.2023	Tilsyn med offentlig myndigheds overholdelse af regler om anmeldelse af brud på persondatasikkerheden	2021-423-0243
14.03.2023	Skatteforvaltningens interne deling af personoplysninger var lovlig og nødvendig for myndighedsudøvelse	2021-32-2645
02.02.2023	Kritik af Statens Serum Instituts mangelfulde oplysning af borgere om behandling af helbredsoplysninger	2021-432-0070
22.12.2022	Privat virksomheds videregivelse af personoplysninger til advokat var i overensstemmelse med reglerne	2021-31-5654
19.12.2022	Kritik af arbejdsgiver for at orientere bredere kreds om baggrund for afskedigelse	2021-31-5737
02.12.2022	Politianmeldelse af privat virksomhed for manglende sletning af kundedata	
29.11.2022	Kritik af Københavns Kommunes manglende oplysningspligt og indsigtsbehandling i advokatundersøgelse	2021-32-2463
21.10.2022	Kritik af Region Hovedstaden for mangelfuld information til borgerne om databehandling og rettigheder	2021-432-0059
08.09.2022	Alvorlig kritik og påbud til Aarhus Kommune for behandling af elevoplysninger i Google Workspace	2021-432-0056
25.08.2022	Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	2021-431-0126
20.07.2022	Kritik af Region Syddanmark for mangelfuld kontrol med personoplysninger til forskning	2020-422-0026
15.07.2022	Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	2022-423-0261
14.07.2022	SIRIUS advokater politianmeldt og indstillet til bøde for manglende behandlingssikkerhed	
12.05.2022	Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	
26.04.2022	Indhentelse af samtykke ved indmeldelse i kundeklub var i overensstemmelse med GDPR	2021-31-5080
05.04.2022	Danske Bank indstilles til bøde for manglende sletning af personoplysninger	
31.03.2022	Tidligere arbejdsgiver kunne afvise at efterkomme anmodning om indsigt	2021-32-2438
29.03.2022	Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	2022-212-3529
07.02.2022	Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	2022-431-0167
31.01.2022	DBA's afslag på sletning af brugeroplysninger var berettiget af hensyn til bekæmpelse af svindel	2021-31-5439
26.01.2022	Alvorlig kritik af DBA for mangelfuld samtykkeløsning og besværlig tilbagetrækning	2020-431-0085
18.01.2022	Datatilsynets tilsyn med Region Nordjyllands administration af adgangskort	2021-422-0033

08.12.2021	Tryg Forsikring frifundet for kritik i sag om behandling af helbredsoplysninger	2020-31-3840
17.11.2021	Kritik af Gladsaxe Kommunes behandling af personoplysninger om hjemmesidebesøgende	2020-432-0047
20.10.2021	Alvorlig kritik af Alstrøm – Din Isenkræmmer ApS for ulovlig behandling af personoplysninger via cookies	2021-431-0125
10.09.2021	Alvorlig kritik og påbud til Helsingør Kommune i sag om Chromebooks og Google Workspace	2020-431-0061
08.09.2021	Region Midtjylland indstillet til bøde for manglende adgangsstyring af følsomme personoplysninger	
17.08.2021	Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	
16.07.2021	Region Syddanmark politianmeldes og indstilles til bøde på 500.000 kr. for alvorligt sikkerhedsbrud	
07.07.2021	Politianmeldelse og bødeindstilling af virksomhed for ulovlig behandling af oplysninger om strafbare forhold	
02.03.2021	Fødearestyrelsens overholdelse af databeskyttelsesreglerne i forbindelse med rekrutteringsprocesser	2019-421-0033
15.01.2021	Ingen kritik af Codan Forsikrings behandlingssikkerhed efter Datatilsynets planlagte tilsyn	2020-41-0063
15.01.2021	Datatilsynets tilsyn med behandlingssikkerheden hos Aleris Hamlet Hospitaler A/S	2020-41-0068
15.01.2021	Tilsyn med Udviklings- og Forenklingsstyrelsens behandlingssikkerhed fører ikke til kritik	2020-421-0078
15.01.2021	Datatilsynets kontrol af informationssikkerhed og risikostyring i Odense Kommune	2020-423-0231
08.12.2020	Ingen kritik af DJØF efter tilsyn med anmeldelse af brud på persondatasikkerheden	2019-41-0035
08.12.2020	Datatilsynets tilsyn med Ase Lønmodtager efter anmeldelse af brud på persondatasikkerheden	2019-41-0036
08.12.2020	Ingen kritik af Ankestyrelsens procedurer for anmeldelse af brud på persondatasikkerheden	2019-421-0029
08.12.2020	Datatilsynets tilsyn med Styrelsen for Patientklagers anmeldelse af brud på persondatasikkerheden	2019-421-0030
08.12.2020	Datatilsynets tilsyn med Bornholms Regionskommunes håndtering af brud på persondatasikkerheden	2019-423-0204
13.11.2020	Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	2020-31-3354
03.11.2020	Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	2019-32-0709
11.09.2020	Alvorlig kritik af Datatilsynet for manglende behandlingssikkerhed og underretning ved brud på persondatasikkerheden	2020-442-8866

18.06.2020	Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse	2019-31-2250
18.06.2020	Alvorlig kritik af testvirksomhed for brud på persondatasikkerheden ved videregivelse af opgavebesvarelser	2019-431-0045
18.05.2020	Alvorlig kritik af privat virksomhed for behandling uden gyldigt samtykke og manglende efterlevelse af sletteanmodning	2019-31-1950
20.12.2019	Alvorlig kritik af Arbejdsmarkedets Feriefond for mangelfuld oplysningspligt og ugyldigt samtykke	2019-32-0639
19.12.2019	Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	2019-442-3996
12.07.2019	Kritik af Politiklagemyndighedens håndtering af de registreredes rettigheder ved efterforskning	2018-813-0001

FORARBEJDE Betænkninger

4 referencer

Straffelovrådets betænkning om freds- og ærekrænkelser

nr. 1563 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 1)

nr. 1565 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 2)

nr. 1565 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – Betænkning nr. 1565, Del II: Bilag med vurderinger af særlovgivning på de enkelte ministerområder

nr. 1565 · 2017 · Justitsministeriet

06

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over datatilsynsbøder og GDPR-overtrædelser (databrud)

Fra Datatilsynets bødeindstilling til domstolenes bødeudmåling efter artikel 83

Version 2 · Opdateret 15. jul. 2026 · 58 afgørelser · 2010-2026

[Læs online](#)**INTRODUKTION**

Danmark har som et af ganske få EU-lande udnyttet databeskyttelsesforordningens artikel 83, stk. 9, til at erstatte de administrative bøder med strafferetlige bøder, der pålægges af domstolene efter politianmeldelse fra Datatilsynet. Praksis falder derfor i to spor: Datatilsynets bødeindstillinger – typisk for manglende sletning (art. 5, stk. 1, litra e), utilstrækkelig behandlingssikkerhed (art. 32) og manglende anmeldelse af databrud (art. 33) – og domstolenes efterfølgende prøvelse, hvor bøderne gennemgående ender markant under det indstillede niveau. Oversigten samler Datatilsynets bødeindstillinger fra Taxa 4x35 (2019) til Privathospitalet Capio (2024), byrettens og landsretternes bødeudmåling, EU-Domstolens rammer for bødeansvaret (bl.a. C-807/21 og den danske forelæggelse i C-383/23) og Højesterets praksis om godtgørelse efter artikel 82.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Danmark har udnyttet databeskyttelsesforordningens artikel 83, stk. 9: bøder for GDPR-overtrædelser er STRAFFERETLIGE og pålægges af domstolene efter politianmeldelse fra Datatilsynet – Datatilsynet kan ikke selv udstede administrative bøder.
- 02** Datatilsynets bødeindstilling er alene en indstilling; retten er ikke bundet af den, og i praksis udmåles bøderne markant lavere – i taxisagen 100.000 kr. mod en indstilling på 1,2-1,3 mio. kr.
- 03** Databeskyttelsesforordningens artikel 83, stk. 2, SKAL følges ved bødeudmålingen, jf. databeskyttelseslovens § 41, stk. 3, og suppleres af straffelovens §§ 80-82.
- 04** Lang sagsbehandlingstid er den hyppigste og mest virkningsfulde nedsættelsesgrund, jf. straffelovens § 82, stk. 1, nr. 13 – i taxisagen nedsatte retten bøden med 2/3.
- 05** Offentlige myndigheder kan straffes for GDPR-overtrædelser uanset straffelovens § 27, stk. 2, jf. databeskyttelseslovens § 41, stk. 6, 2. pkt.; bødeniveauet er dog lavere end for private og fastsættes bl.a. efter indbyggertal og driftsbevilling.

- 06** Manglende logning vender bevisbyrden imod den dataansvarlige: at det ikke KAN konstateres, om uvedkommende har tilgået oplysningerne, er ikke formildende, men følger af den dataansvarliges egen forsømmelse.
- 07** Tekniske og økonomiske vanskeligheder i ældre it-systemer fritager ikke – IT-arkitekturen skal indrettes efter databeskyttelsesreglerne, ikke omvendt.
- 08** Et telefonnummer er en personoplysning; sletning af navnet alene udgør ikke anonymisering.
- 09** Ved manglende flerfaktorauf autentifikation på internetvendte systemer med følsomme oplysninger er sikkerhedsniveauet efter Datatilsynets faste praksis ikke passende efter artikel 32.
- 10** Kryptering af udtagelige lagringsmedier (USB-stik) med personoplysninger anses for en nødvendig og påkrævet sikkerhedsforanstaltning.
- 11** 72-timers-fristen i artikel 33 er selvstændigt sanktioneret – også Datatilsynet selv har fået alvorlig kritik for at overskride den.
- 12** Efter EU-Domstolens dom i C-807/21 forudsætter en bøde til en juridisk person, at overtrædelser er begået forsætligt eller uagtsomt; ansvaret er direkte og forudsætter ikke, at en identificeret fysisk person har handlet.
- 13** Efter EU-Domstolens dom i C-383/23 (dansk forelæggelse) beregnes bødeløftet i artikel 83, stk. 4-6, af HELE virksomhedens (koncernens) globale årsomsætning, mens selve bødens størrelse fastsættes efter kriterierne i artikel 83, stk. 2.
- 14** Tilsynsmyndigheden har efter C-768/21 ikke pligt til at pålægge en sanktion ved ethvert konstateret brud, når det ikke er nødvendigt for at bringe overtrædelser til ophør.
- 15** Et databrud udløser ikke automatisk godtgørelse efter artikel 82 – den registrerede skal godtgøre faktisk immateriel skade, og Højesteret frifandt i december 2025 Gladsaxe Kommune for godtgørelseskrav efter tyveri af en bærbar computer.
- 16** Sager om GDPR-overtrædelser må efter Rigsadvokatmeddelelsen ikke afgøres med bødeforelæg, før bødeniveauet er tilstrækkeligt afklaret i retspraksis, og tiltaleespørgsmålet skal altid forelægges statsadvokaten.

Den danske særordning: strafferetlige bøder i stedet for administrative bøder

§ 1

Databeskyttelsesforordningen bygger som udgangspunkt på, at tilsynsmyndigheden selv pålægger *administrative* bøder. [Artikel 83, stk. 9](#) åbner imidlertid for, at medlemsstater, hvis retssystem ikke kender administrative bøder, i stedet kan anvende strafferetlige bøder pålagt af de kompetente nationale domstole. Danmark har udnyttet denne mulighed.

Hjemlen findes i [databeskyttelseslovens § 41, stk. 1](#) og [stk. 2](#), hvorefter overtrædelser af forordningens centrale forpligtelser straffes »med bøde eller fængsel indtil 6 måneder«. Konsekvensen er, at **Datatilsynet ikke selv kan udstede en bøde** – tilsynet kan alene politianmelde og *indstille* til en bøde, hvorefter anklagemyndigheden rejser tiltale, og domstolen udmåler straffen.

De centrale rammebestemmelser er:

Bestemmelse	Indhold
§ 41, stk. 1	Straf for overtrædelse af bl.a. art. 8, 11, 25-39, 42-43 (svarende til art. 83, stk. 4) og art. 5-7, 9 samt 12-22 (art. 83, stk. 5)
§ 41, stk. 3	»Databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålæggelse af straf efter stk. 1 og 2«
§ 41, stk. 6	Juridiske personer kan straffes; offentlige myndigheder kan straffes uanset straffelovens § 27, stk. 2
§ 41, stk. 7	Forældelsesfristen er 5 år
§ 42	Datatilsynet kan udstede bødeforelæg, hvis den pågældende erklærer sig skyldig
§ 30, stk. 2	Datatilsynet kan indbringe spørgsmål om overtrædelser for retten i den borgerlige retsplejes former

Lovgivers hensigt fremgår tydeligt af de specielle bemærkninger til § 41 i lovforslaget til databeskyttelsesloven:

»Det er med lovforslaget forudsat, at bødeniveauet i de to første kategorier, som gennemfører forordningens krav efter artikel 83 om kriminalisering, forhøjes væsentligt i forhold til det nuværende bødeniveau efter persondataloven.«

Om strafansvaret for det offentlige hedder det:

»Forslaget indebærer, at sådanne offentlige myndigheder mv. – i lighed med private aktører – kan straffes for de overtrædelser, som er kriminaliseret i medfør af de foreslåede stk. 1, 2, 4 og 5. Dette gælder, både når en sådan offentlig myndighed mv. udøver virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private, og når myndigheden mv. udøver offentlig myndighed.«

Bemærkningerne præciserer samtidig, at **domstolene ikke** er omfattet af § 41, stk. 6, 2. pkt., og derfor kun kan straffes efter straffelovens § 27, stk. 2. Det retspolitiske grundlag for ordningen er analyseret indgående i **Betænkning nr. 1565/2017 om databeskyttelsesforordningen og de retlige rammer for dansk lovgivning** (Justitsministeriet).

Bødelofterne følger direkte af forordningen: [artikel 83, stk. 4](#) (10 mio. EUR eller 2 % af den samlede globale årlige omsætning) og [artikel 83, stk. 5](#) (20 mio. EUR eller 4 %). Efter [artikel 83, stk. 3](#) må den samlede bøde ved flere overtrædelser i forbundne behandlingsaktiviteter ikke overstige beløbet for den alvorligste overtrædelse.

LOV

[Databeskyttelsesloven § 30, stk. 2](#)

[Databeskyttelsesloven § 41, stk. 1-3, 6, 7](#)

[Databeskyttelsesloven § 42](#)

[Straffeloven § 27, stk. 2](#)

§ 2 Datatilsynets bødeindstillinger til private virksomheder – fra Taxa 4x35 til Capio

Den første danske bødeindstilling mod en privat virksomhed efter forordningen kom i [Taxa 4x35-sagen](#) af 25. marts 2019. Ved et tilsynsbesøg konstaterede Datatilsynet, at selskabet slettede kundens navn efter to år, men bevarede telefonnummeret i fem år – med det resultat, at **8.873.333 personhenførbare taxature** var opbevaret ud over den nødvendige periode. Selskabet gjorde gældende, at telefonnummeret alene fungerede som teknisk nøgle, og at data var anonymiseret, når navnet var slettet. Datatilsynet afviste dette fuldstændigt: et telefonnummer er en personoplysning, og sletning af navnet er ikke anonymisering. Direktør Cristina Angela Gulisano udtalte:

»Når vi har valgt at indstille til en bøde i denne sag, skyldes det, at der er tale om meget store mængder personoplysninger, der er blevet gemt uden et sagligt formål. Ét af grundprincipperne på databeskyttelsesområdet er, at man kun må behandle oplysninger, man har brug for - og når man ikke har brug for dem længere, skal de slettes med det samme.«

Samme spor følges i [IDdesign-sagen](#) (3. juni 2019), hvor Datatilsynet udtalte alvorlig kritik og indstillede møbelvirksomheden til bøde for overtrædelse af opbevaringsbegrænsningen i [artikel 5, stk. 1, litra e](#), sammenholdt med opbevaringspligten i bogføringslovens § 10, og i [Arp-Hansen Hotel Group-sagen](#) (28. juli 2020), hvor ca. **500.000 gæsteprofiler** var bevaret langt ud over selskabets egne slettefrister. Bøden blev indstillet til 1.100.000 kr. Datatilsynet afviste her udtrykkeligt, at tekniske udfordringer og igangværende systemmodernisering kan fritage for compliance:

»Det er et grundlæggende princip i databeskyttelsesreglerne, at man kun må behandle oplysninger, man har brug for – og når man ikke har brug for dem længere, skal de slettes med det samme.«

En oversigt over de centrale bødeindstillinger mod private aktører:

Sag	Dato	Indstillet bøde	Overtrådt bestemmelse	Kerneforhold
Taxa 4x35	25.03.2019	1,2 mio. kr.	art. 5(1)(e)	8,87 mio. taxature, telefonnr. gemt i 5 år
IDdesign	03.06.2019	Bødeindstilling	art. 5(1)(e), art. 83(4)	Kundeoplysninger ikke slettet
JobTeam	15.05.2020	Bødeindstilling	art. 15, art. 31	Manglende samarbejde med tilsynet + tilsidesat indsigtret
Arp-Hansen Hotel Group	28.07.2020	1,1 mio. kr.	art. 5(1)(e), art. 25	~500.000 gæsteprofiler
PrivatBo	04.08.2020	150.000 kr.	art. 32(1)	CPR-numre på 1.180 beboere videregivet ved fejl
Medicals Nordic	09.07.2021	Bødeindstilling	art. 32(1)	Covid-testresultater sendt via WhatsApp-grupper
Danske Bank	05.04.2022	Bødeindstilling	art. 5(1)(e), art. 5(2)	Manglende sletning
Privathospitalet Capio	01.02.2024	1,5 mio. kr.	art. 32(1)	IDOR-sårbarhed i patientportal + intet databehandlertilsyn

Capio-sagen markerer det hidtil højeste indstillede niveau. Sårbarheden bestod i, at uvedkommende kunne tilgå tredjemands helbredsoplysninger blot ved at ændre URL-adressen efter log-ind, fordi systemet manglede

autorisationskontrol. Hertil kom, at privathospitalet – der selv fungerer som databehandler for flere regioner – i adskillige år **ikke havde ført tilsyn med sine egne databehandlere**. Skærpende momenter var sårbarhedens fundamentale karakter, det store antal registrerede, de særlige kategorier af oplysninger og virksomhedens omsætning.

I [Medicals Nordic-sagen](#) blev der oprettet én WhatsApp-gruppe pr. testcenter, hvor alle medarbejdere automatisk blev inviteret – også uden arbejdsbetinget behov – og hvor fratrådte medarbejdere ikke blev fjernet. Personnumre og testresultater blev transmitteret i grupperne uden forudgående risikovurdering.

LOV	Databeskyttelsesloven § 11, stk. 1	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Danske Bank indstilles til bøde for manglende sletning af personoplysninger	05.04.2022
	Datatilsynet · Politianmeldelse og bødeindstilling til Medicals Nordic I/S for mangelfuld behandlingssikkerhed	09.07.2021
	Datatilsynet · PrivatBo indstillet til bøde efter utilsigtet videregivelse af personoplysninger på over 1.000 beboere	04.08.2020
	Datatilsynet · Arp-Hansen Hotel Group indstillet til bøde for manglende sletning af gæsteprofiler	28.07.2020
	Datatilsynet · JobTeam politianmeldt og indstillet til bøde for manglende samarbejde og tilsidesættelse af indsigtsret	15.05.2020
	Datatilsynet · Alvorlig kritik og bødeindstilling til IDdesign for overtrædelse af princippet om opbevaringsbegrænsning	03.06.2019
	Datatilsynet · Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.	25.03.2019

§ 3 Bødeindstillinger til offentlige myndigheder – kommuner, regioner og statslige styrelser

Adgangen til at straffe offentlige myndigheder er en nyskabelse i forhold til persondataloven og hviler på [databeskyttelseslovens § 41, stk. 6, 2. pkt.](#), jf. [artikel 83, stk. 7](#). Datatilsynet har siden 2021 politianmeldt og indstillet en række myndigheder til bøde:

Myndighed	Dato	Indstillet bøde	Kerneforhold
Vejle Kommune	16.06.2021	Bødeindstilling	Brud på persondatasikkerheden
Udlændingestyrelsen	17.08.2021	50.000 kr.	SALTO-systemet: ingen logning, ingen adgangskontrol, tabt data ved nedbrud
Favrskov Kommune	16.09.2021	Bødeindstilling	Læk af følsomme oplysninger på kommunens hjemmeside
Region Syddanmark	17.09.2021	500.000 kr.	Brud på behandlingssikkerheden
Civilstyrelsen	12.05.2022	100.000 kr.	Ukrypteret USB-stik med 800+ sider følsomme oplysninger bortkom + ingen anmeldelse
Hvidovre Kommune	22.01.2024	Politianmeldelse	Utilstrækkelig sikkerhed ved behandling af børneoplysninger

Lyngby-Taarbæk Kommune	27.11.2024	350.000-400.000 kr.	Ingen MFA; 1.000+ fratrådte havde stadig adgang; ~42.000 berørte
------------------------	------------	---------------------	--

Udlændingestyrelsen-sagen er principiel, fordi oplysningerne indgik i straffesagskæden: manglende registreringer i SALTO-systemet på Udrejsecenter Kærshovedgård førte til fejlbehæftet sagsbehandling, herunder nedsættelse af ydelser og politianmeldelser af beboere. Datatilsynet formulerede en generel standard:

»Det er Datatilsynets opfattelse, at det ved oplysninger og registreringer, der indgår i straffesagskæden eller benyttes til kontrolforanstaltninger, som er underlagt sanktioner, skal sikres at der dels sker logning af alle aktiviteter, dels foretages en sikkerhedskopiering, med sådanne intervaller, at data ikke tabes ved nedbrud.«

Civilstyrelsen-sagen fastslår, at kryptering af udtagelige lagringsmedier »må anses for at være en nødvendig og påkrævet sikkerhedsforanstaltning«. Sagen indeholdt to selvstændige overtrædelser: den manglende kryptering (art. 32) og den manglende anmeldelse af bruddet (art. 33).

Lyngby-Taarbæk-sagen viser Datatilsynets skærpede linje over for manglende flerfaktoraутentifikation:

»Når man giver medarbejderne adgang til it-systemer med personoplysninger direkte fra internettet, øges risikoen for, at uvedkommende – f.eks. hackere – får adgang til oplysningerne og kan misbruge dem. Hvis der gives adgang til beskyttelsesværdige oplysninger, har det længe været et krav, at der skal være implementeret flerfaktoraутentifikation for at sikre et passende beskyttelsesniveau.«

Ved sanktionsvurderingen indgår **kommunens størrelse, indbyggertal og samlede driftsbevilling** – et selvstændigt udmålingsprincip for det offentlige, der sikrer, at bøden er effektiv, proportional og afskrækkende uden at ramme borgerne uforholdsmæssigt.

Hvor overtrædelser helt eller delvis ligger før 25. maj 2018, kan bøde ikke pålægges. Det ses i [Region Syddanmark-sagen om restjournalplatformen](#), hvor ca. **800.000 personers** dokumenter siden 2013 havde ligget på et netværksdrev tilgængeligt for regionens ca. 30.000 ansatte uden logning. Datatilsynet udtalte alvorlig kritik og bemærkede udtrykkeligt, at forholdet »normalt ville kunne give anledning til bødestraf, hvis hele forseelsen havde fundet sted efter GDPR's ikrafttræden«.

LOV	Databeskyttelsesloven § 41, stk. 1, 6	
PRAKSIS	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024
	Datatilsynet · Politianmeldelse af Hvidovre Kommune for utilstrækkelig sikkerhed ved behandling af børneoplysninger	22.01.2024
	Datatilsynet · Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	12.05.2022
	Datatilsynet · Region Syddanmark politianmeldt og indstillet til bøde på 500.000 kr. for brud på behandlingssikkerheden	17.09.2021
	Datatilsynet · Favrskov Kommune indstilles til bøde efter læk af følsomme oplysninger på hjemmeside	16.09.2021
	Datatilsynet · Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	17.08.2021
	Datatilsynet · Vejle Kommune politianmeldes og indstilles til bøde for brud på persondatasikkerheden	16.06.2021
	Datatilsynet · Alvorlig kritik og påbud til Region Syddanmark for utilstrækkelig sikkerhed og manglende underretning	12.06.2020

§ 4 Domstolenes prøvelse: bøderne bliver markant lavere end indstillet

Det mest markante mønster i dansk GDPR-praksis er **afstanden mellem Datatilsynets bødeindstilling og domstolenes faktiske udmåling**.

Det klareste eksempel er [taxisagen](#) (Retten på Frederiksberg, 6. januar 2023). Datatilsynet havde oprindeligt indstillet **1.200.000 kr.**, justeret efter WhatsApp-afgørelsen til et spænd på 1,2-1,4 mio. kr., og ved domsafsigelsen nedlagde anklagemyndigheden påstand om **1,2-1,3 mio. kr.** ud fra selskabets omsætning på ca. 62 mio. kr.

Retten nåede et helt andet resultat. For det første fandt retten det **ikke bevist**, at selskabet havde anvendt oplysningerne til produkt- og forretningsudvikling eller opnået en økonomisk fordel:

»Retten finder herefter ikke, at det er bevist, at Tiltalte har opbevaret telefonnumrene og opsamlingsadresserne som led i produkt- og forretningsudvikling på en måde, hvorved de har haft en økonomisk fordel eller har undgået et tab.«

Overtrædelser blev derfor alene tilregnet selskabet som **uagtsom**. Retten tog udgangspunkt i en normalbøde i den nederste del af spændet – ca. **300.000 kr.** – og nedsatte den herefter med 2/3 til **100.000 kr.** under henvisning til den meget lange sagsbehandlingstid, jf. [straffelovens § 82, stk. 1, nr. 13](#) og stk. 2.

Samme mønster ses i de øvrige domme:

Sag	Instans	Dato	Resultat
SS-3662/2020-ARH	Retten i Aarhus	12.02.2021	Dom for manglende sletning (tilståelsessag)
SS-792/2021-BOR	Byretten	20.01.2022	Virksomhed dømt for uretmæssig videregivelse om tidligere ansat
SS-1471/2021-LYN	Retten i Lyngby	11.02.2022	Overtrædelse ved opbevaring af personoplysninger; straffelovens § 83 anvendt
SS-8331/2020-ROS	Retten i Roskilde	09.03.2022	Kommune: bøde 50.000 kr. (art. 32)
SS-17029/2021-KBH	Københavns Byret	05.04.2022	Fysisk person: bøde 25.000 kr. (påstand 35.000 kr.)
SS-5405/2020-FRB	Retten på Frederiksberg	06.01.2023	Bøde 100.000 kr. (påstand 1,2-1,3 mio. kr.)
SS-1980/2023-HJO	Byretten	06.12.2024	Bøde 120.000 kr. (nedsat fra 150.000 kr.)
SS-715/2024-VLR	Vestre Landsret	27.03.2025	Vejle Kommune: bøde forhøjet til 100.000 kr.
S-185-23	Landsretten	28.04.2025	Bøde nedsat pga. lang sagsbehandlingstid

Bødeniveauet for danske GDPR-domme ligger dermed reelt i intervallet **25.000-120.000 kr.** for de sager, der er nået til dom – ganske uafhængigt af, at forordningens lofter er 10 hhv. 20 mio. EUR. Historisk perspektiv giver [Vestre Landsrets dom af 27. oktober 2011](#) om ulovlig opbevaring af kundedata under den tidligere persondatalov – det er netop dette lave niveau, lovgiver med databeskyttelsesloven ville hæve »væsentligt«.

Vestre Landsrets dom i **Vejle Kommune-sagen** er den eneste fundne afgørelse, hvor bøden er blevet **forhøjet** ved anken – til 100.000 kr. Sagen angik videregivelse af beskyttede adresseoplysninger i den kommunale tandpleje, og gerningsperioden var i anklageskriftet begrænset til juli 2018 – 9. januar 2019.

LOV	Databeskyttelsesloven § 41, stk. 1	Straffeloven § 82, stk. 1	Straffeloven § 83
PRAKSIS			
	Landsretten · Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid		28.04.2025
	Landsretten · Vejle Kommune dømt for brud på databeskyttelsesforordningen – bøde forhøjet til 100.000 kr.		27.03.2025
	Landsretten · Virksomhed dømt for alvorlig overtrædelse af Databeskyttelsesloven: Bøde for ulovlig opbevaring af kundedata		27.10.2011
	Byretten · Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb		06.12.2024
	Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture		06.01.2023
	Byretten · Dom for overtrædelse af databeskyttelsesregler og navneforbud		05.04.2022
	Byretten · Kommune idømt bøde på 50.000 kr. for brud på GDPR ved manglende adgangskontrol til følsomme personoplysninger		09.03.2022
	Byretten · Retten i Lyngby: Afgørelse om overtrædelse af Databeskyttelsesforordningen vedrørende opbevaring af personoplysninger		11.02.2022
	Byretten · Virksomhed dømt for uretmæssig videregivelse af personoplysninger om tidligere ansat		20.01.2022
	Byretten · Dom for overtrædelse af databeskyttelsesforordningen ved manglende sletning af personoplysninger		12.02.2021

§ 5 Artikel 32 – hvad kræver »passende sikkerhed«?

[Artikel 32, stk. 1](#) er den hyppigste hjemmel i danske bødesager. Datatilsynet har i en række tilsyn formuleret en gennemgående standard:

»Det er Datatilsynets opfattelse, at kravet i artikel 32 om passende sikkerhed normalt vil indebære, at den dataansvarlige skal sikre, at oplysninger om registrerede, herunder særligt fortrolige og følsomme personoplysninger, ikke kommer uvedkommende til kendskab, og at den dataansvarlige i den forbindelse bl.a. skal sikre sig, at alle medarbejdere i organisationen i nødvendigt omfang er bekendt med eventuelle interne procedurer for håndtering af personoplysninger [...] og at procedurer, retningslinjer, arbejdsgange, tekniske sikkerhedsforanstaltninger mv. løbende opdateres eller indføres, herunder som følge af konstaterede brud på persondatasikkerheden.«

Standarden er gentaget i tilsynene med [Spar Nord Bank](#), [Nykredit](#) og [Sydbank](#) (alle 31. august 2023), hvor ingen af bankerne fik kritik – bl.a. fordi de kunne dokumentere dataklassifikation, TLS-kryptering, Data Loss Prevention-løsninger, statistisk analyse af gentagne brudtyper og obligatorisk awareness-træning.

Fire tilbagevendende **mangeltyper** udløser kritik eller bøde:

- **Manglende adgangskontrol.** I [Roskilde-sagen](#) lå 135 indstillingsskemaer med følsomme oplysninger om **452 borgere, heraf 402 mindreårige**, på en medarbejderportal, hvor alle kommunens medarbejdere teoretisk havde adgang. Reelt skønnedes 500-800 medarbejdere at have praktisk adgang.
- **Manglende logging.** Retten i Roskilde afviste udtrykkeligt, at den manglende dokumentation for misbrug kunne virke formildende:

»Det findes ikke at kunne føre til et andet resultat, at det ikke har kunnet konstateres, at oplysningerne reelt er blevet tilgået af uvedkommende, idet dette skyldes, at kommunen ikke loggede adgangen til medarbejderportalens, mens den blev anvendt til sagsbehandling.«

- **Manglende flerfaktoraутентifikation** ved internetvendte systemer, jf. [Lyngby-Taarbæk-sagen](#).
- **Manglende tilsyn med databehandlere**, jf. [Capio-sagen](#), hvor tre stikprøvevis udvalgte databehandlere ikke havde været underlagt tilsyn i adskillige år.

Datatilsynet har herudover udtalt alvorlig kritik af [utilstrækkelig sikkerhed omkring børns personoplysninger](#) (25. august 2022) og har meddelt [Aalborg Kommune påbud om systemoverblik og sletning](#) (5. maj 2026). Modsat viser tilsynene med [Salling Group](#), Udviklings- og Forenklingsstyrelsen og Odense Kommune (alle 15. januar 2021), at en dokumenteret risikobaseret tilgang, ISO 27001-forankring og fungerende beredskabsprocedurer normalt fører til, at sagen afsluttes uden kritik.

Et gennemgående princip er, at **it-arkitekturen skal indrettes efter reglerne – ikke omvendt**. I taxisagen bemærkede Datatilsynet, at det ikke er acceptabelt at fastsætte slettefrister tre år længere end nødvendigt, blot fordi det er teknisk besværligt at efterleve loven. Samme afvisning af »tekniske begrænsninger« findes i Arp-Hansen- og Udlændingestyrelsen-sagerne.

LOV	Databeskyttelsesloven § 41, stk. 1	
PRAKSIS	Byretten · Kommune idømt bøde på 50.000 kr. for brud på GDPR ved manglende adgangskontrol til følsomme personoplysninger	09.03.2022
	Datatilsynet · Datatilsynet meddeler Aalborg Kommune påbud om systemoverblik og sletning af personoplysninger	05.05.2026
	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Ingen kritik af privat virksomhed for anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	25.08.2022
	Datatilsynet · Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	17.08.2021
	Datatilsynet · Datatilsynets tilsyn med Salling Group A/S vedrørende it-sikkerhed og rettighedsstyring	15.01.2021
	Datatilsynet · Tilsyn med Udviklings- og Forenklingsstyrelsens behandlingssikkerhed fører ikke til kritik	15.01.2021
	Datatilsynet · Datatilsynets kontrol af informationssikkerhed og risikostyring i Odense Kommune	15.01.2021
	Datatilsynet · Arp-Hansen Hotel Group indstillet til bøde for manglende sletning af gæsteprofiler	28.07.2020
	Datatilsynet · Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.	25.03.2019

Artikel 33 og 34 – 72-timers-fristen og underretning af de registrerede

Efter [artikel 33, stk. 1](#) skal den dataansvarlige anmelde et brud på persondatasikkerheden til Datatilsynet »uden unødigt forsinkelse og om muligt senest 72 timer«, medmindre det er **usandsynligt**, at bruddet indebærer en risiko for fysiske personers rettigheder. Efter [artikel 33, stk. 5](#) skal **alle** brud dokumenteres – også de ikke-anmeldelsespligtige.

Den mest pædagogiske afgørelse om fristen er Datatilsynets **alvorlige kritik af sig selv** (11. september 2020). Ved en flytning blev en almindelig affaldsbeholder ved en misforståelse markeret som makuleringsbeholder, og fortrolige dokumenter blev i ca. seks måneder bortskaffet som almindeligt papiraffald. Bruddet blev konstateret 5. august 2020, men først anmeldt 10. august 2020 – efter fristens udløb. Datarådet udtalte alvorlig kritik og lagde vægt på tilsynets særlige stilling:

»Datatilsynet har i den forbindelse lagt vægt på, at tilsynet – som tilsynsmyndighed på databeskyttelsesområdet – har en særlig forpligtelse til at iagttage og overholde krav, der følger af myndighedens eget ansvarsområde.«

Manglende anmeldelse indgår også som **selvstændig overtrædelse** i bødeindstillingerne: i [Civilstyrelsen-sagen](#) blev det bortkomne USB-stik konstateret 26. august 2020, men aldrig anmeldt – hvilket sammen med den manglende kryptering udløste bødeindstillingen på 100.000 kr.

[Artikel 34](#) om underretning af de registrerede aktualiseres, når bruddet indebærer **høj risiko**. Region Syddanmark forsøgte i [restjournalsagen](#) at undlade underretning med henvisning til, at platformen kun var internt tilgængelig, at det krævede it-kundskab at finde dokumenterne, og at alle ansatte havde tavshedspligt. Datatilsynet afviste og meddelte påbud efter [artikel 58, stk. 2, litra e](#):

»Generelt kan det – hvis man har mistet kontrollen over om oplysningers fortrolighed er kompromitteret – ikke ved at få stoppet den pågældende sårbarhed, siges at risikoen for misbrug af de oplysninger der måtte være tilgængelige, er blevet mindre.«

Efterfølgende afhjælpning fjerner altså ikke den **historiske** risiko. Er individuel underretning umulig eller uforholdsmæssigt byrdefuld, kan der ske offentlig meddelelse efter [artikel 34, stk. 3, litra c](#) – som Datatilsynet selv gjorde i sin egen sag ved at offentliggøre nyheder om bruddet på hjemmesiden.

Omvendt viser tilsynsrækken fra 2020 og 2023, at et **højt antal anmeldelser ikke i sig selv er kritisabelt**. I tilsynene med bankerne bemærkede Datatilsynet udtrykkeligt, at et højere antal anmeldelser lige så vel kan være udtryk for et større internt fokus og en mere stringent anmeldelsespraksis. Tilsvarende blev der ikke udtalt kritik af [DJØF](#) efter en gennemgang af 15 registrerede hændelser, som foreningen selv havde vurderet ikke-anmeldelsespligtige, eller af [AROS Privathospital](#):

»Henset til, at AROS Privathospital Partnerselskab i den pågældende periode ikke har registreret brud på persondatasikkerheden, og idet tilsynet ikke har fundet indikationer på, at dette skulle være sket, har Datatilsynet fundet, at privathospitalet har iværksat de foranstaltninger, der er nødvendige for at kunne overholde kravene i databeskyttelsesforordningens artikel 33, stk. 1.«

Sen anmeldelse er derimod kritisabel, jf. [Datatilsynets alvorlige kritik af Region Syddanmark for manglende adgangsstyring og sen anmeldelse](#) (17. juli 2020).

LOV [Databeskyttelsesloven § 41, stk. 1](#)

PRAKSIS	Datatilsynet · Ingen kritik af privat virksomhed for anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden	31.08.2023

Datatilsynet · Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden	31.08.2023
Datatilsynet · Tilsyn med procedurer for anmeldelse af brud på persondatasikkerheden hos privat virksomhed	31.08.2023
Datatilsynet · Rettidig anmeldelse af brud på persondatasikkerheden hos en privat virksomhed	31.08.2023
Datatilsynet · Tilsyn med offentlig myndigheds overholdelse af regler om anmeldelse af brud på persondatasikkerheden	31.08.2023
Datatilsynet · Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	12.05.2022
Datatilsynet · Datatilsynet finder ingen grund til kritik af Region Syddanmarks håndtering af sikkerhedsbrud	08.12.2020
Datatilsynet · Ingen kritik af DJØF efter tilsyn med anmeldelse af brud på persondatasikkerheden	08.12.2020
Datatilsynet · Manglende grundlag for kritik af AROS Privathospital efter anmeldelse af sikkerhedsbrud	08.12.2020
Datatilsynet · Alvorlig kritik af Datatilsynet for manglende behandlingssikkerhed og underretning ved brud på persondatasikkerheden	11.09.2020
Datatilsynet · Alvorlig kritik af Region Syddanmark for manglende adgangsstyring og sen anmeldelse af sikkerhedsbrud	17.07.2020
Datatilsynet · Alvorlig kritik og påbud til Region Syddanmark for utilstrækkelig sikkerhed og manglende underretning	12.06.2020

Bødeudmålingen efter artikel 83, stk. 2 – skærpende og formildende momenter

§ 7

Databeskyttelseslovens § 41, stk. 3 gør artikel 83, stk. 2 **obligatorisk** ved bødeudmålingen.

Rigsadvokatmeddelelsen om databeskyttelse i straffesager, pkt. 5.1.2, opregner momenterne og præciserer, at:

»Opremsningen er ikke udtømmende og suppleres af de almindelige bestemmelser i straffelovens §§ 80-82.«

De momenter, der i praksis vejer tungest, kan grupperes således:

Skærpende:

- **Antal berørte registrerede** – 8,87 mio. taxature (Taxa 4x35), ca. 500.000 gæsteprofiler (Arp-Hansen), ca. 800.000 personer (Region Syddanmark), ca. 42.000 (Lyngby-Taarbæk).
- **Oplysningernes karakter** – særlige kategorier efter art. 9 (helbred), oplysninger om strafbare forhold, CPR-numre og oplysninger om børn. I Roskilde-sagen lagde retten vægt på, at 402 af 452 berørte var **mindreårige**.
- **Overtrædelsens varighed** – Lyngby-Taarbæk-manglerne havde bestået siden hhv. 2016 og 2018.
- **Grundlæggende karakter af den svigtende foranstaltning** – Capio-sårbarheden »burde være opdaget i forbindelse med test«.
- **Tidligere påtaler om samme forhold**, jf. art. 83, stk. 2, litra e og i.
- **Forsæt** – i [SS-1980/2023-HJO](#) lagde retten vægt på, at videregivelsen skete **forsætligt** og til flere kunder, jf. forordningens præambelbetragtning 150 og 151.
- **Virksomhedens omsætning** – der indgår for at sikre en afskrækkende virkning; for myndigheder anvendes i stedet indbyggertal og driftsbevilling.

Formildende:

- **Uagtsom (frem for forsætlig) tilregnelse** – afgørende i taxisagen.
- **Samarbejde med tilsynet og efterfølgende afhjælpning**, jf. art. 83, stk. 2, litra c og f.
- **Egen anmeldelse af bruddet**, jf. art. 83, stk. 2, litra h.
- **Manglende økonomisk fordel** – retten fandt i taxisagen netop ikke bevist, at selskabet havde »haft en økonomisk fordel eller har undgået et tab«.
- **Lang sagsbehandlingstid** (se næste afsnit).

I [SS-1980/2023-HJO](#) – hvor et revisionsselskab havde sendt e-mail til sine kunder om, at en tidligere medarbejder havde begået underslæb – fastsatte retten bøden ud fra selskabets nettoomsætning (5.437.000 kr.), oplysningernes karakter (strafbare forhold, jf. [databeskyttelseslovens § 8, stk. 4](#)), skaden for den forurettede og forsættet. Retten fandt, at interesseafvejningen i § 8 ikke var opfyldt:

»Retten finder efter en samlet vurdering af sagen, at videregivelsen af oplysningerne om Forurettedes private forhold ikke var nødvendige for at varetage Tiltalte ApS' legitime interesse i at orientere kunderne om, at Forurettede ikke længere var ansat.«

For **fysiske personer** ligger niveauet lavere og justeres efter indkomstforhold. I [SS-17029/2021-KBH](#) – hvor en privatperson på Facebook havde offentliggjort navne og billeder på to sigtede i en drabssag i strid med [artikel 10](#) og et navneforbud – nedsatte retten bøden fra anklagemyndighedens påstand på 35.000 kr. til **25.000 kr.** under hensyn til, at tiltalte var hjemløs og modtog 6.100 kr. om måneden.

LOV

[Databeskyttelsesloven § 8, stk. 4](#)[Databeskyttelsesloven § 41, stk. 3](#)[Straffeloven § 80](#)[Straffeloven § 82, stk. 1](#)

PRAKSIS	Byretten · Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb	06.12.2024
	Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture	06.01.2023
	Byretten · Dom for overtrædelse af databeskyttelsesregler og navneforbud	05.04.2022
	Byretten · Kommune idømt bøde på 50.000 kr. for brud på GDPR ved manglende adgangskontrol til følsomme personoplysninger	09.03.2022
	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Arp-Hansen Hotel Group indstillet til bøde for manglende sletning af gæsteprofiler	28.07.2020
	Datatilsynet · Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.	25.03.2019

§ 8 Lang sagsbehandlingstid som den dominerende nedsættelsesgrund

Ingen enkeltfaktor har haft større betydning for det faktiske bødeniveau end **sagsbehandlingstiden**. Kæden fra brud → Datatilsynets tilsyn/afgørelse → politianmeldelse → efterforskning → tiltale → dom er lang, og domstolene lader systematisk forsinkelsen komme den tiltalte til gode efter [straffelovens § 82, stk. 1, nr. 13](#).

I [taxisagen](#) – tilsyn 3. oktober 2018, dom 6. januar 2023 – udtalte Retten på Frederiksberg:

»Retten finder på denne baggrund, at straffen bør nedsættes med 2/3 til 100.000 kr., jf. straffelovens § 82, stk. 1, nr. 13 og stk. 2.«

I [SS-1980/2023-HJO](#) blev bøden nedsat fra 150.000 kr. til 120.000 kr., og retten redegjorde detaljeret for forløbet:

»Retten har nedsat bøden fra 150.000 kr. til 120.000 kr. som følge af den lange sagsbehandlingstid, som ikke findes at kunne bebrejdes Tiltalte ApS. Retten har herved lagt vægt på, at forholdet er begået den 27. januar 2020. Forurettede har fremsendt klage til Datatilsynet den 15. februar 2022, som den 2. december 2022 har anmeldt Tiltalte ApS til politiet. Retten har modtaget anklageskrift den 15. juni 2023 og berammet til hovedforhandling den 6. december 2024.«

Samme mønster gentages i landsretten: [S-185-23](#) (28. april 2025) – »Virksomhed idømt **nedsat** bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid« – hvor landsretten anvendte [straffelovens § 83](#), og hvor forudgående forelæggelse for EU-Domstolen yderligere havde forlænget forløbet. Også [Retten i Lyngbys dom](#) af 11. februar 2022 anvendte straffelovens § 83.

Den praktiske konsekvens er en **strukturel udhuling af det bødeniveau, lovgiver forudsatte**: forarbejderne til § 41 forudsatte en væsentlig forhøjelse i forhold til persondataloven, men i praksis ædes forhøjelsen op af den procesbetingede nedsættelse. Det er en systemisk – ikke en tilfældig – effekt af, at Danmark har valgt den strafferetlige model efter artikel 83, stk. 9, med dens længere proceskæde.

LOV	Databeskyttelsesloven § 41, stk. 1	Straffeloven § 82, stk. 1	Straffeloven § 83
PRAKSIS	Landsretten · Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid 28.04.2025 Byretten · Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb 06.12.2024 Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture 06.01.2023 Byretten · Retten i Lyngby: Afgørelse om overtrædelse af Databeskyttelsesforordningen vedrørende opbevaring af personoplysninger 11.02.2022		

§ 9 EU-Domstolens rammer for bødeansvaret – herunder den danske forelæggelse i C-383/23

EU-Domstolen har i en række domme fastlagt rammerne for artikel 83, som de danske domstole er bundet af.

Skyldkravet og det direkte ansvar (C-807/21). I [Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen](#) (5. december 2023) fastslog Domstolen, at en dataansvarlig juridisk person kan pålægges bøde **direkte** – det er ikke en betingelse, at overtrædelsen forudgående er tilregnet en identificeret fysisk person – men at bøden forudsætter, at overtrædelsen er begået **forsætligt eller uagtsomt**. Dette skyldkrav er sammenfaldende med det tilregningskrav, som danske domstole under alle omstændigheder anvender, jf. taxisagen, hvor uagtsomhed netop blev afgørende for bødens størrelse.

Dataansvar og fælles dataansvar (C-683/21). I [Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR](#) (samme dato) præciseres, hvornår en enhed er dataansvarlig, og hvornår der er fælles dataansvar efter artikel 26 – afgørende for, hvem der overhovedet kan gøres til bødesubjekt.

Beregningsgrundlaget – »virksomhed« = koncernen (C-383/23). Den vigtigste dom for dansk praksis er [Beregning af GDPR-bøder: Begrebet »virksomhed« omfatter hele koncernens omsætning](#) af 13. februar 2025. Sagen udspringer af en **dansk forelæggelse** i en GDPR-bødesag og fastslår, at loftet i [artikel 83, stk. 4-6](#) beregnes

af hele **virksomhedens (koncernens) samlede globale årlige omsætning** – ikke kun af den enkelte juridiske persons omsætning. Selve bødens størrelse skal derimod fastsættes efter de konkrete kriterier i artikel 83, stk. 2. Dommen hæver dermed det teoretiske loft betragteligt for koncernforbundne selskaber, men ændrer ikke ved, at den konkrete udmåling forbliver forholdsmæssig.

Ingen automatisk sanktionspligt (C-768/21). I [Tilsynsmyndighedens skønsbeføjelse ved brud på persondatasikkerheden under GDPR](#) (26. september 2024) fastslog Domstolen, at tilsynsmyndigheden ikke har pligt til at gøre brug af sine korrigerende beføjelser – herunder bøde – ved ethvert konstateret brud, når det ikke er nødvendigt for at afhjælpe manglen. Det understøtter Datatilsynets praksis, hvor langt de fleste tilsyn afsluttes uden kritik eller alene med kritik eller påbud.

Behandlingsbegrebet (C-740/22). I [Mundtlig videregivelse af oplysninger om straffedomme som behandling af personoplysninger under GDPR](#) (7. marts 2024) fastslog Domstolen, at også **mundtlig** videregivelse er »behandling«, når oplysningerne er eller vil blive indeholdt i et register:

»Muligheden for at omgå anvendelsen af denne forordning ved at videregive personoplysninger mundtligt i stedet for skriftligt er nemlig åbenbart uforenelig med dette formål.«

LOV	Databeskyttelsesloven § 41, stk. 3	
PRAKSIS	EU-Domstolen · Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	13.02.2025
	EU-Domstolen · Tilsynsmyndighedens skønsbeføjelse ved brud på persondatasikkerheden under GDPR	26.09.2024
	EU-Domstolen · Mundtlig videregivelse af oplysninger om straffedomme som behandling af personoplysninger under GDPR	07.03.2024
	EU-Domstolen · Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	05.12.2023
	EU-Domstolen · Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR (C-683/21)	05.12.2023
	Landsretten · Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid	28.04.2025
	Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture	06.01.2023

Anklagemyndighedens behandling af GDPR-sager –

§ 10 Rigsadvokatmeddelelsen

Fordi bøderne er strafferetlige, er anklagemyndighedens sagsbehandling en selvstændig retskilde.

[Rigsadvokatmeddelelsen, afsnittet: Databeskyttelse - Straffesager](#) (2022) fastsætter en tæt bundet procedure.

Datatilsynets rolle beskrives i [pkt. 3.1](#): borgere kan klage til Datatilsynet **eller** anmelde direkte til politiet; vurderer tilsynet, at forholdet bør strafforfølges, kan det politianmelde. Anmeldes samme forhold begge steder, skal politikredsen som udgangspunkt **afvente Datatilsynets afgørelse**.

Obligatorisk høring af Datatilsynet. Efter [pkt. 3.10.3](#) skal der »altid indhentes en udtalelse fra Datatilsynet, hvori tilsynet bl.a. udtaler sig om sanktionsspørgsmålet«, inden der rejses tiltale for overtrædelse af de databeskyttelsesretlige regler.

Obligatorisk forelæggelse for statsadvokaten. Efter [pkt. 3.7](#) skal politikredsen forelægge tiltalepørgsmålet – **herunder strafpåstanden** – for statsadvokaten i alle sager. Domme, hvor anklagemyndigheden ikke har fået fuldt medhold i tiltalen og/eller sanktionspåstanden, skal forelægges statsadvokaten inden ankefristens udløb.

Forbud mod bødeforelæg. [Pkt. 3.3](#) fastslår, at:

»sager om overtrædelse af databeskyttelsesreglerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis«

Dette er baggrunden for, at [databeskyttelseslovens § 42](#) om bødeforelæg i praksis stort set ikke anvendes på det centrale GDPR-område, og at hver enkelt sag føres for retten.

Bødevejledningerne. Efter [pkt. 3.10.5](#) skal Datatilsynets »Bødevejledning – Udmåling af bøder til fysiske personer«, notatet om »Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer« samt notatet om registermisbrug **bilageres på alle sager**, hvori der nedlægges påstand om bøde udmålt efter det databeskyttelsesretlige niveau. Formålet er dobbelt:

»På denne måde skal det sikres, at der ikke udmåles en lavere bøde for overtrædelsen end bødeniveauet for tilsvarende overtrædelser af forordningen, ligesom bødeniveauet for overtrædelsen ikke må overskride grænserne for bødeniveauet i forordningens artikel 83.«

Tilsvarende henviser [pkt. 5.1.2](#) til *Datatilsynets bødevejledning vedrørende udmåling af bøder til virksomheder* og til Artikel 29-gruppens retningslinjer af 3. oktober 2017 om administrative bøder.

Retningslinjerne trådte i kraft **27. september 2021**; for gerningstidspunkter forud herfor kan bødepåstanden fastsættes med udgangspunkt i bødeniveauet på gerningstidspunktet, og sagen må da gerne afgøres med bødeforelæg, jf. [pkt. 3.10.4](#).

LOV

[Databeskyttelsesloven § 41, stk. 3](#)[Databeskyttelsesloven § 42](#)[Retsplejeloven § 721](#)[Retsplejeloven § 749](#)

§ 11 Registermisbrug – uberettigede opslag som strafferetligt grænseland

En særlig sagstype er **registermisbrug**: ansattes uberettigede opslag i myndigheders it-systemer. Her overlapper de databeskyttelsesretlige regler med [straffelovens § 155](#) om misbrug af stilling og §§ 152-152 c om tavshedspligt – og valget af hjemmel har betydning, fordi tilregnelseskrevet efter de databeskyttelsesretlige regler er lavere.

Rigsadvokatmeddelelsen tager udtrykkeligt højde for dette i [pkt. 3.10.3](#):

»Inden sager om overtrædelser med databeskyttelsesretlige elementer eventuelt henlægges eller påtaleopgives, skal det altid overvejes, om der i stedet er grundlag for at gøre et strafansvar gældende efter de databeskyttelsesretlige regler (f.eks. pga. lavere tilregnelseskrav).«

Retspraksis illustrerer spændingen. I [SS-4567/2023-VIB](#) (14. oktober 2025) blev en kommunalt ansat **frifundet** for misbrug af stilling efter straffelovens § 155 trods ca. 130 uberettigede opslag i sagsbehandlingssystemet SAPA. Spørgsmålet er så principielt, at [Procesbevillingsnævnet den 27. november 2025 meddelte 3.-instansbevilling](#) i en sag om netop tjenestemisbrug ved kommunalt ansattes uberettigede opslag.

Ældre praksis viser, at opslag uden tjenstlig anledning i sig selv er strafbart: i [SS-1885/2010-ODE](#) blev en polititjenestemand dømt for to uberettigede opslag i Kriminalregistret efter straffelovens §§ 152 og 155, men frifundet for den videregående videregivelse.

Databeskyttelsesretten kan også optræde **kumulativt** med almindelig strafferet. I [SS-881/2025-LYN](#) (12. maj 2026) blev der rejst tiltale både for databedrageri efter [straffelovens § 279 a](#), jf. [§ 286, stk. 2](#), og for overtrædelse af databeskyttelsesforordningen ved uautoriseret brug af en anden persons rettigheder til sundhedsydelser gennem 113 transaktioner.

LOV	Straffeloven § 152	Straffeloven § 155	Straffeloven § 279a
PRAKSIS	Byretten · Databedrageri ved uautoriseret brug af sundhedsydelser og overtrædelse af databeskyttelsesforordningen – konfiskation af 3.911,99 kr. 12.05.2026 Byretten · Frifindelse for misbrug af stilling ved uberettigede opslag i kommunalt datasystem 14.10.2025 Byretten · Polititjenestemand dømt for uberettiget opslag i Kriminalregistret 24.06.2010 Procesbevillingsnævnet · Procesbevillingsnævnet: 3.-instansbevilling om tjenstemisbrug (straffeloven § 155) ved kommunalt ansattes uberettigede opslag i sagsbehandlingssystem 27.11.2025		

§ 12 Databrud som civilretligt grundlag: godtgørelse efter artikel 82

Ud over bøden kan et databrud udløse **civilretligt** ansvar efter [artikel 82](#), hvorefter enhver, der har lidt materiel eller immateriel skade som følge af en overtrædelse, har ret til erstatning.

Højesteret tog stilling til rækkevidden i [dommen af 19. december 2025](#) (BS-14485/2025-HJR m.fl.) om godtgørelse for immateriel skade efter tyveri af en bærbar computer med personoplysninger. Højesteret [frifandt Gladsaxe Kommune](#) for godtgørelseskravene. Afgørelsen fastslår, at et databrud **ikke automatisk** udløser godtgørelse – den registrerede må godtgøre en faktisk immateriel skade.

Dommen skal læses i lyset af EU-Domstolens praksis:

- I [C-741/21](#) (11. april 2024) fortolkes begrebet immateriel skade og den dataansvarliges mulighed for ansvarsfritagelse efter artikel 82, stk. 3.
- I [C-200/23](#) (4. oktober 2024) fastslog Domstolen, at selv et **kortvarigt tab af kontrol** kan udgøre immateriel skade – men at den registrerede skal godtgøre faktisk at have lidt en skade:

»Artikel 82, stk. 1, i forordning 2016/679 skal fortolkes således, at den registreredes kortvarige tab af kontrol over sine personoplysninger [...] kan være tilstrækkeligt til at forvolde en »immateriel skade«, for så vidt som den registrerede godtgør, at vedkommende faktisk har lidt en sådan skade, hvor lille den end måtte være, uden at begrebet »immateriel skade« kræver, at det godtgøres, at der foreligger yderligere konkrete negative konsekvenser.«

Domstolen præciserede samtidig, at erstatningen efter artikel 82 har en **rent kompenserende – ikke afskrækkende – funktion**. Den afskrækkende funktion ligger i bøden efter artikel 83. Det er den systematiske forklaring på, at godtgørelsesniveauet er lavt, mens bødeløftet er højt.

En beslægtet, men praktisk vigtig pointe fra [C-200/23](#): en **udtalelse fra tilsynsmyndigheden** efter artikel 58, stk. 3, litra b, kan **ikke** fritage den dataansvarlige for erstatningsansvar. Den dataansvarlige kan altså ikke gemme sig bag en velvillig tilkendegivelse fra Datatilsynet.



LOV	Databeskyttelsesloven § 30, stk. 2	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	Højesteret · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	19.12.2025
	EU-Domstolen · Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)	04.10.2024
	EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024

§ 13 Sammenfatning – det praktiske retsbillede

Dansk GDPR-håndhævelse har en **karakteristisk profil**, der adskiller sig fra resten af EU:

- 1. To myndigheder, ét bødespor.** Datatilsynet konstaterer, kritiserer, påbyder og *indstiller* – men det er domstolene, der straffer. Datatilsynets bødeindstilling er ikke bindende for hverken anklagemyndigheden eller retten, og hver eneste sag må efter Rigsadvokatmeddelelsen føres for retten, indtil bødeniveauet er afklaret.
- 2. Et stort spring mellem indstilling og dom.** Indstillinger på 1,1-1,5 mio. kr. (Taxa 4x35, Arp-Hansen, Capiro) er endt i domme på 25.000-120.000 kr. i de sager, der er pådømt. To faktorer forklarer springet: tilregnelsen findes ofte kun **uagtsom**, og **lang sagsbehandlingstid** nedsætter bøden – i taxisagen med hele 2/3.
- 3. Artikel 32 er den centrale hjemmel.** Manglende adgangskontrol, manglende logning, manglende flerfaktorauf autentifikation, manglende kryptering af flytbare medier og manglende databehandlertilsyn er de fem tilbagevendende mangeltyper.
- 4. Ingen bagatelundskyldning for tekniske begrænsninger.** Ældre it-systemer, dyre opgraderinger og igangværende moderniseringsprojekter er ikke ansvarsfritagende. Systemet skal indrettes efter reglerne.
- 5. Manglende logning skader den dataansvarlige.** Kan det ikke dokumenteres, om uvedkommende har tilgået oplysningerne, tæller dette **imod** – ikke for – den dataansvarlige, jf. Retten i Roskilde og Region Syddanmark-sagerne.
- 6. Det offentlige straffes efter et selvstændigt niveau.** Kommuner og styrelser kan straffes uanset [straffelovens § 27, stk. 2](#), men bøden fastsættes efter indbyggertal og driftsbevilling og ligger lavere end for private.
- 7. EU-retten hæver loftet, men ikke gulvet.** [C-383/23](#) betyder, at koncernomsætningen udgør beregningsgrundlaget for loftet, og [C-807/21](#) fastholder skyldkravet. Men den konkrete udmåling styres fortsat af artikel 83, stk. 2, og de danske strafudmålningsregler.
- 8. Godtgørelse og bøde er to forskellige spor.** Bøden efter artikel 83 er afskrækkende; godtgørelsen efter artikel 82 er rent kompenserende. Højesteret frifandt i december 2025 Gladsaxe Kommune for godtgørelseskrav efter et databrud – et databrud udløser ikke i sig selv en betalingsforpligtelse over for de registrerede.

Praktisk konsekvens for dataansvarlige: Den bedste beskyttelse mod bøde er (i) dokumenterede og *implementerede* slettefrister, (ii) adgangsstyring baseret på arbejdsbetinget behov med periodisk kontrol, (iii) logning, (iv) MFA på alle internetvendte systemer med beskyttelsesværdige oplysninger, (v) reelt databehandlertilsyn, og (vi) en anmeldelsesprocedure, der kan holde 72-timers-fristen. De virksomheder og myndigheder, der kunne dokumentere netop dette – Salling Group, Sydbank, Nykredit, Spar Nord, AROS Privathospital – slap uden kritik.

LOV	Databeskyttelsesloven § 41, stk. 1-3, 6	Straffeloven § 27, stk. 2
	Straffeloven § 82, stk. 1	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	EU-Domstolen · Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	13.02.2025
	EU-Domstolen · Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	05.12.2023
	Landsretten · Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid	28.04.2025
	Landsretten · Vejle Kommune dømt for brud på databeskyttelsesforordningen – bøde forhøjet til 100.000 kr.	27.03.2025
	Byretten · Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb	06.12.2024
	Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture	06.01.2023
	Byretten · Dom for overtrædelse af databeskyttelsesregler og navneforbud	05.04.2022
	Byretten · Kommune idømt bøde på 50.000 kr. for brud på GDPR ved manglende adgangskontrol til følsomme personoplysninger	09.03.2022
	Datatilsynet · Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	01.02.2024
	Datatilsynet · Ingen kritik af privat virksomhed for anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Datatilsynets tilsyn med Salling Group A/S vedrørende it-sikkerhed og rettighedsstyring	15.01.2021
	Datatilsynet · Manglende grundlag for kritik af AROS Privathospital efter anmeldelse af sikkerhedsbrud	08.12.2020
	Datatilsynet · Arp-Hansen Hotel Group indstillet til bøde for manglende sletning af gæsteprofiler	28.07.2020
	Datatilsynet · Alvorlig kritik og påbud til Region Syddanmark for utilstrækkelig sikkerhed og manglende underretning	12.06.2020
	Datatilsynet · Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.	25.03.2019

REFERENCE Lovgrundlag

5 paragraffer

Databeskyttelsesloven § 8	stk. 4	Databeskyttelsesloven § 30	stk. 2
Databeskyttelsesloven § 41	stk. 1-3, 6, 7	Databeskyttelsesloven § 42	
Straffeloven § 82	stk. 1		

MATERIALE Citerede afgørelser

58 afgørelser

HØJESTERET · ØVERSTE INSTANS

2

19.12.2025	Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	10337-12149
19.12.2025	Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	14485-2025-2025-14653-2025-1 og 16195-2025

EU-DOMSTOLEN · EUROPÆISK DOMSTOL

7

13.02.2025	Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	C-383/23
04.10.2024	Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)	C-200/23
26.09.2024	Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	C-768/21
11.04.2024	Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	C-741/21
07.03.2024	Mundtlig videregivelse af oplysninger om straffedomme som behandling af personoplysninger under GDPR	C-740/22
05.12.2023	Betingelser for dataansvar, fælles dataansvar og pålæggelse af administrative bøder efter GDPR (C-683/21)	C-683/21
05.12.2023	Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	C-807/21

LANDSRETTE · ANKEINSTANS

3

28.04.2025	Virksomhed idømt nedsat bøde for overtrædelse af databeskyttelsesregler på grund af lang sagsbehandlingstid	9601-11193
27.03.2025	Vejle Kommune dømt for brud på databeskyttelsesforordningen – bøde forhøjet til 100.000 kr.	9568-11151
27.10.2011	Virksomhed dømt for alvorlig overtrædelse af Databeskyttelsesloven: Bøde for ulovlig opbevaring af kundedata	

BYRETTE · FØRSTE INSTANS

10

12.05.2026	Databedrageri ved uautoriseret brug af sundhedsydelser og overtrædelse af databeskyttelsesforordningen – konfiskation af 3.911,99 kr.	10682-12668
14.10.2025	Frifindelse for misbrug af stilling ved uberettigede opslag i kommunalt datasystem	10474-12342
06.12.2024	Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb	7051-8477

06.01.2023	Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture	4826-5814
05.04.2022	Dom for overtrædelse af databeskyttelsesregler og navneforbud	4907-5916
09.03.2022	Kommune idømt bøde på 50.000 kr. for brud på GDPR ved manglende adgangskontrol til følsomme personoplysninger	2256-2687
11.02.2022	Retten i Lyngby: Afgørelse om overtrædelse af Databeskyttelsesforordningen vedrørende opbevaring af personoplysninger	3822-4617
20.01.2022	Virksomhed dømt for uretmæssig videregivelse af personoplysninger om tidligere ansat	2016-2414
12.02.2021	Dom for overtrædelse af databeskyttelsesforordningen ved manglende sletning af personoplysninger	4836-5829
24.06.2010	Polititjenestemand dømt for uberettiget opslag i Kriminalregistret	6925-8316

DATATILSYNET · NÆVN / KLAGEINSTANS

33

05.05.2026	Datatilsynet meddeler Aalborg Kommune påbud om systemoverblik og sletning af personoplysninger	2026-432-0055
27.11.2024	Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	
01.02.2024	Privathospitalet Capio A/S indstilles til bøde på 1,5 mio. kr. for brud på sikkerheden	
22.01.2024	Politianmeldelse af Hvidovre Kommune for utilstrækkelig sikkerhed ved behandling af børneoplysninger	
31.08.2023	Ingen kritik af privat virksomhed for anmeldelse af brud på persondatasikkerheden	2021-41-0132
31.08.2023	Tilsyn med virksomheders overholdelse af regler om anmeldelse af brud på persondatasikkerheden	2021-41-0133
31.08.2023	Datatilsynets tilsyn med virksomheds håndtering og anmeldelse af brud på persondatasikkerheden	2021-41-0134
31.08.2023	Tilsyn med procedurer for anmeldelse af brud på persondatasikkerheden hos privat virksomhed	2021-41-0135
31.08.2023	Rettidig anmeldelse af brud på persondatasikkerheden hos en privat virksomhed	2021-41-0137
31.08.2023	Tilsyn med offentlig myndigheds overholdelse af regler om anmeldelse af brud på persondatasikkerheden	2021-423-0243
25.08.2022	Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	2021-431-0126
12.05.2022	Civilstyrelsen indstilles til bøde på 100.000 kr. for brud på persondatasikkerheden	
05.04.2022	Danske Bank indstilles til bøde for manglende sletning af personoplysninger	
17.09.2021	Region Syddanmark politianmeldt og indstillet til bøde på 500.000 kr. for brud på behandlingssikkerheden	

16.09.2021	Favrskov Kommune indstilles til bøde efter læk af følsomme oplysninger på hjemmeside	
17.08.2021	Udlændingestyrelsen politianmeldes og indstilles til bøde for grove sikkerhedsbrister	
09.07.2021	Politianmeldelse og bødeindstilling til Medicals Nordic I/S for mangelfuld behandlingssikkerhed	
16.06.2021	Vejle Kommune politianmeldes og indstilles til bøde for brud på persondatasikkerheden	
15.01.2021	Datatilsynets tilsyn med Salling Group A/S vedrørende it-sikkerhed og rettighedsstyring	2020-41-0064
15.01.2021	Tilsyn med Udviklings- og Forenklingsstyrelsens behandlingssikkerhed fører ikke til kritik	2020-421-0078
15.01.2021	Datatilsynets kontrol af informationssikkerhed og risikostyring i Odense Kommune	2020-423-0231
08.12.2020	Ingen kritik af DJØF efter tilsyn med anmeldelse af brud på persondatasikkerheden	2019-41-0035
08.12.2020	Manglende grundlag for kritik af AROS Privathospital efter anmeldelse af sikkerhedsbrud	2019-41-0037
08.12.2020	Datatilsynet finder ingen grund til kritik af Region Syddanmarks håndtering af sikkerhedsbrud	2019-422-0024
11.09.2020	Alvorlig kritik af Datatilsynet for manglende behandlingssikkerhed og underretning ved brud på persondatasikkerheden	2020-442-8866
04.08.2020	PrivatBo indstillet til bøde efter utilsigtet videregivelse af personoplysninger på over 1.000 beboere	
28.07.2020	Arp-Hansen Hotel Group indstillet til bøde for manglende sletning af gæsteprofiler	
17.07.2020	Alvorlig kritik af Region Syddanmark for manglende adgangsstyring og sen anmeldelse af sikkerhedsbrud	2018-442-0026
18.06.2020	Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse	2019-31-2250
12.06.2020	Alvorlig kritik og påbud til Region Syddanmark for utilstrækkelig sikkerhed og manglende underretning	2020-442-6448
15.05.2020	JobTeam politianmeldt og indstillet til bøde for manglende samarbejde og tilsidesættelse af indsigtsret	
03.06.2019	Alvorlig kritik og bødeindstilling til IDdesign for overtrædelse af princippet om opbevaringsbegrænsning	2018-41-0015
25.03.2019	Datatilsynet indstiller taxaselskab til bøde på 1,2 mio. kr.	
PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS		2
16.06.2025	Twist om hjemmel til privat parkeringskontrol på privat fællesvej ved Dommervænget i Roskilde	park-4617

11.05.2023 Ugyldige kontrolafgifter efter teknisk fejl i EasyPark-app ved langtidsparkering park-2687

PROCESBEVILLINGSNÆVNET · NÆVN / KLAGEINSTANS 1

27.11.2025 Procesbevillingsnævnet: 3.-instansbevilling om tjenestemisbrug (straffeloven § 155) ved kommunalt ansattes uberettigede opslag i sagsbehandlingssystem 25/25838

FORARBEJDE Betænkninger

1 reference

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 2)
nr. 1565 · 2017 · Justitsministeriet

07

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over DSA/DMA – platformes due diligence-forpligtelser og håndhævelse

Due diligence-pyramiden, VLOP-udpegelse og den delte håndhævelse mellem Kommissionen og den danske koordinator

Version 2 · Opdateret 16. jul. 2026 · 20 afgørelser · 2014–2025

[Læs online](#)

INTRODUKTION

DSA-forordningen (forordning (EU) 2022/2065) og DMA-forordningen (forordning (EU) 2022/1925) udgør tilsammen EU's systemiske platformsregulering: DSA pålægger formidlingstjenester gradvist skærpede due diligence-forpligtelser afhængigt af tjenestens type og størrelse, mens DMA underlægger udpegede gatekeepere en katalog af adfærdsforpligtelser. I Danmark er forordningen suppleret af lov nr. 1765 af 28. december 2023, der udpeger en national koordinator for digitale tjenester og tillægger denne undersøgelses- og håndhævelsesbeføjelser med bøderammer op til 6 pct. af den globale omsætning. Praksis på området er endnu overvejende EU-baseret og procesretlig: Unionens retsinstanser har i en række kendelser om VLOP-udpegelser fastslået, at gennemsigtighedshensynet vejer tungere end platformenes økonomiske interesser, og at udpegelsen som udgangspunkt gennemføres uden opsættende virkning.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 DSA's due diligence-forpligtelser er kumulativt lagdelte: enhver onlineplatform bærer både hostingtjenesternes og formidlingstjenesternes forpligtelser, og en VLOP bærer dem alle plus kapitel III, afdeling 5.
- 02 Kommissionen har enekompetence over VLOP/VLOSE'ernes systemiske risikoforpligtelser (DSA art. 56, stk. 2), mens etableringsmedlemsstaten har enekompetence over alle øvrige udbydere (art. 56, stk. 1).
- 03 En udpegelse som meget stor onlineplatform får virkning fire måneder efter meddelelsen, og et annulationssøgsmål har ikke i sig selv opsættende virkning.
- 04 Ved begæring om foreløbige forholdsregler mod DSA-forpligtelser vejer EU-lovgivers gennemsigtighedshensyn tungere end platformens rent økonomiske interesser (Aylo/Pornhub og WebGroup/XVideos).
- 05 Interesseafvejningen er et selvstændigt led, adskilt fra fumus boni juris – men skal foretages ud fra den antagelse, at hovedsagen ikke tages til følge, og altså med Kommissionens VLOP-vurdering lagt til grund.

- 06** En ansøger om foreløbige forholdsregler kan ikke påberåbe sig en skade for tredjeparter, der er forskellig fra den skade, som er gjort gældende til støtte for uopsættelighed.
- 07** Platformsforpligtelser der berører ytringsfriheden kræver indbyggede garantier mod overfjernelse af lovligt indhold for at være forenelige med Chartrets artikel 11 (Polen mod Parlamentet og Rådet).
- 08** DSA art. 28 om beskyttelse af mindreårige er totalharmoniseret; nationale alderskontrolkrav kan ikke pålægges onlineplatforme oven i forordningen.
- 09** Hjemlandsprincippet spærrer for, at destinationsmedlemsstater pålægger platforme etableret i andre medlemsstater selvstændige registrerings-, indberetnings- og gebyrkrav.
- 10** Den danske koordinator handler i fuld uafhængighed, jf. lovens § 4 – regeringen har ingen instruktionsbeføjelse i konkrete sager, heller ikke om prioritering.
- 11** Danske bøder for DSA-overtrædelser kan udgøre op til 6 pct. af den globale omsætning, tvangsbøder op til 5 pct. af den gennemsnitlige daglige globale omsætning, og afgørelserne kan ikke påklages administrativt.
- 12** DMA-gatekeeperstatus udløses af kvantitative formodninger (7,5 mia. EUR omsætning eller 75 mio. EUR markedsverdi, 45 mio. slutbrugere og 10.000 erhvervsbrugere), som kun kan afkræftes med tilstrækkeligt underbyggede argumenter, der klart rejser tvivl om formodningerne.
- 13** DMA-bøder kan nå 10 pct. af den globale omsætning – og 20 pct. ved gentagen tilsidesættelse af samme forpligtelse inden for otte år.

§ 1 To forordninger, to reguleringslogikker – og hvad denne oversigt ikke dækker

DSA og DMA blev vedtaget med få dages mellemrum i efteråret 2022, men de forfølger vidt forskellige formål og har hver sin håndhævelseslogik.

	DSA – forordning (EU) 2022/2065	DMA – forordning (EU) 2022/1925
Reguleringsobjekt	Alle formidlingstjenester (mere conduit, caching, hosting)	Udpegede gatekeepere med centrale platformstjenester
Reguleringsstype	Proces- og risikoregulering (due diligence)	Ex ante-adfærdsregulering (forbud og påbud)
Udløsende kriterium	Tjenestens type + brugerantal (45 mio./md. → VLOP)	Kvantitative tærskler + Kommissionens udpegelse
Håndhævelse	Delt: national koordinator + Kommissionen	Kommissionen alene
Bøderamme	6 pct. af global omsætning	10 pct. – 20 pct. ved gentagelse
Anvendelse fra	17. februar 2024 (dele fra 16. november 2022)	Maj 2023 / marts 2024 for gatekeepere

DSA trådte i kraft den 16. november 2022 og finder anvendelse fra den 17. februar 2024, dog således at bl.a. [artikel 24, stk. 2, 3 og 6](#), [artikel 33, stk. 3-6](#) og [artikel 40, stk. 13](#) fandt anvendelse allerede fra ikrafttrædelsen. Det er netop den tidlige anvendelse af art. 33, der gjorde det muligt for Kommissionen at udpege de første 17 platforme og 2 søgemaskiner med virkning fra den 25. august 2023 – over et halvt år før forordningens almindelige anvendelsesdato.

Forarbejderne til den danske gennemførelseslov beskriver formålet præcist:

Forordningen om digitale tjenester fastsætter harmoniserede regler for ydelse af formidlingstjenester, herunder en ramme for betinget ansvarsfritagelse for udbydere af formidlingstjenester; regler om specifikke due diligence-forpligtelser, der er skræddersyet til visse specifikke kategorier af udbydere af formidlingstjenester, og regler om gennemførelse og håndhævelse af forordningen om digitale tjenester, herunder vedrørende samarbejde og koordinering mellem de kompetente myndigheder.

Denne oversigt dækker **det andet og tredje ben** – due diligence-forpligtelserne og håndhævelsesarkitekturen. Den **betingede ansvarsfritagelse** i DSA art. 4-6 (mere conduit, caching og hosting) og platformenes erstatnings- og strafansvar for brugeres ulovlige indhold hører derimod under [platformansvar](#). Dark patterns i cookieflows behandles under [cookies-samtykke](#), markedsføringsretlig online-vildledning under [vildledende-markedsføring-online](#), og profilering/automatiserede afgørelser under [ai-systemer-gdpr](#).

Trappemodellen: due diligence-forpligtelser efter tjenestens type og størrelse

§ 2

DSA's kapitel III er bygget som en **kumulativ pyramide**. Hvert lag lægger sig oven på de underliggende, så en meget stor onlineplatform bærer samtlige forpligtelser fra alle fire afdelinger. Forarbejderne til den danske lov beskriver det som, at »[f]orpligtelserne er differentieret på baggrund af typen og størrelsen af tjenesten samt antallet af brugere«.

Lag 1 – alle formidlingstjenester (afdeling 1):

- [Artikel 11](#): ét enkelt elektronisk kontaktpunkt for myndigheder, Kommissionen og Det Europæiske Råd for Digitale Tjenester – med angivelse af de sprog, der anvendes.
- [Artikel 13](#): udbydere uden etablering i Unionen skal udpege en **retlig repræsentant**, der efter [art. 13, stk. 3](#) selv kan drages til ansvar for manglende overholdelse. Udpegningen udgør *ikke* etablering i Unionen, jf. stk. 5 – en vigtig præcisering for jurisdiktionsspørgsmålet.
- [Artikel 14-15](#): vilkår og betingelser samt årlig gennemsigtighedsrapportering.

Lag 2 – hostingtjenester (afdeling 2): anmeldelsesmekanismer og handlepligt ([art. 16](#)) og begrundelsespligt ([art. 17](#)).

Lag 3 – onlineplatforme (afdeling 3): intern klagebehandling, udenretslig tvistbilæggelse, pålidelige indberettere, misbrugsværn, udvidet rapportering, forbud mod dark patterns, reklametransparens, anbefalingssystemers parametre og beskyttelse af mindreårige ([art. 20-28](#)).

Lag 4 – VLOP/VLOSE (afdeling 5): systemisk risikovurdering og -afbødning, krisemekanisme, uafhængig revision, reklamearkiv og forskeradgang ([art. 34-40](#)).

EU-Domstolen har ikke endnu fortolket selve rækkevidden af disse forpligtelser. Men Domstolens generelle tilgang til **due diligence-begrebet** i beslægtede regelsæt er oplysende. I [C-117/24](#) (JYSK) om tømmerforordningen fastslog Domstolen, at det **ikke er tilstrækkeligt** for et datterselskab blot at have adgang til moderselskabets due diligence-ordning: forpligtelsen »indebærer en aktiv handling fra den enkelte virksomheds side«, og virksomheden skal selv kunne fremlægge og dokumentere sine risikovurderinger direkte over for tilsynet. Domstolen fremhævede, at myndighedernes kontrolmuligheder »ville blive alvorligt svækket, hvis virksomheder blot kunne henvise til en tredjeparts registre og vurderinger«. Samme logik ligger bag DSA art. 34, stk. 3, hvorefter støttedokumenterne til risikovurderingen skal opbevares i mindst tre år og efter anmodning sendes til Kommissionen og koordinatoren. I [C-370/23](#) understregede Domstolen tilsvarende, at due diligence-pligten følger den aktør, der reelt har rådigheden – ikke den, der formelt har defineret sig ud af rollen.

PRAKSIS	EU-Domstolen · Krav til virksomheders egne due diligence-ordninger for træ og træprodukter i koncerner	13.11.2025
	EU-Domstolen · Definition af »virksomhed« og »omsætning« ved salg af træ til fældning efter EU's tømmerforordning	21.11.2024

§ 3 Notice-and-action, begrundelsespligt og klageadgang – DSA's processuelle kerne

Kernen i DSA's due diligence-arkitektur er en **processuel retssikkerhedskæde** omkring indholdsmoderation: anmeldelse → beslutning → begrundelse → intern klage → udenretslig tvistbilæggelse → domstol.

Anmeldelsesmekanismen i [art. 16](#) skal være »let tilgængelig og brugervenlig« og give mulighed for anmeldelse udelukkende ad elektronisk vej. Bestemmelsens [stk. 3](#) er retligt central, fordi den kobler den processuelle pligt sammen med ansvarsspørgsmålet:

De i denne artikel omhandlede anmeldelser anses for at tilvejebringe konkret kendskab med henblik på artikel 6 til den pågældende specifikke information, når de sætter en omhyggelig hostingtjenesteudbyder i stand til at bestemme, hvori det ulovlige ved den pågældende aktivitet eller information består, uden først at måtte foretage en retlig undersøgelse.

Efter [art. 16, stk. 6](#) skal anmeldelser behandles »rettidigt, omhyggeligt, uden forskelsbehandling og objektivt«, og anvendes automatiserede metoder, skal det oplyses.

Begrundelsespligten i [art. 17](#) – det såkaldte *statement of reasons* – udløses ved enhver af fire indgrebstyper: begrænsning af synlighed (herunder degradering), suspension af betalinger, suspension af tjenesten og lukning af konto. Begrundelsen skal efter [art. 17, stk. 3](#) bl.a. angive det påberåbte **retsgrundlag** eller **aftalegrundlag**, om automatiserede metoder er anvendt, det territoriale anvendelsesområde og klagemulighederne. Efter [art. 24, stk. 5](#) skal alle begrundelser indsendes til Kommissionens offentligt tilgængelige, maskinlæsbare **DSA Transparency Database** – en gennemsigtighedsmekanisme uden fortilfælde i EU-retten.

Intern klagebehandling efter [art. 20](#) skal være gratis, elektronisk og tilgængelig i mindst seks måneder. To krav er værd at fremhæve: efter [stk. 4](#) skal platformen **omgøre** sin beslutning uden unødigt forsinkelse, hvis klagen giver tilstrækkeligt grundlag, og efter [stk. 6](#) må beslutningen ikke træffes »udelukkende på grundlag af automatiserede metoder« – der skal være tilsyn af behørigt kvalificeret personale.

Udenretslig tvistbilæggelse efter [art. 21](#) certificeres af koordinatoren for digitale tjenester for op til fem år. Organet kan **ikke** pålægge parterne en bindende løsning, jf. [art. 21, stk. 2](#), men omkostningsfordelingen er asymmetrisk: taber platformen, betaler den alle gebyrer og modtagerens rimelige udgifter; taber brugeren, betaler brugeren intet – medmindre denne åbenlyst har handlet i ond tro, jf. [stk. 5](#). Afgørelsen skal træffes inden 90 kalenderdage, i komplekse sager højst 180.

Hele denne kæde er i dansk ret bødesanktioneret, jf. [§ 10, stk. 1](#), der udtrykkeligt nævner artikel 16, stk. 1, 2 eller 4-6, artikel 17, stk. 1-4, artikel 20 og artikel 21.

LOV

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester
[§ 10, stk. 1](#)

§ 4 Pålidelige indberettere og værn mod misbrug – art. 22-23

Pålidelige indberettere (*trusted flaggers*) efter [art. 22](#) er DSA's institutionaliserede kanal for kvalificerede anmeldelser. Status tildeles af koordinatoren for digitale tjenester i etableringslandet på grundlag af tre kumulative betingelser i [art. 22, stk. 2](#): særlig ekspertise, uafhængighed af enhver udbyder af onlineplatforme, og omhyggelig, nøjagtig og objektiv anmeldelsespraksis. Platformene skal give sådanne anmeldelser **prioritet** og træffe beslutning uden unødigt forsinkelse.

Ordningen er tovejs. Efter [art. 22, stk. 6](#) kan en platform, der har oplysninger om, at en pålidelig indberetter har indgivet et betydeligt antal upræcise eller ubegrundede anmeldelser, videregive dette til koordinatoren – og finder koordinatoren legitime grunde til at indlede undersøgelse, **suspenderes** statussen mens undersøgelsen pågår. Tilbagekaldelse efter [stk. 7](#) forudsætter kontradiktion. I Danmark har DSA-tilsynet tildelt to organisationer status som pålidelig indberetter, herunder RettighedsAlliancen.

Misbrugsværnet i [art. 23](#) er formuleret som en **pligt**, ikke en beføjelse: platformen *skal* suspendere tjenesten over for modtagere, der ofte leverer åbenbart ulovligt indhold ([stk. 1](#)), og *skal* suspendere behandlingen af anmeldelser fra dem, der ofte indgiver åbenbart grundløse anmeldelser eller klager ([stk. 2](#)). Begge dele forudsætter forudgående advarsel og en rimelig periode. [Stk. 3](#) opstiller fire obligatoriske vurderingsmomenter – antal, relativ andel, grovhed og hensigt – der skal anvendes »fra sag til sag rettidigt, omhyggeligt og objektivt«. Bestemmelsen er dermed en lovfæstet **proportionalitetstest** på privat retshåndhævelse, og efter [stk. 4](#) skal politikken og eksemplerne fremgå af vilkårene.

Antallet af suspensioner efter art. 23 skal rapporteres særskilt i den halvårslige gennemsigtighedsrapport, opdelt efter årsag, jf. [art. 24, stk. 1, litra b](#).

§ 5 Reklametransparens, forbuddet mod dark patterns og anbefalingssystemernes parametre

Forbuddet mod dark patterns i [art. 25, stk. 1](#) er formuleret bredt:

Udbydere af onlineplatforme må ikke udforme, organisere eller drive deres onlinegrænseflader på en måde, der vildleder eller manipulerer tjenestemodtagerne, eller på en måde, som på anden vis væsentligt fordrejer eller forringer tjenestemodtagernes evne til at træffe frie og informerede beslutninger.

Afgørende er dog [art. 25, stk. 2](#): forbuddet gælder **ikke** for praksis, der er omfattet af direktiv 2005/29/EF om urimelig handelspraksis eller af GDPR. DSA art. 25 er altså en *residualbestemmelse*, der lukker hullet mellem markedsføringsretten (som forudsætter en handelspraksis over for forbrugere) og databeskyttelsesretten (som forudsætter behandling af personoplysninger). Forarbejderne til den danske lov er opmærksomme på snitfladen og bemærker, at art. 25-28 »har snitflader til lovgivning, som hører under henholdsvis Forbrugerombudsmandens eller Datatilsynets tilsynskompetence«, og at kompetente myndigheder derfor kan rådføre sig med disse – dog uden at være bundet af svaret, henset til uafhængighedskravet.

De eksempler, Kommissionen efter [art. 25, stk. 3](#) kan udstede retningslinjer om, genkendes umiddelbart i dansk markedsføringspraksis. Forbrugerombudsmanden fandt i [afgørelse af 19. februar 2024](#), at et samtykkeflow, hvor et »nej« udløste en advarsel om, at selskabet så ikke kunne rådgive optimalt, var både vildledende og en **aggressiv handelspraksis** – og at samtykket derfor var ugyldigt. I [afgørelse af 25. august 2014](#) fastslog Forbrugerombudsmanden, at forhåndsafkrydsning af en ikke-obligatorisk tillægsydelse strider mod god markedsføringsskik, og i [afgørelse af 8. september 2021](#), at et samtykke ikke er gyldigt, hvis kunden afbryder købsflowet, før en handling klart afslutter afgivelsen. Disse sager afgøres efter markedsføringsloven – men de illustrerer præcis den type grænsefladedesign, som DSA art. 25 rammer, når markedsføringsloven ikke gør.

Reklametransparens efter [art. 26, stk. 1](#) kræver, at brugeren i realtid kan identificere, at der er tale om en reklame, hvem den vises på vegne af, hvem der har betalt, og de vigtigste målretningsparametre. [Art. 26, stk. 3](#) forbyder reklamer baseret på profilering ved brug af **særlige kategorier af personoplysninger** efter [GDPR art. 9, stk. 1](#) – et forbud der supplerer, men ikke erstatter, GDPR's egen regulering. EU-Domstolen fastslog i [C-446/21](#) (Schrems mod Meta), at dataminimeringsprincippet er til hinder for, at et socialt netværk »uden begrænsninger med hensyn til tid, og uden at der sondres på grundlag af disse oplysningers art« sammenstiller alle indsamlede personoplysninger til målrettet reklame – og at en persons offentlige tilkendegivelse af sin seksuelle orientering ikke giver platformen adgang til at behandle *andre* oplysninger om samme forhold indhentet uden for platformen.

Anbefalingssystemer efter [art. 27](#) skal have deres vigtigste parametre beskrevet i vilkårene på »klart og forståeligt sprog«, med angivelse af de kriterier, der har størst betydning, og **grundene til deres relative betydning**. Findes der flere anbefalingsmuligheder, skal der efter [art. 27, stk. 3](#) tilbydes en funktionalitet, der er »direkte og let tilgængelig« fra det sted i grænsefladen, hvor informationen prioriteres.

PRAKSIS	EU-Domstolen · Dataminimering og behandling af følsomme personoplysninger til personaliseret reklame på sociale netværk	04.10.2024
	Forbrugerombudsmanden · Vildledende samtykkeflow: Forsikringssselskab indskræpes for aggressiv markedsføringspraksis	19.02.2024
	Forbrugerombudsmanden · Samtykke til markedsføring og 'tabt kurv-påmindelser' i online købsflow	08.09.2021
	Forbrugerombudsmanden · Forhåndsafkrydsning af pladsbillet er i strid med god markedsføringsskik	25.08.2014

Beskyttelse af mindreårige efter art. 28 – og totalharmoniseringens spærrevirkning

§ 6

Artikel 28 pålægger onlineplatforme, der er tilgængelige for mindreårige, at indføre »passende og forholdsmæssige foranstaltninger til at sikre et højt niveau af privatlivets fred, tryghed og sikkerhed«. **Stk. 2** forbyder profileringsbaserede reklamer, når platformen »med rimelig sikkerhed« ved, at modtageren er mindreårig – og **stk. 3** indeholder en central balance: overholdelsen må **ikke** forpligte platformen til at behandle yderligere personoplysninger for at vurdere, om modtageren er mindreårig. Bestemmelsen er dermed konstrueret, så alderskontrol ikke bliver en bagvej til øget dataindsamling.

Bestemmelsens **totalharmoniserende** karakter har allerede fået konkret dansk betydning. I **rigsadvokatmeddelelsen om tobak, alkohol og elektroniske cigaretter** fastslås det udtrykkeligt, at det skærpede krav om effektiv elektronisk aldersverifikation ved fjernsalg af e-cigaretter

vil ikke omfatte online platforme, jf. definitionen i artikel 3, litra 1, i forordning om digitale tjenester, herunder online platforme, der giver forbrugere mulighed for at indgå aftaler om fjernsalg med erhvervsdrivende, idet beskyttelse af mindreårige, herunder foranstaltninger om alderskontrol, falder inden for forordningens totalharmoniserede område.

Det er et markant eksempel på DSA's **spærrevirkning**: den danske lovgiver kunne ikke pålægge onlineplatforme et nationalt alderskontrolkrav, selv om formålet – beskyttelse af mindreårige – er sammenfaldende med forordningens.

Samme spærrevirkning gør sig gældende horisontalt. I **C-665/22** fandt Domstolen, at nationale indberetningskrav for onlineplatforme etableret i andre medlemsstater strider mod princippet om hjemlandskontrol – en afgørelse truffet på grundlag af P2B-forordningen og servicedirektivet, men med samme systematik som DSA art. 56, stk. 1. Og i **C-555/23** satte Domstolen den modsatte grænse: selv når en medlemsstat har tilsidesat EU-retten ved at undtage onlineudbydere fra en forpligtelse, kan de nationale domstole ikke »udfylde hullet« ved analogi for at pålægge administrative sanktioner – princippet om lovhjemmel for straf i **Chartrets artikel 49, stk. 1** sætter en absolut grænse for overensstemmende fortolkning. Det er en pointe med direkte relevans for DSA-håndhævelsen: bødehemlen i **§ 10** opregner udtømmende de artikler, hvis overtrædelse er strafbar, og listen kan ikke udvides ved fortolkning.

LOV

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester
§ 10

PRAKSIS	EU-Domstolen · Beskyttelse af den menneskelige værdighed i online-medietjenester og grænserne for overensstemmende fortolkning i straffesager	26.06.2025
	EU-Domstolen · Nationale indberetningskrav for onlineplatforme i strid med princippet om hjemlandskontrol	30.05.2024

§ 7 VLOP-udpegelsen efter art. 33 og domstolsprøvelsen: Zalando, Aylo og WebGroup

Den mest udviklede DSA-praksis handler ikke om forpligtelsernes *indhold*, men om **udpegelsen** og dens umiddelbare virkning.

Efter **art. 33, stk. 1** omfatter afdeling 5 platforme og søgemaskiner med et gennemsnitligt månedligt antal aktive tjenestemodtagere i Unionen på **45 mio. eller derover**, som er udpeget efter **stk. 4**. Udpegelsesproceduren rummer to bemærkelsesværdige træk: Kommissionen kan udpege en platform, **selv om** udbyderen ikke har

overholdt sin oplysningspligt efter art. 24, stk. 2-3, og selv om udbyderen ikke fremsætter bemærkninger inden for de ti arbejdsdage, den har fået. Forpligtelserne indtræder efter **stk. 6 fire måneder** efter meddelelsen – uafhængigt af, om der er anlagt annulationssøgsmål.

Zalando – C-647/23 – er den første DSA-sag ved Domstolen. Kendelsen af 11. januar 2024 angår ikke realiteten, men interventionsadgangen: Domstolen ophævede Rettens afslag på intervention i Zalandos annulationssøgsmål mod udpegelsen efter art. 33. Kendelsen viser, at udpegelsessager efter art. 33 har en bredere kreds af berørte end blot Kommissionen og platformen.

Aylo/Pornhub – C-511/24 – er den vigtigste afgørelse til dato. Kommissionen udpegede ved afgørelse C(2023) 8842 final af 20. december 2023 Pornhub som VLOP. Aylo anlagde annulationssøgsmål og begærede suspension af pligten til at føre reklamearkiv efter art. 39, navnlig fordi offentliggørelsen af oplysninger om **fysiske personer** som annoncører efter art. 39, stk. 2, litra b og c ville risikere at skabe en »doxing-liste«. Rettens præsident afslog (T-138/24 R) – der forelå både fumus boni juris og uopsættelighed, men interesseafvejningen faldt ud til EU-lovgivers fordel.

Domstolens vicepræsident **korrigerede** Rettens begrundelse på ét punkt, men forkastede appellen. For det første er interesseafvejningen et selvstændigt led:

»[D]et fremgår af fast retspraksis, at afvejningen af de modstridende interesser udgør et særskilt trin i forhold til prøvelsen af, om der foreligger fumus boni juris. [...] Følgerne af en udsættelse eller [...] en umiddelbar gennemførelse af den anfægtede afgørelse er i princippet ikke forskellige afhængigt af, hvilket anbringende der lægges til grund for fumus boni juris [...]« (præmis 21)

Rettens præsident havde derfor begået en retlig fejl ved at afskære hensynet til de optrædendes privatliv alene med den begrundelse, at det ikke indgik i fumus-vurderingen. Men fejlen var uden betydning, fordi begrundelsen kunne erstattes:

»Hvis den ret, der behandler en begæring om foreløbige forholdsregler, under hensyn til en sådan risiko måtte konkludere, at de interesser, der taler for at træffe de foreløbige forholdsregler, skal have forrang, ville den foreløbige forholdsregel i sidste ende afgørende være baseret på nødvendigheden af at undgå, at der indtræder en skade, hvis alvorlige og uoprettelige karakter ikke er bevist, selv om et sådant bevis principielt er en forudsætning for, at de foreløbige forholdsregler kan træffes« (præmis 28)

Aylo havde alene påberåbt sig **økonomisk** skade som uopsættelighedsgrundlag; risikoen for identifikation af fysiske personer indgik kun til underbygning heraf. Selskabet kunne derfor ikke ad bagvejen gøre tredjeparters privatlivsskade gældende i interesseafvejningen.

Afgørende for oversigten er dernæst vicepræsidentens **metodiske** præcisering: interesseafvejningen skal – modsat uopsættelighedsvurderingen – foretages ud fra den antagelse, at hovedsagen **ikke** vil blive taget til følge. Rettens præsident havde derfor med rette lagt Kommissionens vurdering af, at Pornhub er en VLOP, til grund, uden selvstændigt at prøve, om tærsklen faktisk var nået. Det betyder i praksis, at en platform næppe kan opnå suspension ved at bestride selve udpegelseskriteriet.

WebGroup/XVideos – C-620/24, kendelse af 25. februar 2025 – bekræfter linjen: også her blev appellen om opsættende virkning for gennemsigtighedsforpligtelserne efter art. 39 afvist. To kendelser inden for et halvt år med samme udfald over for to strukturelt ens platforme etablerer et **klart mønster**: DSA's gennemsigtighedsforpligtelser gennemføres, mens søgsmålet verserer.

PRAKSIS	EU-Domstolen · Afvisning af appel om opsættende virkning for XVideos' gennemsigtighedsforpligtelser under retsakten om digitale tjenester (DSA)	25.02.2025
	EU-Domstolen · Pornhub-sagen: EU-Domstolens afvisning af suspension af gennemsigtighedskrav under DSA	06.09.2024
	EU-Domstolen · Domstolen ophæver afslag på intervention i sag om Zalando's status som meget stor onlineplatform	11.01.2024

Systemisk risikovurdering, afbødning og krisemekanisme – art. 34-36

§ 8

Artikel 34 er DSA's mest originale bidrag: en pligt til at »identificere, analysere og vurdere omhyggeligt alle systemiske risici i Unionen, der udspringer af udformningen eller virkemåden af deres tjeneste«. De fire risikokategorier i **art. 34, stk. 1** er brede:

- **litra a)** udbredelse af ulovligt indhold
- **litra b)** negativ indvirkning på grundlæggende rettigheder – med udtrykkelig opregning af Chartrets art. 1 (værdighed), 7 (privatliv), 8 (databeskyttelse), 11 (ytrings- og informationsfrihed, herunder mediepluralisme), 21 (ikkeforskelsbehandling), 24 (børns rettigheder) og 38 (forbrugerbeskyttelse)
- **litra c)** negativ indvirkning på samfundsdebat, valgprocesser og offentlig sikkerhed
- **litra d)** kønsbaseret vold, folkesundhed, mindreårige og fysisk/psykisk velbefindende

Vurderingen skal ske mindst årligt og **forud** for ibrugtagning af funktionaliteter med kritisk indvirkning. Efter **art. 34, stk. 2** skal fem faktorer inddrages – anbefalingssystemernes udformning, indholdsmoderationssystemerne, vilkårene og håndhævelsen heraf, reklamevisningssystemerne og udbyderens datarelaterede praksis – og risikoen for **bevidst manipulation**, herunder ikkeautentisk brug, skal analyseres særskilt. Vurderingen skal tage hensyn til »særlige regionale eller sproglige aspekter, herunder når de er specifikke for en medlemsstat« – hvilket har direkte betydning for danske forhold.

Afbødningen i **art. 35, stk. 1** skal være »rimelig, forholdsmæssig og effektiv« og skræddersyet, »under særlig hensyntagen til sådanne foranstaltningers indvirkning på grundlæggende rettigheder«. Katalogets elleve punkter spænder fra tilpasning af algoritmiske systemer (litra d) og reklamesystemer (litra e) til alderskontrol og forældrekontrol (litra j) og – bemærkelsesværdigt – mærkning af deepfakes (litra k). Bestemmelsen indeholder altså en dobbelt proportionalitetstest: foranstaltningerne skal være effektive nok til at afbøde risikoen, men må ikke selv krænke grundrettigheder.

Denne dobbelthed er nøjagtigt det spørgsmål, EU-Domstolen behandlede i **C-401/19** (Polen mod Parlamentet og Rådet) om DSM-direktivets art. 17. Dommen af 26. april 2022 er den centrale konstitutionelle præcedens for platformsforpligtelser i lyset af Chartret: en forpligtelse, der de facto tvinger platforme til at kontrollere brugerindhold, udgør et indgreb i ytringsfriheden efter **Chartrets artikel 11**, men er lovlig, når EU-lovgiver har indbygget tilstrækkelige garantier mod overfjernelse af lovligt indhold. Overført til DSA betyder det, at art. 35-foranstaltninger skal designes med de processuelle modvægte i art. 17, 20 og 21 som integreret del – ikke som eftertanke.

Krisemekanismen i **art. 36** er DSA's mest indgribende instrument. Kommissionen kan efter henstilling fra Det Europæiske Råd for Digitale Tjenester pålægge en VLOP at vurdere, om tjenesten bidrager til en alvorlig trussel mod offentlig sikkerhed eller folkesundhed, og at iværksætte specifikke foranstaltninger. Retssikkerhedsgarantierne er tilsvarende skarpe: foranstaltningerne skal være »strengt nødvendige, begrundede

og forholdsmæssige», og afgørelsen er efter [art. 36, stk. 3, litra c](#) begrænset til **højst tre måneder** ad gangen, med mulighed for forlængelse med tre måneder. Valget af de konkrete foranstaltninger forbliver hos udbyderen, jf. [stk. 5](#).

PRAKSIS EU-Domstolen · Polen mod Parlamentet og Rådet: Lovligheden af platformes filtreringsforpligtelser i 26.04.2022
ophavsretsdirektivet (Sag C-401/19)

Uafhængig revision, reklamearkiv og forskeradgang – art. 37, 39 og 40

DSA's tilsyn med VLOP'er hviler på tre eksterne kontrolmekanismer, der supplerer myndighedstilsynet.

Uafhængig revision efter [art. 37](#) sker årligt for platformens egen regning og omfatter samtlige kapitel III-forpligtelser samt tilsagn under adfærdskodekser og kriseprotokoller. Revisionserklæringen er trinopdelt – »positiv«, »positiv med bemærkninger« eller »negativ«, jf. [art. 37, stk. 4, litra g](#) – og ved en ikke-positiv erklæring skal platformen inden en måned vedtage en **revisionsrapport om gennemførelsen**, jf. [stk. 6](#). Gennemfører den ikke anbefalingerne, skal den begrunde det og redegøre for alternative foranstaltninger. Platformen skal efter [stk. 2](#) »afholde sig fra at hæmme, uretmæssigt at påvirke eller at undergrave udførelsen af revisionen« – en pligt, der spejler Domstolens betoning i [C-117/24](#) af, at due diligence-ordninger skal kunne efterprøves effektivt af den kontrollerende instans.

Reklamearkivet efter [art. 39](#) – genstanden for både Aylo- og XVideos-sagerne – kræver en søgbar, API-tilgængelig database, der dækker visningsperioden plus ét år. De syv datapunkter i [art. 39, stk. 2](#) omfatter reklamens indhold, hvem den vises på vegne af, hvem der har betalt, visningsperioden, målretningsparametrene (inklusive **eksklusionskriterier**) og antal modtagere opdelt pr. medlemsstat. Databasen må ikke indeholde personoplysninger om *modtagerne* – men [art. 39, stk. 2, litra b og c](#) kræver identifikation af annoncøren, også når denne er en fysisk person. Det var netop den asymmetri, Aylo forgæves søgte suspenderet.

Forskeradgangen efter [art. 40](#) er todelt. Efter [stk. 1](#) skal VLOP'en give koordinatoren eller Kommissionen adgang til tilsynsnødvendige oplysninger, og efter [stk. 3](#) redegøre for »udformningen, logikken, virkemåden og afprøvningen af deres algoritmiske systemer, herunder deres anbefalingssystemer« – en algoritmisk forklaringspligt over for myndighederne. Efter [stk. 4](#) kan koordinatoren i etableringslandet pålægge platformen at give **kontrolunderlagte forskere** adgang til data alene med henblik på forskning i systemiske risici. De syv betingelser i [stk. 8](#) omfatter tilknytning til en forskningsinstitution, uafhængighed af kommercielle interesser, finansieringstransparens, datasikkerhed, nødvendighed/proportionalitet og forpligtelse til gratis offentliggørelse af resultaterne.

Platformen kan efter [stk. 5](#) inden 15 dage anmode om ændring af anmodningen, men **kun** af to grunde: at den ikke har adgang til oplysningerne, eller at adgang ville skabe væsentlige sårbarheder i tjenestens sikkerhed eller for forretningshemmeligheder. Anmodningen skal da ledsages af forslag til alternative adgangsveje, jf. [stk. 6](#) – undtagelsen er altså konstrueret som en *forhandlingspligt*, ikke en veto. Danske forskere kan efter [stk. 9](#) indgive ansøgning til den danske koordinator, som foretager en indledende vurdering og videresender til etableringslandets koordinator – men den endelige afgørelse ligger hos sidstnævnte. Da ingen VLOP er etableret i Danmark, er den danske koordinators rolle her i praksis rent forberedende.

Spændingen mellem gennemsigtighed og fortrolighed er allerede prøvet på EU-plan. Den Europæiske Ombudsmand fandt i maj 2026 [fejladministration i Kommissionens afslag på aktindsigt i X's](#)

[DSA-risikovurderingsrapport](#) og udtalte, at han »remains unconvinced that a general presumption of non-disclosure can be applied to risk assessment reports drawn up under the DSA« – netop fordi rapporterne er tiltænkt offentliggørelse. Kommissionens generelle fortrolighedsformodning for DSA-undersøgelsesdokumenter er dermed under pres.

PRAKSIS	EU-Domstolen · Krav til virksomheders egne due diligence-ordninger for træ og træprodukter i koncerner	13.11.2025
	EU-Domstolen · Pornhub-sagen: EU-Domstolens afvisning af suspension af gennemsigtighedskrav under DSA	06.09.2024

§ 10 Kompetencefordelingen efter art. 56 – hvem håndhæver hvad

[Artikel 56](#) fordeler håndhævelsen i fire lag, og fordelingen er afgørende for, hvad en dansk koordinator overhovedet kan gøre:

Situation	Kompetent myndighed	Hjemmel
Almindelig formidlingstjeneste	Etableringslandets koordinator (enekompetence)	art. 56, stk. 1
VLOP/VLOSE – kapitel III, afdeling 5 (systemiske risici)	Kommissionen (enekompetence)	art. 56, stk. 2
VLOP/VLOSE – øvrige forpligtelser	Kommissionen og etableringslandet	art. 56, stk. 3 og 4
Udbyder uden EU-etablering	Den medlemsstat, hvor den retlige repræsentant er	art. 56, stk. 6
Udbyder uden retlig repræsentant	Alle medlemsstater (+ Kommissionen ved VLOP)	art. 56, stk. 7

To mekanismer forhindrer kompetencekollision. For det første fortrænger Kommissionens procedureindledning nationalt tilsyn: efter [art. 56, stk. 4](#) har etableringslandet kun kompetence over VLOP'ens ikke-systemiske forpligtelser, »hvis Kommissionen ikke har indledt en procedure for den samme overtrædelse«. Betragtning 139 begrundet dette udtrykkeligt med hensynet til at undgå »overlaping, uoverensstemmelser og risici set ud fra **ne bis in idem**-princippet«. For det andet indeholder [art. 56, stk. 7](#) en underretnings- og spærremekanisme: agter en koordinator at udøve beføjelser over for en udbyder uden retlig repræsentant, skal alle andre koordinators og Kommissionen underrettes – og efter underretningen »må andre medlemsstaters kompetente myndigheder ikke indlede procedurer for samme adfærd«.

Samarbejdet udmøntes gennem **gensidig bistand** ([art. 57](#)), **anmodning om indgriben** ([art. 58](#) – etableringslandet skal svare inden to måneder), **henvisning til Kommissionen** ([art. 59](#)) og **fælles undersøgelser** ([art. 60](#)). Det praktiske omdrejningspunkt er informationsudvekslingssystemet **AGORA**, hvis operationelle rammer er fastlagt i [Kommissionens gennemførelsesforordning \(EU\) 2024/607](#); efter [art. 6](#) er hver koordinator særskilt dataansvarlig for sine egne behandlingsaktiviteter i systemet. Procedurereglerne for Kommissionens egne kontrolbesøg, overvågning og aktindsigt findes i [gennemførelsesforordning \(EU\) 2023/1201](#).

Det Europæiske Råd for Digitale Tjenester ([art. 61-62](#)) er en uafhængig rådgivende gruppe af koordinatorene under Kommissionens formandskab. Rådet har ikke bindende beføjelser, men dets henstillinger har vægt: efter betragtning 133 skal en beslutning om at afvige fra en henstilling »forklares behørigt og kan tages i betragtning

af Kommissionen ved vurderingen af, om den pågældende medlemsstat overholder denne forordning». Hver medlemsstat har én stemme; Kommissionen har ingen.

§ 11 Den danske koordinator: udpegning, ressortvandring og uafhængighed

Danmark gennemførte de nødvendige supplerende foranstaltninger ved **lov nr. 1765 af 28. december 2023** (L 60, 2023-24), der efter § 1 »supplerer« forordningen. Forarbejderne forklarer nødvendigheden præcist:

Forordningen gælder umiddelbart i Danmark og må som udgangspunkt ikke gennemføres i national ret, jf. artikel 288 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF). Flere bestemmelser i forordningen kræver imidlertid, at der foretages visse gennemførelsesforanstaltninger.

Lovens anvendelsesområde i § 2 er trukket op efter art. 56: loven gælder, hvor Danmark er tillagt tilsyns- og håndhævelseskompetence – dvs. når udbyderen har hovedforretningssted i Danmark, når en ikke-EU-etableret udbyder har udpeget dansk retlig repræsentant, eller når en ikke-EU-etableret udbyder slet ikke har udpeget repræsentant og tjenesten er tilgængelig for danske brugere. Hertil kommer bistandssituationerne efter art. 57, stk. 2, art. 60, stk. 4, og art. 66, stk. 3.

Ressortvandringen fortjener særlig opmærksomhed, fordi loven på dette punkt ikke længere afspejler virkeligheden. Efter § 3, stk. 1 udpeges **Konkurrence- og Forbrugerstyrelsen** som kompetent myndighed og som koordinator for digitale tjenester. Forarbejderne begrundet valget med, at styrelsen var ressortmyndighed for forordningen og for e-handelsloven, og allerede var uafhængig tilsynsmyndighed for konkurrenceloven og lov om håndhævelse af P2B-forordningen. Styrelsen **meddelte i december 2023**, at brugere kunne klage fra den 17. februar 2024.

Men kort efter blev opgaven flyttet. Ved **bekendtgørelse om ændring i forretningernes fordeling mellem ministrene** (august 2024) blev bl.a. »ressortansvaret for sager vedrørende regulering af tech-virksomheder [...] ressortansvaret for DSA-tilsynet« overført fra Erhvervsministeriet til det nyoprettede Digitaliseringsministerium – bemærkelsesværdigt nok **undtaget** sager vedrørende DMA-forordningen, som blev hos Erhvervsministeriet. Tilsynet ligger siden hos **Digitaliseringsstyrelsen**, der i dag varetager både rollen som kompetent tilsynsmyndighed og som koordinator for digitale tjenester. Ved **bekendtgørelse af 11. juni 2026** blev Digitaliseringsministeriet nedlagt og forretningerne overført til Uddannelses- og Forskningsministeriet, hvis betegnelse samtidig ændredes til **Forsknings-, Uddannelses- og Digitaliseringsministeriet** – det ressort, loven i dag er registreret under på retsinformation.dk. Lovens § 3, stk. 1, henviser altså fortsat til Konkurrence- og Forbrugerstyrelsen, mens det faktiske tilsyn udøves af Digitaliseringsstyrelsen. Ved rådgivning om klageadgang bør man derfor gå efter den faktiske ressortfordeling, ikke lovteksten alene.

Uafhængigheden er lovfæstet i § 4, der gengiver art. 50, stk. 2. Forarbejderne trækker konsekvenserne skarpt op:

Regeringen har således ikke instruktionsbeføjelse over for kompetente myndigheder og koordinatoren for digitale tjenester vedrørende konkrete sager, der afgøres efter forordningen om digitale tjenester, denne lov eller regler udstedt i medfør heraf, herunder i forhold til prioritering, og udarbejdelse af vejledninger.

Uafhængigheden omfatter også deltagelsen i Det Europæiske Råd for Digitale Tjenester og afgivelsen af egne høringssvar. Og den slår igennem i ansættelsesretten: det vil efter forarbejderne »ikke være sagligt at afskedige

styrelsens ansatte af årsager relateret til en korrekt varetagelse af deres opgaver eller beføjelser som en del af en uafhængig tilsynsmyndighed« – herunder for ikke at følge en udefrakommende instruks.

Aktivitetsniveauet er højere end Danmarks størrelse tilsiger. Det danske DSA-tilsyn modtog i 2024 **119 klager**, hvoraf 17 blev videresendt til det irske tilsyn og 1 til det hollandske; 2 klager kom fra andre koordinatore. Danmark var dermed det tredje mest klageramte tilsyn i EU efter Irland og Nederlandene – på trods af at ingen VLOP eller VLOSE er etableret i Danmark. Meta er etableret i Irland, Snapchat har udpeget retlig repræsentant i Nederlandene, og Zalando er placeret i Tyskland.

LOV

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 1

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 2

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 3, stk. 1, 2

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 4

Undersøgellesbeføjelser, kontrolundersøgelser og sanktioner i dansk

§ 12 ret

Den danske håndhævelseslov supplerer forordningen på fire punkter: sagsoptagelse, kontrolundersøgelser, sanktioner og offentlighed.

Sagsoptagelse og prioritering. Efter § 5, stk. 1 kan sager optages af egen drift, på baggrund af klage eller efter anmodning fra Kommissionen eller andre koordinatore. Prioriteringen skal efter stk. 2 navnlig ske ud fra forordningens formål i art. 1 – myndigheden har altså et **opportunitetsprincip**, ikke en pligt til at behandle enhver klage. Retssikkerhedsmæssigt væsentligt er stk. 3: afgørelser »kan ikke indbringes for anden administrativ myndighed«. Der er ingen administrativ rekurs – prøvelsen sker ved domstolene.

Kontrolundersøgelser. § 6 tillægger myndighederne beføjelserne i art. 51, stk. 1-3, og § 7 udbygger dem efter mønster fra konkurrenceretten:

- Kontrolundersøgelser kræver **retskendelse** og behørig legitimation, men kan finde sted **uanmeldt**, jf. § 7, stk. 2.
- Den kontrolunderlagte har **pligt** til at underkaste sig undersøgelsen, jf. stk. 3.
- Myndigheden kan efter stk. 4 kræve, at udbyderen »giver adgang til og forklarer **it-systemers og algoritmers funktioner og strukturer**« – en national algoritmeforklaringspligt, der spejler DSA art. 40, stk. 3.
- Stk. 5 regulerer digital spejling detaljeret: data skal forsegles inden undersøgelsens afslutning, den kontrollerede kan kræve at overvære gennemgangen, kopi skal udleveres senest 40 hverdage efter, og data skal slettes, hvis der ikke findes dokumentation for overtrædelse – eller når sagen er endeligt afgjort.
- Forsegling kan ske i op til 3 hverdage, jf. stk. 6, og politiet kan yde bistand, jf. stk. 9.

Rammerne for sådanne beføjelser er trukket op i forordningens betragtning 116, hvorefter udøvelsen skal sikre »de grundlæggende rettigheder til effektive retsmidler og til en upartisk domstol, herunder retten til et forsvar, og retten til respekt for privatlivet«, og skal stå i rimeligt forhold til overtrædelsens karakter og skade.

Sanktionerne følger en trappe:

Reaktion	Ramme	Hjemmel
Påbud om ophør	Frist fastsættes af myndigheden	§ 8
Daglige/ugentlige tvangsbøder	Op til 5 pct. af gennemsnitlig daglig global omsætning	§ 9, stk. 2
Bøde for materiel overtrædelse	Op til 6 pct. af global omsætning	§ 10, stk. 1 og 3
Bøde for manglende påbudsefterlevelse	Op til 1 pct. af global omsætning eller indkomst	§ 10, stk. 2 og 3

Rammerne svarer nøjagtigt til [art. 52, stk. 3 og 4](#). Ved udmåling lægges der efter [§ 10, stk. 4](#) vægt på omsætningen, og i **skærpende** retning på samtidig pådømmelse af flere overtrædelser. Juridiske personer kan straffes efter straffelovens 5. kapitel, jf. [stk. 5](#).

Administrative bødeforelæg efter [§ 11](#) er begrænset til de mest ukomplicerede sager: enten de udtrykkeligt opregnede bestemmelser i stk. 1, eller – efter [stk. 3](#) – tilfælde hvor overtræderen »ikke har opfyldt **noget** af pligten«. Forudsætningen er en skyldserklæring, og vedtagelse har samme virkning som en dom. Mere komplicerede sager skal for domstolene.

Offentlighed. [§ 12, stk. 1](#) undtager DSA-sager fra offentlighedsloven bortset fra notat- og journaliseringspligten i lovens §§ 13 og 15 – og undtagelsen følger med, hvis oplysningerne videregives til en anden forvaltningsmyndighed. Til gengæld pålægger [stk. 2](#) myndigheden aktivt at **offentliggøre** påbud samt domme og bødevedtagelser, dog med redigering for forretningshemmeligheder af væsentlig økonomisk betydning, jf. [stk. 3](#). Modellen er altså lukket sagsbehandling, offentligt resultat.

LOV

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 5, stk. 1-3](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 6](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 7, stk. 2-9](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 8](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 9, stk. 1, 2](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 10, stk. 1-5](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 11, stk. 1, 3](#)

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 12, stk. 1-3](#)

DMA's gatekeeper-regime: udpegelse efter art. 3 og § 13 adfærdsforpligtelserne

DMA vender logikken om. Hvor DSA regulerer *processer*, forbyder og påbyder DMA konkrete *adfærdstyper* – og gør det ex ante, uden krav om påvisning af dominans eller konkurrenceskade.

Udpegelsen efter [art. 3, stk. 1](#) hviler på tre materielle kriterier: betydelig indvirkning på det indre marked, status som vigtig gateway for erhvervsbrugere, og en grundfæstet og varig stilling. [Stk. 2](#) omsætter dem til kvantitative **formodninger**:

Kriterium	Tærskel
Betydelig indvirkning (litra a)	Årlig EU-omsætning $\geq$ 7,5 mia. EUR i hvert af de seneste tre regnskabsår, eller markedsværdi $\geq$ 75 mia. EUR – plus samme tjeneste i mindst 3 medlemsstater
Vigtig gateway (litra b)	$\geq$ 45 mio. månedlige aktive slutbrugere og $\geq$ 10.000 årlige aktive erhvervsbrugere i EU
Grundfæstet stilling (litra c)	Litra b opfyldt i hvert af de seneste tre regnskabsår

Virksomheden skal selv underrette Kommissionen inden to måneder efter tærskeloverskridelse ([stk. 3](#)), og udpegelsen sker inden 45 arbejdsdage ([stk. 4](#)). Undlader virksomheden at underrette **og** at besvare en anmodning efter art. 21, kan Kommissionen udpege den på grundlag af de foreliggende oplysninger – samme mekanisme som DSA art. 33, stk. 4.

Modbevisadgangen i [art. 3, stk. 5](#) er snæver. Virksomheden kan fremlægge »tilstrækkeligt underbyggede argumenter« for, at den undtagelsesvis ikke opfylder de materielle kriterier – men Kommissionen kan **afvise** argumenterne uden markedsundersøgelse, hvis de ikke »klart rejser tvivl om formodningerne«. Kun hvis argumenterne klart rejser tvivl, indledes proceduren i art. 17, stk. 3. Omvendt kan Kommissionen efter [art. 3, stk. 8](#) udpege en virksomhed, der **ikke** når tærsklerne, på grundlag af syv kvalitative elementer – netværkseffekter, datadrevne fordele, fastlåsnings og skifteomkostninger, konglomeratstruktur og vertikal integration mv. Forpligtelserne indtræder seks måneder efter udpegelsen, jf. [stk. 10](#).

Denne konstruktion er blevet prøvet. EU-Retten [afviste den 8. juli 2026 Apples anfægtelse af gatekeeper-udpegelsen for App Store og iOS](#) (sagerne **T-1080/23** og **T-214/24**) – den første realitetsprøvelse af DMA's udpegelsessystem, og et resultat der bekræfter formodningsmodellens robusthed.

Adfærdsforpligtelserne fordeler sig på tre artikler:

Artikel 5 – umiddelbart anvendelige forbud og påbud:

- [Stk. 2](#): forbud mod at **kombinere og krydsanvende persondata** på tværs af tjenester uden specifikt valg og GDPR-gyldigt samtykke. Afvises samtykket, må gatekeeperen kun spørge igen **én gang om året**. Bestemmelsen er den direkte DMA-parallell til det, EU-Domstolen behandlede databeskyttelsesretligt i [C-446/21](#).
- [Stk. 3-4](#): forbud mod **paritetsklausuler** og ret for erhvervsbrugere til at kommunikere og kontrahere frit uden for platformen – kernen i **anti-steering**.
- [Stk. 6](#): forbud mod at hindre erhvervs- eller slutbrugere i at rejse spørgsmål om gatekeeperens manglende regelefterlevelse over for offentlige myndigheder, herunder nationale retter.
-

Stk. 7: forbud mod at kræve brug af gatekeeperens egen identifikationstjeneste, browsermotor eller betalingssystem.

- **Stk. 9-10:** daglig, gratis reklameprisgennemsigtighed over for annoncører og udgivere.

Artikel 6 – forpligtelser der kan præciseres efter art. 8:

- **Stk. 2:** forbud mod at bruge erhvervsbrugeres **ikke-offentligt tilgængelige data** i konkurrence med dem – udtrykkeligt inklusive klik-, søge-, visnings- og taledata.
- **Stk. 3-4:** afinstallation, ændring af standardindstillinger, **valgskærme** ved førstegangsbrug, og **sideloading** af tredjeparts-appbutikker. Sikkerhedsundtagelsen er dobbelt betinget: foranstaltningerne skal være »strengt nødvendige og forholdsmæssige« og behørigt begrundet af gatekeeperen.
- **Stk. 5:** forbuddet mod **selvbegunstigelse** – gatekeeperen må ikke behandle egne tjenester eller produkter mere gunstigt i rangordningen og skal anvende »gennemsigtige, retfærdige og ikkediskriminerende betingelser«.
- **Stk. 9-11:** dataportabilitet i realtid for slutbrugere, dataadgang for erhvervsbrugere (personoplysninger dog kun med slutbrugerens samtykke), og FRAND-adgang til søgedata for konkurrerende søgemaskiner – med anonymisering af personoplysninger.

Artikel 7 – **interoperabilitet** for nummeruafhængige interpersonelle kommunikationstjenester, udrullet i tre trin (ved udpegelsen, efter to år, efter fire år). To garantier er indbygget: sikkerhedsniveauet, herunder eventuel end-to-end-kryptering, skal opretholdes på tværs af de interoperable tjenester (**stk. 3**), og der må kun udveksles de personoplysninger, der er »strengt nødvendige«, i fuld overensstemmelse med GDPR (**stk. 8**). Slutbrugeren bestemmer selv, om funktionaliteten skal bruges (**stk. 7**).

Bøderammerne i **art. 30** er EU-rettens skarpeste: op til **10 pct.** af den samlede globale omsætning ved forsætlig eller uagtsom tilsidesættelse af art. 5, 6 eller 7 (**stk. 1**) – og op til **20 pct.** ved samme eller lignende tilsidesættelse vedrørende samme centrale platformstjeneste inden for de foregående **otte år** (**stk. 2**). Procedureovertrædelser – herunder manglende underretning efter art. 3, stk. 3, og undladelse af at oprette en compliancefunktion efter art. 28 – koster op til 1 pct. (**stk. 3**).

Kommissionen udstedte i april 2025 de første afgørelser om manglende overholdelse: mod **Meta** for »pay or consent«-reklamemodellen og mod **Apple** for tilsidesættelse af anti-steering-forpligtelsen. Europa-Parlamentet **kritiserede i april 2026 bødeniveauet som beskedent** og fremhævede vedvarende bekymringer om Googles selvbegunstigelse, TikToks brug af adfærdspåvirkende samtykkeskærme, Microsofts standardindstillinger og Booking.coms fortsatte paritetsklausuler. I november 2025 indledte Kommissionen undersøgelser af, om **Amazon Web Services** og **Microsoft Azure** skal udpeges som gatekeepere for cloudtjenester, og den 28. april 2026 offentliggjordes den første DMA-review.

PRAKSIS **EU-Domstolen** · Dataminimering og behandling af følsomme personoplysninger til personaliseret reklame på sociale netværk 04.10.2024

§ 14 Samspillet med GDPR, P2B-forordningen og markedsføringsretten

DSA og DMA lever i et tæt reguleret nabolag, og afgrænsningen har praktisk betydning for, hvilken myndighed man skal gå til.

P2B-forordningen ([forordning \(EU\) 2019/1150](#)) regulerer forholdet mellem platform og **erhvervsbruger**, hvor DSA regulerer forholdet til **tjenestemodtageren** bredt. Overlappene er markante: [P2B art. 5](#) kræver, at de vigtigste rangordningsparametre og »årsagerne til den relative betydning af disse vigtigste parametre« oplyses i vilkårene – næsten ordret det samme som DSA art. 27, stk. 2, litra b, blot rettet mod erhvervsbrugere. [P2B art. 4](#) kræver begrundelse på varigt medium ved begrænsning, suspension eller ophør – DSA art. 17's forgænger. Og forordningen har samme genindsættelsespligt ved tilbagekaldelse. Ifølge P2B's betragtning 27 kan hensynet til kommercielle interesser »aldrig føre til afslag på at oplyse om de vigtigste parametre, der afgør rangordningen« – en fortolkningsanvisning der med god ret kan overføres til DSA art. 27.

P2B-forordningen håndhæves i Danmark af Konkurrence- og Forbrugerstyrelsen. Styrelsen [rapporterede i februar 2026](#), at danske virksomheder oplever reglerne som uklare, og at et kommissionsforslag vil videreføre bl.a. art. 4 og art. 11 frem til 31. december 2032. Den territoriale grænse blev trukket af EU-Domstolen i [C-665/22](#): nationale indberetningskrav over for platforme etableret i andre medlemsstater strider mod hjemlandsprincippet.

GDPR er DSA's vigtigste nabo. DSA regulerer *gennemsigtighed og proces*; GDPR regulerer *lovligheden* af selve databehandlingen. To sager illustrerer grænsefladen. I [C-492/23](#) tog Domstolen stilling til, hvornår operatøren af en onlinemarkedsplads er **dataansvarlig** for følsomme oplysninger i brugerannoncer – et spørgsmål DSA slet ikke besvarer, men som afgør, hvem der bærer GDPR-ansvaret for det indhold, DSA's notice-and-action-mekanisme håndterer. Og i [C-175/20](#) fastslog Domstolen, at en myndigheds indsamling af store datamængder fra en onlineportal er underlagt GDPR art. 5, og at myndigheden ikke kan fravige dataminimeringsprincippet uden klar og præcis lovhjemmel:

Den dataansvarlige, herunder når denne handler inden for rammerne af den opgave i samfundets interesse, som vedkommende er blevet pålagt, [kan] ikke generelt og udifferentieret [...] foretage indsamling af personoplysninger, og [...] skal afholde sig fra at indsamle oplysninger, som ikke er strengt nødvendige, henset til formålene med behandlingen.

Dommen har direkte betydning for udøvelsen af undersøgelsesbeføjelserne efter DSA art. 51 og [§ 7](#): også en DSA-koordinator skal proportionalitetsafgrænse sin dataindsamling – hvilket netop er baggrunden for lovens detaljerede sletteregler i § 7, stk. 5. Beslægtet er [C-136/17](#), hvor Domstolen pålagde søgemaskineudbydere en **strengere prøvelse** ved anmodninger om fjernelse af links til følsomme oplysninger – en afvejningsmodel, der ligger tæt på DSA art. 16's krav om omhyggelig og objektiv anmeldelsesbehandling.

Markedsføringsretten er tredje nabo. DSA art. 25, stk. 2, viger udtrykkeligt for direktiv 2005/29/EF, og Forbrugerombudsmanden fastholder sin kompetence over platformes egen handelspraksis. Ombudsmanden [fastslog i marts 2024](#), at onlineplatforme har ansvar for vildledende grøn markedsføring, og analyserede eksplicit forholdet mellem DSA art. 6's ansvarsfritagelse og markedsføringslovens §§ 5, 6 og 13. Grænsen mellem platformens *eget budskab* og brugerens indhold er trukket af EU-Domstolen i [C-148/21](#) (Louboutin mod Amazon): en hybrid platform gør selv brug af et varemærke, hvis

en almindeligt oplyst og rimeligt opmærksom bruger af dette websted skaber en forbindelse mellem denne operatørs tjenesteydelser og det pågældende tegn [...] [og] kan få det indtryk, at det er den nævnte operatør, der selv i sit eget navn og for egen regning markedsfører de varer, der er forsynet med det nævnte tegn.

Ensartet præsentation af egne og tredjeparters tilbud, eget distributørlogo på alle annoncer og supplerende logistikydelser trækker i retning af egen brug. Kriteriet er retligt beslægtet med DSA's krav om, at forbrugeren skal kunne se, at handlen sker med en tredjepartssælger – en pligt, [ekspertgruppen om tech-giganters rolle](#)

i december 2024 kritiserede for at kunne opfyldes »på mange måder«, uden at det i praksis bliver tydeligt for forbrugeren, hvem der bærer ansvaret. I forlængelse heraf ligger [C-76/24](#), hvor Domstolen fastslog, at territorialitetsprincippet ikke må kunne omgås ved blot at flytte lageret til udlandet, når onlineudbuddet er målrettet beskyttelseslandet – samme funktionelle tilgang som DSA's tilknytningskriterium.

Endelig afgrænser [C-697/23](#) (Check24) og [C-100/24](#) (bonprix) de markedsføringsretlige begreber, der grænser op til DSA's reklameregler – henholdsvis at en ren sammenligningstjeneste ikke er »konkurrent« og derfor falder uden for sammenlignende reklame, og at et »reklametilbud« omfatter enhver objektiv, sikker og adfærdspåvirkende fordel. Ældre praksis som [C-146/16](#) (DHL Paket) viser den strukturelt tilsvarende afvejning: oplysninger kan gives via platformen frem for i selve reklamen, forudsat de er nemt og hurtigt tilgængelige.

En fjerde nabo er under opbygning: [forordning \(EU\) 2024/900 om gennemsigtighed i politisk reklame](#), der lægger et sektorspecifikt lag oven på DSA art. 26 og 39. Og på det svindelbekæmpende felt sikrede det danske EU-formandskab i december 2025 [en aftale om, at store platforme skal verificere annoncører af finansielle tjenester](#) og potentielt betale erstatning, hvis de er informeret om svindelindhold og ikke fjerner det.

LOV

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 7, stk. 5

PRAKSIS	EU-Domstolen · Operatøren af en onlinemarkedsplads som dataansvarlig for følsomme oplysninger i annoncer	02.12.2025
	EU-Domstolen · Varemærkeindehaveres ret til at forbyde oplagring af varer i udlandet ved målrettet onlinesalg	01.08.2025
	EU-Domstolen · Fortolkning af begrebet 'reklametilbud' ved onlinereklamer for betaling på faktura	15.05.2025
	EU-Domstolen · Kvalificering af onlinetjenester til sammenligning af forsikringer som 'sammenlignende reklame' og kravet om et konkurrenceforhold	08.05.2025
	EU-Domstolen · Nationale indberetningskrav for onlineplatforme i strid med princippet om hjemlandskontrol	30.05.2024
	EU-Domstolen · Louboutin mod Amazon: Ansvar for varemærkekrænkelser på online markedspladser ved blandet forretningsmodel	22.12.2022
	EU-Domstolen · Skattemyndigheders adgang til personoplysninger fra online-portaler og overholdelse af GDPR-principper	24.02.2022
	EU-Domstolen · Søgemaskineudbydere forpligtelser ved behandling af følsomme personoplysninger og retten til at blive glemt	24.09.2019
	EU-Domstolen · Krav om oplysning af erhvervsdrivendes identitet i trykte reklamer for onlineplatforme (DHL Paket)	29.03.2017

§ 15 Sammenfatning: hvor står praksis i dag

Praksis på DSA/DMA-området er stadig ung, men mønstrene er allerede tydelige – og de peger konsekvent i retning af **håndhævelsens forrang**.

1. Udepegsen står ved magt, mens sagen kører. Tre afgørelser inden for godt et år – [C-647/23](#) (Zalando), [C-511/24](#) (Aylo) og [C-620/24](#) (WebGroup) – viser, at Unionens retsinstanser ikke suspenderer DSA-forpligtelser, mens annullationssøgsmål verserer. Den metodiske nøgle er vicepræsidentens præcisering i Aylo: interesseafvejningen foretages ud fra den antagelse, at hovedsagen ikke tages til følge, og Kommissionens VLOP-vurdering lægges derfor til grund. En platform kan altså ikke via foreløbige forholdsregler få prøvet, om

den overhovedet er en VLOP. Kombineret med, at forpligtelserne indtræder fire måneder efter meddelelsen efter [art. 33, stk. 6](#), betyder det, at compliance i praksis skal være på plads, længe før retten har taget stilling.

2. Rent økonomisk skade rækker ikke. Aylo påberåbte sig annoncørflugt og risiko for en »doxing-liste«. Domstolen afviste: tredjeparters skade, der er forskellig fra den påberåbte uopsættelighedsskade, kan ikke bære en foreløbig forholdsregel, og selskabet havde ikke dokumenteret, at annonceindtægterne fra fysiske personer truede dets langsigtede eksistens. Barren for suspension af DSA-forpligtelser ligger derfor meget højt.

3. Grundrettighedsafvejningen er indbygget, ikke efterfølgende. [C-401/19](#) fastslår, at platformsförpligtelser der berører ytringsfriheden kun består, når lovgiver har indbygget garantier mod overfjernelse. DSA er konstrueret efter denne skabelon: art. 34, stk. 1, litra b, gør grundrettighedspåvirkning til en selvstændig systemisk risiko, art. 35, stk. 1, kræver hensyn til grundrettighederne ved afbødningen, og art. 17, 20 og 21 leverer de processuelle modvægte. Omvendt sætter [C-555/23](#) grænsen den anden vej: bødehemler kan ikke udvides ved analogi, heller ikke for at reparere en mangelfuld gennemførelse.

4. Totalharmoniseringen binder også dansk lovgiver. Rigsadvokatmeddelelsen om e-cigaretter dokumenterer, at et nationalt alderskontrollkrav ikke kan pålægges onlineplatforme, fordi art. 28 dækker feltet. Sammen med hjemlandsprincippet i [C-665/22](#) efterlader det et snævert nationalt råderum – hvilket i praksis gør Kommissionen til den afgørende aktør på VLOP-området.

5. Den danske koordinator er struktureret som klageomfordeler. Uden VLOP'er etableret i Danmark ligger den reelle håndhævelse over tech-giganterne hos Kommissionen og de irske, hollandske og tyske koordinators. Alligevel modtog det danske tilsyn 119 klager i 2024 – tredje flest i EU – hvoraf 18 blev videregivet. Den danske koordinators mest markante bidrag er derfor foreløbig tildelingen af status som pålidelig indberetter og den forberedende vurdering af danske forskeres dataadgangsansøgninger efter [art. 40, stk. 9](#).

6. Regelgrundlaget er i bevægelse – men loven står stille. Lov nr. 1765 af 28. december 2023 er aldrig blevet ændret eller konsolideret, og der er ingen vedtagne, ikke-konsoliderede ændringer. Til gengæld har ressortet flyttet sig to gange siden vedtagelsen: fra Erhvervsministeriet til Digitaliseringsministeriet i 2024 og videre til Forsknings-, Uddannelses- og Digitaliseringsministeriet i juni 2026. Konsekvensen er, at lovens [§ 3, stk. 1](#) fortsat udpeger Konkurrence- og Forbrugerstyrelsen, mens tilsynet faktisk udøves af Digitaliseringsstyrelsen. Bemyndigelsen i [§ 3, stk. 2](#) til at udpege andre kompetente myndigheder er endnu ikke udnyttet i en selvstændig bekendtgørelse.

7. DMA-håndhævelsen er trådt ind i realitetsfasen. Kommissionens første non-compliance-afgørelser mod Meta og Apple i april 2025, EU-Rettens stadfæstelse af Apples gatekeeper-udpegelse i juli 2026, de igangværende cloud-undersøgelser mod AWS og Azure, og Europa-Parlamentets kritik af bødeniveauet i april 2026 tegner tilsammen et billede af et regime, der er ved at finde sit leje – men hvor spørgsmålet om, hvorvidt 10/20-procentsrammerne faktisk udnyttes, endnu er åbent.

LOV

[Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 3, stk. 1, 2](#)

PRAKSIS	EU-Domstolen · Beskyttelse af den menneskelige værdighed i online-medietjenester og grænserne for overensstemmende fortolkning i straffesager	26.06.2025
	EU-Domstolen · Afvisning af appel om opsættende virkning for XVideos' gennemsigtighedsforpligtelser under retsaktens om digitale tjenester (DSA)	25.02.2025
	EU-Domstolen · Pornhub-sagen: EU-Domstolens afvisning af suspension af gennemsigtighedskrav under DSA	06.09.2024

EU-Domstolen · Nationale indberetningskrav for onlineplatforme i strid med princippet om hjemlandskontrol	30.05.2024
EU-Domstolen · Domstolen ophæver afslag på intervention i sag om Zalandos status som meget stor onlineplatform	11.01.2024
EU-Domstolen · Polen mod Parlamentet og Rådet: Lovligheden af platformes filtreringsforpligtelser i ophavsretsdirektivet (Sag C-401/19)	26.04.2022

REFERENCE Lovgrundlag

6 paragraffer

Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 3	stk. 1	Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 5	stk. 3
Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 7	stk. 2	Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 9	stk. 2
Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 10	stk. 1, 3	Lov om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester § 12	stk. 1

MATERIALE Citerede afgørelser

20 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		17
02.12.2025	Operatøren af en onlinemarkedsplads som dataansvarlig for følsomme oplysninger i annoncer	C-492/23
13.11.2025	Krav til virksomheders egne due diligence-ordninger for træ og træprodukter i koncerner	C-117/24
01.08.2025	Varemærkeindehaveres ret til at forbyde oplagring af varer i udlandet ved målrettet onlinesalg	C-76/24
26.06.2025	Beskyttelse af den menneskelige værdighed i online-medietjenester og grænserne for overensstemmende fortolkning i straffesager	C-555/23
15.05.2025	Fortolkning af begrebet 'reklametilbud' ved onlinereklamer for betaling på faktura	C-100/24
08.05.2025	Kvalificering af onlinetjenester til sammenligning af forsikringer som 'sammenlignende reklame' og kravet om et konkurrenceforhold	C-697/23
25.02.2025	Afvisning af appel om opsættende virkning for XVideos' g ennemsigtighedsforpligtelser under retsaken om digitale tjenester (DSA)	C-620/24
21.11.2024	Definition af »virksomhed« og »omsætning« ved salg af træ til fældning efter EU's tømmerforordning	C-370/23
04.10.2024	Dataminimering og behandling af følsomme personoplysninger til personaliseret reklame på sociale netværk	C-446/21

06.09.2024	Pornhub-sagen: EU-Domstolens afvisning af suspension af gennemsigtighedskrav under DSA	C-511/24
30.05.2024	Nationale indberetningskrav for onlineplatforme i strid med princippet om hjemlandskontrol	C-665/22
11.01.2024	Domstolen ophæver afslag på intervention i sag om Zalando's status som meget stor onlineplatform	C-647/23
22.12.2022	Louboutin mod Amazon: Ansvar for varemærkekrænkelser på online markedspladser ved blandet forretningsmodel	C-148/21
26.04.2022	Polen mod Parlamentet og Rådet: Lovligheden af platformes filtreringsforpligtelser i ophavsretsdirektivet (Sag C-401/19)	C-401/19
24.02.2022	Skattemyndigheders adgang til personoplysninger fra online-portaler og overholdelse af GDPR-principper	C-175/20
24.09.2019	Søgemaskineudbydere forpligtelser ved behandling af følsomme personoplysninger og retten til at blive glemt	C-136/17
29.03.2017	Krav om oplysning af erhvervsdrivendes identitet i trykte reklamer for onlineplatforme (DHL Paket)	C-146/16

FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS

3

19.02.2024	Vildledende samtykkeflow: Forsikringsselskab indskærpes for aggressiv markedsføringspraksis
08.09.2021	Samtykke til markedsføring og 'tabt kurv-påmindelser' i online købsflow
25.08.2014	Forhåndsafkrydsning af pladsbillet er i strid med god markedsføringsskik

08

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over GDPR-erstatning (databeskyttelsesforordningen art. 82)

Betingelser, bevisbyrde og udmåling efter Højesterets Gladsaxe-dom

Version 2 · Opdateret 16. jul. 2026 · 20 afgørelser · 2021-2026

[Læs online](#)**INTRODUKTION**

Databeskyttelsesforordningens artikel 82 giver den registrerede et selvstændigt civilretligt krav på erstatning for materiel og immateriel skade som følge af uberettiget behandling af personoplysninger – et krav, der er gennemført ordret i databeskyttelseslovens § 40, og som kun kan rejses ved domstolene. EU-Domstolen har i en lang række domme siden 2023 fastlagt tre kumulative betingelser (overtrædelse, konkret skade og årsagssammenhæng), afvist enhver bagatelgrænse for immateriel skade og samtidig fastholdt, at det er den registrerede, der bærer bevisbyrden for skaden. Højesteret satte med dommen af 19. december 2025 i Gladsaxe-sagen den danske ramme: frygt for fremtidigt misbrug af lække oplysninger kan udgøre en erstatningsberettiget immateriel skade, men kun når frygten er velbegrundet og både frygten og dens negative konsekvenser er behørigt bevist. Udmålingen er rent kompenserende – ikke pønalt – og de danske beløb er tilsvarende moderate.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Artikel 82, stk. 1, stiller tre kumulative betingelser: en overtrædelse af forordningen, en konkret materiel eller immateriel skade og årsagssammenhæng mellem de to – overtrædelsen i sig selv giver ikke ret til erstatning.
- 02** Der gælder ingen bagatel- eller alvorstærskel for immateriel skade, men den registrerede bærer selv bevisbyrden for både skaden og årsagssammenhængen.
- 03** Immateriel skade omfatter negative følelser som frygt eller utilfredshed udløst af tab af kontrol over oplysningerne, potentielt misbrug eller krænkelse af omdømme – forudsat at følelserne og deres negative konsekvenser godtgøres.
- 04** Frygt for fremtidigt misbrug af lække oplysninger kan i sig selv være en erstatningsberettiget skade, men kun hvis frygten er velbegrundet under de specifikke omstændigheder og for den pågældende person, og både frygten og dens negative konsekvenser er behørigt bevist.
- 05** Den blotte henvisning til en frygt – uden godtgjorte negative konsekvenser – udløser ikke erstatning efter artikel 82.

- 06 Artikel 82, stk. 2 og 3, fastsætter et præsumptionsansvar (culpa med omvendt bevisbyrde): den registrerede beviser overtrædelse, skade og kausalitet, mens den dataansvarlige skal bevise, at vedkommende ikke er skyld i den skadevoldende begivenhed.
- 07 En dataansvarlig kan ikke fritages efter artikel 82, stk. 3, blot ved at henvise til, at fejlen blev begået af en medarbejder, der handlede i strid med instruksen, jf. artikel 29.
- 08 Er flere dataansvarlige eller databehandlere involveret i samme behandling, hæfter de solidarisk for hele skaden over for den registrerede med indbyrdes regres, jf. artikel 82, stk. 4 og 5.
- 09 Erstatningen efter artikel 82 er rent kompenserende – den har hverken pønal eller afskrækkende funktion – og bødekriterierne i artikel 83 kan derfor ikke anvendes ved udmålingen.
- 10 Graden af skyld hos den dataansvarlige er uden betydning for erstatningens størrelse.
- 11 Når den lidte skade ikke er alvorlig, kan der tilkendes en ubetydelig erstatning; dansk praksis ligger derfor lavt – fx 2.500 kr. for uberettiget videregivelse af en helbredsdiagnose.
- 12 En undskyldning kan efter EU-retten være tilstrækkelig godtgørelse, men Højesteret har fastslået, at der ikke i dansk ret på nuværende tidspunkt er hjemmel til den godtgørelsesform.
- 13 Artikel 82 fortrænger ikke tortgodtgørelse efter erstatningsansvarslovens § 26, der kræver en kvalificeret, culpøs krænkelse af en vis grovhed – de to grundlag påberåbes side om side, men med forskellige betingelser og markant forskellige beløbsniveauer.
- 14 Kravet skal rejses ved domstolene, jf. artikel 82, stk. 6 – hverken Datatilsynet eller Folketingets Ombudsmand kan tilkende erstatning.
- 15 Betænkning nr. 1565/2017 forudsatte, at artikel 82 næppe dækkede ikke-økonomisk skade i en dansk kontekst; den forudsætning er efterfølgende underkendt af EU-Domstolens praksis.

§ 1 Artikel 82 og databeskyttelseslovens § 40 – én bestemmelse i to lag

Det civilretlige erstatningskrav ved uberettiget behandling af personoplysninger hviler på [databeskyttelsesforordningens artikel 82](#), der som forordningsbestemmelse gælder umiddelbart i Danmark. Bestemmelsens kerne er stk. 1:

Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

[Databeskyttelseslovens § 40](#) gentager reglen på nationalt niveau:

Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov og databeskyttelsesforordningen, har ret til erstatning efter databeskyttelsesforordningens artikel 82.

Paragraffen har ikke selvstændigt indhold. Af de paragrafspecifikke forarbejder til bestemmelsen – fremsat som [lovforslag nr. L 68 af 25. oktober 2017](#) og vedtaget som **lov nr. 502 af 23. maj 2018** – fremgår det udtrykkeligt:

Bestemmelsen er en ordret gennemførelse af forordningens artikel 82, stk. 1. Som det fremgår af betænkningen, side 917, udvider forordningsbestemmelsen gældende ret, ved at databehandleren også kan være erstatningsansvarlig. Derudover præciserer bestemmelsen ordlydsmæssigt, at der er ret til erstatning for materiel og immateriel skade [...] Derudover fastsætter forordningens artikel 82, stk. 2 og 3, at der fortsat gælder et præsumptionsansvar. Det præciseres i forordningens artikel 82, stk. 4 og 5, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for regres.

Hele bestemmelsens arkitektur kan opsummeres således:

Stykke	Indhold
Stk. 1	Retten til erstatning for materiel og immateriel skade
Stk. 2	Hæftelsessubjekterne – dataansvarlig altid, databehandler kun ved brud på databehandlerspecifikke pligter eller instruksbrud
Stk. 3	Ansvarsfritagelse, hvis den pågældende beviser ikke at være skyld i den skadevoldende begivenhed
Stk. 4 og 5	Solidarisk hæftelse og indbyrdes regres
Stk. 6	Værneting – kravet anlægges ved domstolene, jf. artikel 79, stk. 2

Det praktisk afgørende er, at forordningen – i modsætning til bøderegerne i [artikel 83](#) – hverken fastsætter beløbsrammer, takster eller udmålingskriterier. Som Justitsministeriets databeskyttelsesudvalg bemærkede i [Betænkning nr. 1565/2017, Del I, bind 2, s. 267](#):

Derudover fastsætter forordningen ikke i artikel 82, stk. 1, de nærmere betingelser for at fastslå erstatningsansvaret og den deraf følgende erstatningssum, i modsætning til området for administrative bøder, jf. forordningens artikel 83, stk. 1-6, hvor forordningen er meget udtrykkelig i forhold til bødestørrelserne.

Udfyldningen er derfor overladt til EU-Domstolen (for betingelserne) og til de nationale domstole (for udmålingen), inden for rammerne af ækvivalens- og effektivitetsprincipperne.

LOV

[Databeskyttelsesforordningen § 79, stk. 2](#)[Databeskyttelsesforordningen § 82](#)[Databeskyttelsesforordningen § 83](#)[Databeskyttelsesloven § 40](#)

Betænkning nr. 1565/2017: lovgivers forudsætning, som § 2 EU-Domstolen har overhalet

En praksisoversigt over artikel 82 kan ikke læses uden det forarbejds-mæssige udgangspunkt – for det er blevet overhalet af EU-Domstolen. Forarbejderne til [databeskyttelseslovens § 40](#) henviser i det hele til [Betænkning nr. 1565/2017, Del I, bind 2, afsnit 9.6 \(s. 910-918\)](#) samt til afsnit 2.8 i lovforslagets almindelige bemærkninger.

Gældende ret før forordningen. Persondatalovens § 69 gennemførte databeskyttelsesdirektivets artikel 23 og fastsatte et præsumptionsansvar for den dataansvarlige. Om rækkevidden anførte [Betænkning nr. 1483/2006 om tv-overvågning, s. 73](#):

Bestemmelsen antages navnlig at omfatte økonomisk skade. Hvis den konkrete skade vedrører en krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, og krænkelsen ikke har ledt til et formuetab, er der således formentlig alene mulighed for en økonomisk kompensation, hvis det i øvrigt følger af lov.

Den "anden lovregel" var [erstatningsansvarslovens § 26](#) om tortgodtgørelse. Databeskyttelsesudvalget bekræftede i [betænkning nr. 1565/2017, s. 256](#), at Justitsministeriet havde lagt til grund, at godtgørelse uden formuetab "falder uden for persondatalovens § 69", og at kravet i stedet måtte gøres gældende efter § 26 – hvorimod Registerudvalget i [Betænkning nr. 1345/1997](#) havde ment, at også ikke-økonomisk skade var omfattet.

Udvalgets konklusion i 2017. Da udvalget skulle vurdere forordningens artikel 82, nåede det til et resultat, som i dag er forladt. På [s. 267](#) hedder det:

*På det foreliggende grundlag, herunder med den foreliggende praksis fra EU-Domstolen og EU-lovgiver, er der således ikke tilstrækkelig grundlag for at fastslå, at **godtgørelse** for ikke-økonomisk skade er omfattet af retten til **erstatning** for materiel eller immateriel skade efter artikel 82, stk. 1. I hvert fald ikke, hvis der i en medlemsstat ikke normalt uden særskilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. Immateriel skade i forordningens forstand må, i en dansk kontekst, antageligvis forstås som den almindelige eller rene formueskade [...]*

Denne forudsætning holdt ikke. EU-Domstolen har siden fastslået, at begreberne "materiel eller immateriel skade" og "erstatning" i artikel 82, stk. 1, er **selvstændige EU-retlige begreber**, som ikke kan defineres ved henvisning til national ret – netop det synspunkt, Højesteret gengav i Gladsaxe-dommen med henvisning til [C-200/23](#), præmis 139. Immateriel skade dækker i dag netop de negative følelser, som udvalget i 2017 antog faldt uden for bestemmelsen.

To punkter fra betænkningen står derimod uændret. For det første konstaterede udvalget på [s. 268](#), at forordningen udvider gældende ret:

Artikel 82, stk. 1, udvider gældende ret ved at også databehandlere kan være erstatningsansvarlige.

For det andet fastslog udvalget samme sted, at artikel 82 ikke fortrænger den nationale tortregel:

Forordningens artikel 82, stk. 1, ændrer ikke på den mulighed, der eksisterer efter dansk ret, til i visse tilfælde, at udbetale godtgørelse for tort i medfør af erstatningsansvarslovens § 26 for en ikke-økonomisk skade. En sådan bestemmelse må anses for at være en sanktion efter forordningens artikel 84 [...]

De to spor – artikel 82 og [erstatningsansvarslovens § 26](#) – løber derfor side om side, og det er præcis det, den danske praksis viser.

LOV

Databeskyttelsesforordningen § 82, stk. 1

Databeskyttelsesforordningen § 84

Databeskyttelsesloven § 40

Erstatningsansvarsloven § 26

PRAKSIS

EU-Domstolen · Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)

04.10.2024

§ 3 De tre kumulative betingelser – overtrædelsen i sig selv er ikke nok

Grundstenen i EU-Domstolens fortolkning er, at [artikel 82, stk. 1](#) opstiller **tre kumulative betingelser** – udviklet fra og med Domstolens dom af 4. maj 2023 i **sag C-300/21 (Österreichische Post)** og siden gentaget i samtlige efterfølgende domme:

1. **En overtrædelse** af databeskyttelsesforordningen.
2. **En konkret skade** – materiel eller immateriel – som den registrerede faktisk har lidt.
3. **Årsagssammenhæng** mellem overtrædelsen og skaden.

Konsekvensen er skarp: en overtrædelse af forordningen udløser **ikke i sig selv** erstatning. Den registrerede, der blot kan påvise, at oplysninger er behandlet ulovligt, har intet krav, medmindre der føres bevis for en skade, der er en følge af netop denne overtrædelse. Det er dette forhold, der forklarer, hvorfor så mange danske sager ender med frifindelse, selv om selve databrudet er ubestridt.

Domstolen bekræftede rammen i [C-667/21](#) (MDK Nordrhein), hvor en ansat krævede 20.000 EUR for en medicinsk tjenestes behandling af hans helbredsoplysninger. Domstolen præciserede, at den registrerede skal føre bevis for overtrædelsen, den lidt skade og årsagsforbindelsen – mens den dataansvarlige bærer bevisbyrden for ansvarsfritagelse. I [C-741/21](#) (juris GmbH) fastholdt Domstolen, at overtrædelsen af forordningens bestemmelser ikke i sig selv giver ret til erstatning, og at det påhviler den registrerede at godtgøre de negative konsekvenser.

Højesteret gengav i Gladsaxe-dommen [BS-14485/2025-HJR m.fl.](#) EU-Domstolens definition af immateriel skade:

En immateriel skade efter artikel 82 omfatter negative følelser, som den pågældende oplever som følge af en uautoriseret videregivelse af vedkommendes personoplysninger til en tredjemand, såsom frygt eller utilfredshed, der udløses af et tab af kontrol over oplysningerne, af et potentielt misbrug af oplysningerne eller af en krænkelse af vedkommendes omdømme, for så vidt som den registrerede godtgør, at vedkommende har sådanne følelser, og godtgør de negative konsekvenser heraf som følge af den omhandlede overtrædelse af forordningen.

Sætningens sidste led – "for så vidt som den registrerede godtgør" – er hele sagens kerne.

LOV	Databeskyttelsesforordningen § 82, stk. 1	
PRAKSIS	Højesteret · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	19.12.2025
	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024
	EU-Domstolen · Behandling af ansattes helbredsoplysninger og betingelser for erstatning for immateriel skade i henhold til GDPR	21.12.2023

§ 4 Ingen bagatelgrænse – men bevisbyrden ligger fuldt hos den registrerede

En tilbagevendende indsigelse fra dataansvarlige har været, at små eller flygtige gener ikke bør udløse ansvar. Den indsigelse er afvist principielt.

I [C-456/22](#) fastslog EU-Domstolen, at [artikel 82, stk. 1](#) **ikke** indeholder nogen bagatelgrænse eller tærskel for skadens alvor. Det samme blev bekræftet i [C-590/22](#), hvor Domstolen udtrykkeligt afviste alvorsgrad som betingelse for kompensation. Der findes med andre ord ingen nedre grænse for, hvor lille en immateriel skade må være, for at den kan erstattes.

Dette må imidlertid ikke forveksles med en lempelse af beviskravet. De to spørgsmål er adskilte:

- **Alvorstærskel (afvist):** Skaden behøver ikke at nå en vis intensitet for at være erstatningsberettiget.
- **Bevisbyrde (uændret):** Den registrerede skal fortsat **godtgøre**, at skaden faktisk er indtrådt, og at den skyldes overtrædelsen.

Denne kombination – ingen tærskel, fuld bevisbyrde – er den vanskeligste balance i praksis. Højesteret formulerede den anden side af mønten i Gladsaxe-dommen [BS-14485/2025-HJR](#):

Erstatningen eller godtgørelsen, der skal kompensere skaden fuldt ud, fastsættes af de nationale domstole ved anvendelse af nationale regler og under overholdelse af de EU-retlige principper om ækvivalens og effektivitet. Når den skade, som personen har lidt, ikke er alvorlig, kan der tilkendes vedkommende en ubetydelig erstatning eller godtgørelse.

Fraværet af en bagatelgrænse betyder altså ikke, at bagateller udløser store beløb – det betyder, at de udløser små beløb, forudsat at de overhovedet bevises.

I [C-182/22](#) præciserede Domstolen i samme retning begrebet "identitetstyveri" i forordningens forstand – det forudsætter, at en tredjemand faktisk har antaget den registreredes identitet, og en ret til erstatning er ikke betinget af, at et sådant kvalificeret misbrug er sket. Også her er det den konkrete, beviste skade – ikke etiketten på hændelsen – der afgør sagen.

LOV	Databeskyttelsesforordningen § 82, stk. 1	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024
	EU-Domstolen · Retten til erstatning for immateriel skade ved databrud og fortolkningen af identitetstyveri under GDPR	20.06.2024
	EU-Domstolen · Ret til erstatning for immateriel skade under GDPR: Ingen bagatelgrænse for skadens alvor	14.12.2023

§ 5 Frygt for fremtidigt misbrug: hvornår er frygten velbegrundet og behørigt bevist?

Det praktisk vigtigste spørgsmål efter et databrud er, om den registreredes **frygt for, at oplysningerne på et tidspunkt misbruges**, i sig selv er en erstatningsberettiget immateriel skade. Svaret er ja – betinget.

EU-Domstolen fastslog i [C-590/22](#), at frygt for datamisbrug kan udgøre immateriel skade. Højesteret sammenfattede i Gladsaxe-dommen [BS-14485/2025-HJR m.fl.](#) retstilstanden i to led:

Når en person, der kræver erstatning eller godtgørelse, påberåber sig en frygt for, at der i fremtiden vil ske et misbrug af den pågældendes personoplysninger som følge af en overtrædelse af forordningen, skal den nationale ret

navnlig efterprøve, om denne frygt kan anses for at være velbegrundet under de specifikke omstændigheder og for den pågældende person.

En persons frygt for, at vedkommendes personoplysninger som følge af en overtrædelse af forordningen er blevet videregivet til tredjemand, uden at det kan godtgøres, at dette faktisk har været tilfældet, er tilstrækkelig til at begrunde en ret til erstatning eller godtgørelse efter artikel 82, såfremt denne frygt og de negative konsekvenser af denne er behørigt bevist. Den blotte henvisning til en frygt – uden godtgjorte negative konsekvenser – kan ikke give anledning til erstatning eller godtgørelse efter artikel 82.

Heraf udkrystalliserer der sig en **to-trins-prøvelse**, som de danske domstole skal gennemføre:

- **Trin 1 – er frygten velbegrundet?** Vurderingen er dobbelt konkret: den skal foretages "under de specifikke omstændigheder" (hvilke oplysninger, hvilken eksponering, hvilken risiko for faktisk misbrug) og "for den pågældende person" (den registreredes individuelle situation). En generisk uro over, at data er på afveje, er ikke nok.
- **Trin 2 – er frygten og dens negative konsekvenser behørigt bevist?** Frygten skal dokumenteres som en faktisk oplevet tilstand, og der skal påvises negative konsekvenser af den. Frygt uden konsekvenser er ikke en erstatningsberettiget skade.

Notér nuancen: det er **ikke** en betingelse, at oplysningerne faktisk er kommet til tredjemands kendskab. En velbegrundet og bevist frygt er tilstrækkelig, selv om videregivelsen ikke kan godtgøres. Beviskravet flyttes altså fra hændelsen til virkningen hos den registrerede.

EU-Domstolen har markeret grænsen fra begge sider. I [C-200/23](#) (Agentsia po vpisvaniyata) – som Højesteret udtrykkeligt inddrog som supplerende retsgrundlag – var spørgsmålet, om et **kortvarigt tab af kontrol** over personoplysninger, der blev lagt online i et handelsregister, i sig selv kan udgøre immateriel skade, eller om der kræves yderligere konkrete negative konsekvenser. Og i [C-655/23](#) (IP), ligeledes påberåbt for Højesteret, behandlede Domstolen forholdet mellem erstatning efter artikel 82 og forebyggende undladelsespåbud.

LOV	Databeskyttelsesforordningen § 82, stk. 1	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	Højesteret · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	19.12.2025
	EU-Domstolen · Erstatning for immateriel skade og forebyggende undladelsespåbud efter databeskyttelsesforordningen (GDPR)	04.09.2025
	EU-Domstolen · Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)	04.10.2024
	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024

Gladsaxe-sagen gennem tre instanser (2021-2025) – den danske referencesag

§ 6

Gladsaxe-sagen er den eneste danske sag om [artikel 82](#), der er prøvet af Højesteret, og den definerer derfor beviskravet i dansk ret. Sagen udsprang af, at Gladsaxe Kommune havde behandlet oplysninger om ca. 20.000 borgere – herunder CPR-numre – i et regneark, og at en bærbar computer med oplysningerne blev stjålet.

Instans	Sag	Dato	Udfald
Retten i Glostrup	BS-19120/2019-GLO	11. maj 2021	Frifindelse for erstatningskravene
Østre Landsret	BS-19616/2021-OLR	19. november 2024	Stadfæstelse – brud på datasikkerheden, men ingen erstatning
Procesbevillingsnævnet	3.-instansbevilling af 4. marts 2025	4. marts 2025	Bevilling meddelt, jf. retsplejeloven § 371
Højesteret	BS-14485/2025-HJR m.fl.	19. december 2025	Frifindelse – manglende bevis for skade og for velbegrundet frygt

Det bemærkelsesværdige er, at **selve overtrædelsen var fastslået** allerede af landsretten – kommunen var "dømt for brud på datasikkerhed" – uden at det gav borgerne noget krav. Netop dette illustrerer betingelse nr. 2 og 3 i artikel 82: skade og kausalitet er selvstændige hurdle.

Højesteret afgrænsede opgaven skarpt:

Som nævnt er hovedspørgsmålet, om A, B, C og D har godtgjort, at de har lidt skade omfattet af artikel 82, og om skaden er en følge af kommunens behandling af deres personoplysninger i regnearket eller sikkerhedsbruddet ved tyveriet af computeren.

Sagens **kausalitetsproblem** er lærerigt. Af Højesterets supplerende sagsfremstilling fremgår:

Retten i Aarhus har den 10. februar 2022 afsagt dom i en straffesag om bl.a. det databedrageri, som C i marts 2019 var udsat for. Vestre Landsret afsagde ankedom i sagen den 23. december 2022. Dommene er ikke fremlagt for Højesteret.

Selv hvor en af de registrerede faktisk var udsat for databedrageri, var det altså ikke godtgjort, at netop dette misbrug var en følge af kommunens overtrædelse. En konstateret skade uden bevist årsagssammenhæng til overtrædelsen udløser intet krav efter artikel 82.

Højesteret inddrog udtrykkeligt EU-Domstolens nyeste praksis som supplerende retsgrundlag:

Ud over de domme, der er nævnt i landsrettens dom, har EU-Domstolen i dom af 4. oktober 2024 i sag C-200/23 (Agentsia po vpisvaniyata) og i dom af 4. september 2025 i sag C-655/23 (IP) fortolket artikel 82 i databeskyttelsesforordningen [...]

Det blev endvidere oplyst, at Gladsaxe Kommune i december 2018 iværksatte kryptering af alle computere med Windows 10 og besluttede at indkøbe software til kryptering af Windows 7-computere – et forhold, der belyser efterfølgende afhjælpning, men som ikke i sig selv kunne påvirke spørgsmålet om skade og kausalitet.

LOV	Databeskyttelsesforordningen § 82 Retsplejeloven § 371	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025

Højesteret · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	19.12.2025
EU-Domstolen · Erstatning for immateriel skade og forebyggende undladelsespåbud efter databeskyttelsesforordningen (GDPR)	04.09.2025
EU-Domstolen · Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)	04.10.2024
Landsretten · Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	19.11.2024
Byretten · Afgørelse i sag om databrud i Gladsaxe Kommune: Frifindelse for erstatningskrav	11.05.2021
Procesbevillingsnævnet · Procesbevillingsnævnet: 3.-instansbevilling om immateriel skade efter GDPR artikel 82 ved databrud med 20.000 borgeres CPR-numre	04.03.2025

§ 7 Præsumptionsansvaret og ansvarsfritagelsen i artikel 82, stk. 3

Ansvarsgrundlaget efter artikel 82 er et **præsumptionsansvar** – culpa med omvendt bevisbyrde. Det er kontinuiteten fra persondatalovens § 69, og det bekræftes udtrykkeligt i forarbejderne til [databeskyttelseslovens § 40](#): "forordningens artikel 82, stk. 2 og 3, [fastsætter], at der fortsat gælder et præsumptionsansvar".

EU-Domstolen slog konstruktionen fast i [C-667/21](#), præmis 94:

Det fremgår således af en samlet analyse af artikel 82, at denne artikel fastsætter en ordning med culpaansvar, hvorefter bevisbyrden ikke påhviler den person, der har lidt skade, men den dataansvarlige.

Bevisbyrderne fordeler sig altså således:

Element	Hvem bærer bevisbyrden?
Overtrædelse af forordningen	Den registrerede
Konkret materiel/immateriel skade	Den registrerede
Årsagssammenhæng	Den registrerede
Fravær af skyld i den skadevoldende begivenhed (stk. 3)	Den dataansvarlige/databehandleren

Fritagelsen efter stk. 3 er snæver. I [C-741/21](#) (juris GmbH) tog Domstolen stilling til netop det argument, der er hyppigst i praksis: at overtrædelsen skyldtes en medarbejder, der handlede i strid med den dataansvarliges instruks. Domstolen afviste, at en dataansvarlig kan fritages for ansvar alene ved at henvise til uagtsomhed hos en person, der handler under vedkommendes myndighed. Sammenhængen er [artikel 29](#):

Databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, behandler kun disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Den dataansvarlige svarer med andre ord for sine folk. Ville en medarbejderfejl kunne bære ansvarsfritagelse, ville [artikel 82](#) miste sin effektive virkning, eftersom stort set enhver overtrædelse i en organisation kan tilbagesføres til en konkret persons handling.

Ansvarsfritagelsen skal derfor bæres af, at den skadevoldende **begivenhed** ligger uden for den pågældendes ansvarssfære – ikke af, at fejlen kan lokaliseres til et bestemt led i organisationen. Modstykket er, at når den dataansvarlige har gennemført passende tekniske og organisatoriske foranstaltninger, jf. [artikel 32, stk. 1](#), styrkes muligheden for at løfte bevisbyrden efter stk. 3.

Selv når fritagelsen ikke lykkes, hjælper det ikke den registrerede, hvis skaden ikke er bevist. Det er netop den kombination, Gladsaxe-sagen viser: fastslået sikkerhedsbrud, ingen ansvarsfritagelse – og alligevel frifindelse, fordi betingelse 2 og 3 svigtede.

LOV	Databeskyttelsesforordningen § 29	Databeskyttelsesforordningen § 32, stk. 1
	Databeskyttelsesforordningen § 82, stk. 2-3	Databeskyttelsesloven § 40
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024
	EU-Domstolen · Behandling af ansattes helbredsoplysninger og betingelser for erstatning for immateriel skade i henhold til GDPR	21.12.2023

§ 8 Solidarisk hæftelse og regres mellem dataansvarlige og databehandlere

Forordningen udvidede gældende ret på ét afgørende punkt: hvor persondatalovens § 69 kun hjemlede ansvar for den **dataansvarlige**, kan også **databehandleren** ifalde ansvar efter [artikel 82, stk. 2](#). Databeskyttelsesudvalget beskrev nyskabelsen i [betænkning nr. 1565/2017, s. 268](#):

Det er dermed nyt i forhold til gældende ret, at ansvarsgrundlaget for en databehandler under nærmere fastlagte omstændigheder – navnlig hvis databehandleren ikke overholder de forpligtelser, som følger af forordningen – er reguleret af forordningens artikel 82, stk. 2. Dette kan f.eks. være tilfældet, hvis databehandleren uden godkendelse fra den dataansvarlige gør brug af en anden databehandler, jf. forordningens artikel 28, stk. 2.

Hæftelsen er asymmetrisk:

- **Den dataansvarlige** hæfter for enhver skade forvoldt af behandling, der overtræder forordningen.
- **Databehandleren** hæfter kun (i) ved tilsidesættelse af pligter, der er rettet specifikt mod databehandlere, eller (ii) ved at undlade at følge eller handle i strid med den dataansvarliges lovlige instrukser.

Er flere involveret i **samme behandling**, følger det af [artikel 82, stk. 4](#), at de hæfter **solidarisk for hele skaden** – udtrykkeligt begrundet i formålet om "at sikre fuld erstatning til den registrerede". Den registrerede skal derfor ikke udrede den interne ansvarsfordeling mellem myndighed, leverandør og underleverandør, men kan rette hele kravet mod ét led. Den indbyrdes fordeling håndteres bagefter ved regres efter [artikel 82, stk. 5](#), hvor den, der har betalt fuld erstatning, kan kræve de øvriges andel tilbage "i overensstemmelse med betingelserne i stk. 2".

Et beslægtet solidaritetsprincip findes i EU-rettens øvrige databeskyttelsesregimer. I [C-755/21](#) tog EU-Domstolen stilling til Europol-forordningens artikel 50 og fastslog et solidarisk ansvar mellem Europol og den berørte medlemsstat ved ulovlig behandling af personoplysninger. Konstruktionen er ikke identisk med artikel 82, men understøtter det bærende hensyn: den registrerede skal kunne opnå fuld erstatning uden at skulle placere ansvaret i et komplekst netværk af aktører.

LOV	Databeskyttelsesforordningen § 28, stk. 2	Databeskyttelsesforordningen § 82, stk. 2, 4-5
PRAKSIS		

§ 9 Rent kompenserende – derfor må artikel 83's bødekriterier ikke bruges ved udmålingen

Et af de hyppigste fejlgreb i procedurer om artikel 82 er at argumentere for et højt beløb ud fra **overtrædelsens grovhed** – antallet af berørte, oplysningernes følsomhed, den dataansvarliges forsæt. Det er ikke lovligt.

EU-Domstolen fastslog i [C-667/21](#), præmis 84:

En økonomisk erstatning på grundlag af [artikel 82] skal anses for at være »fuld«, hvis den fuldstændigt kompenserer den skade, der konkret er lidt på grund af overtrædelsen af forordningen, uden at det med henblik på en sådan ydelse af fuldstændig kompensation er nødvendigt at pålægge betaling af erstatning med karakter af straf.

Dommen afviste dermed, at [artikel 82, stk. 1](#) har en afskrækkende eller straffende funktion. Erstatningen er **rent kompenserende**: hverken mere eller mindre end den faktisk lidt skade. Samme dom fastslog, at **graden af skyld** (simpel eller grov uagtsomhed, forsæt) er uden betydning for erstatningens størrelse – et princip, der blev gentaget i [C-741/21](#) og i [C-507/23](#).

Den pønale side af forordningen varetages af helt andre instrumenter – [artikel 83](#) (administrative bøder) og [artikel 84](#) (øvrige sanktioner). Det er dér, kriterierne om overtrædelsens karakter, alvor og varighed, antal berørte registrerede, forsæt/uagtsomhed og virksomhedens omsætning hører hjemme, jf. [artikel 83, stk. 2](#). At de to spor er adskilte, fremgår også af, at Danmark har valgt strafferetlige bøder frem for administrative, jf. [artikel 83, stk. 9](#) – se EU-Domstolens danske forelæggelsessag [C-383/23](#) om koncernomsætningens betydning for bødemaksimum og [C-807/21](#) (Deutsche Wohnen) om skyldkravet ved bøder mod juridiske personer. Bødesporet behandles selvstændigt i [datatilsynsboder-gdpr-overtraedelser](#) og er ikke emnet her – men afgrænsningen er retligt afgørende netop fordi kriterierne **ikke må vandre** fra artikel 83 til artikel 82.

Undskyldning som godtgørelsesform. I [C-507/23](#) åbnede EU-Domstolen for, at en undskyldning kan udgøre passende godtgørelse. Højesteret gengav princippet – og lukkede døren i dansk ret:

En undskyldning kan anses for en passende godtgørelse, bl.a. når det er umuligt at genoprette den situation, der forelå, før skaden indtraf, forudsat at denne form for godtgørelse har hjemmel i national ret.

Højesteret bemærker, at der i dansk ret på nuværende tidspunkt ikke er hjemmel til, at en godtgørelse for en skade som følge af en overtrædelse af forordningen kan bestå i en undskyldning fra den ansvarlige.

En dataansvarlig kan altså ikke i Danmark afværge et artikel 82-krav ved at tilbyde en undskyldning. Forbeholdet "på nuværende tidspunkt" indbyder til, at spørgsmålet kan flytte sig, hvis lovgiver skaber hjemlen.

LOV

[Databeskyttelsesforordningen § 82, stk. 1](#)
[Databeskyttelsesforordningen § 83, stk. 2, 9](#)
[Databeskyttelsesforordningen § 84](#)

PRAKSIS

Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger

19.12.2025

EU-Domstolen · Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning

13.02.2025

EU-Domstolen · Erstatning for immateriel skade efter GDPR: Undskyldning som godtgørelse og betydningen af den dataansvarliges skyld	04.10.2024
EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024
EU-Domstolen · Behandling af ansattes helbredsoplysninger og betingelser for erstatning for immateriel skade i henhold til GDPR	21.12.2023
EU-Domstolen · Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	05.12.2023

§ 10 Udmålingsniveauet i dansk praksis: moderate beløb, store spring mellem grundlagene

Fordi erstatningen er rent kompenserende og skal fastsættes efter nationale regler inden for ækvivalens- og effektivitetsprincipperne, ligger de danske beløb lavt – og i skarp kontrast til de beløb, der kan opnås, når krænkelsen kvalificeres som tort eller som et konventionsbrud.

Afgørelse	Forhold	Grundlag	Udfald
BS-27044/2020-OLR (ØL, 21/8-2025)	Ulovlig videregivelse af følsom helbredsoplysning (diagnose)	Art. 82, jf. dbl. § 40	2.500 kr.
BS-27044/2020-OLR (samme forhold)	Samme forhold	EAL § 26, stk. 1	Frifindelse
BS-14485/2025-HJR m.fl. (HR, 19/12-2025)	Regneark + tyveri af computer, ca. 20.000 borgere	Art. 82	Frifindelse
BS-53777/2023-VIB (Viborg, 12/1-2026), sagsøger 1	Videregivelse af psykolog- og helbredsoplysninger til gerningsmand	Princippet i EAL § 26, stk. 1 + EMRK art. 8	112.500 kr.
BS-53777/2023-VIB , sagsøger 2	Samme forhold (moderen)	Princippet i EAL § 26, stk. 1 + EMRK art. 8	0 kr. – anerkendelse tilstrækkelig
BS-25262/2021-HJR (HR, 22/6-2022)	Systematiske person- og celleundersøgelser	Princippet i EAL § 26 + EMRK art. 13	30.000 kr.

Referencesagen for artikel 82-niveauet er Østre Landsrets dom af 21. august 2025 i [BS-27044/2020-OLR](#). Sagen var henvist til landsretten som første instans efter [retsplejelovens § 226, stk. 1](#) – altså anset for principiel. Landsretten tilkendte **2.500 kr.** i erstatning efter artikel 82 for den uberettigede videregivelse af en helbredsdiagnose, men **frifandt** for det parallelle krav efter [erstatningsansvarslovens § 26](#).

Dommen er instruktiv af tre grunde:

- **Beløbsniveauet er beskedent, selv for følsomme oplysninger.** En diagnose er en særlig kategori af personoplysninger, men artikel 82 kompenserer den konkrete lidte skade – ikke oplysningskategoriens abstrakte følsomhed.
- **De to grundlag giver forskellige resultater på samme faktum.** At § 26 ikke var opfyldt, mens artikel 82 var, viser at artikel 82 har den **lavere** tærskel for ansvar, men også det **lavere** beløbsniveau.
- **Effektivitetsprincippet er opfyldt med små beløb.** Højesteret bekræftede, at når skaden ikke er alvorlig, "kan der tilkendes vedkommende en ubetydelig erstatning eller godtgørelse".

Springet til 112.500 kr. i [BS-53777/2023-VIB](#) skal derfor ikke læses som et artikel 82-niveau. Retten i Viborg tilkendte beløbet efter **princippet i erstatningsansvarslovens § 26, stk. 1**, hvor et voldtægtsoffers

psykolognotater og børnefaglige undersøgelser var videregivet til gerningsmanden som led i Civilstyrelsens regresssag. Retten fandt krænkelsen grov og med konstaterbar psykisk forværring; for moderen fandt retten derimod, at **anerkendelsen af krænkelsen i sig selv udgjorde tilstrækkelig kompensation** uden økonomisk udbetaling. Sagen blev afgjort af tre dommere.

LOV

[Databeskyttelsesforordningen § 82](#)[Databeskyttelsesloven § 40](#)[Erstatningsansvarsloven § 26, stk. 1](#)[Retsplejeloven § 226, stk. 1](#)

PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	Højesteret · Højesteret fastslår, at systematiske daglige person- og celleundersøgelser af terrorsigtet var retsstridige og krænkede menneskerettighederne	22.06.2022
	Landsretten · Erstatning for immateriel skade efter databeskyttelsesforordningen ved ulovlig videregivelse af følsomme helbredsoplysninger	21.08.2025
	Byretten · Civilstyrelsen dømt til at betale 112.500 kr. for videregivelse af følsomme oplysninger om voldtægtsoffer til gerningsmand	12.01.2026

§ 11 Samspillet med erstatningsansvarslovens § 26 og EMRK artikel 8

Artikel 82 fortrænger ikke de nationale godtgørelsesregler. Databeskyttelsesudvalget fastslog det udtrykkeligt i [betænkning nr. 1565/2017, s. 268](#), og dansk praksis behandler rutinemæssigt de to krav samtidigt. Forskellen ligger i betingelserne:

	Artikel 82	EAL § 26, stk. 1
Ansvarsgrundlag	Præsumptionsansvar (omvendt bevisbyrde)	Culpa hos skadevolder
Krænkelsens karakter	Enhver overtrædelse af forordningen	Retsstridig krænkelse af frihed, fred, ære eller person
Kvalifikationskrav	Ingen alvorstærskel	Culpøs adfærd af en vis grovhed
Skyldgradens betydning for beløbet	Ingen	Indgår i skønnet
Typisk beløbsniveau	Lavt (fx 2.500 kr.)	Betydeligt højere

Kravet om kvalificeret grovhed under § 26 blev formuleret i [Betænkning nr. 1483/2006, s. 73](#):

En sådan lovregel findes i erstatningsansvarslovens § 26, hvorefter den, der er ansvarlig for en retsstridig krænkelse af en andens frihed, fred, ære eller person, skal betale den forurettede godtgørelse for tort. Anvendelsen af denne bestemmelse er betinget af, at skadevolden har udvist en culpøs adfærd af en vis grovhed, men det er ingen betingelse, at krænkelsen er strafbar.

Det er netop denne grovhedstærskel, der forklarer, hvorfor Østre Landsret i [BS-27044/2020-OLR](#) kunne tilkende erstatning efter artikel 82 og samtidig frifinde efter § 26 på samme faktum. Artikel 82 har den lavere ansvarstærskel – § 26 har det højere beløb.

Det tredje spor er EMRK. Hvor behandlingen af personoplysninger udgør et uproportionalt indgreb i privatlivet, kan **EMRK artikel 8** aktualisere en godtgørelse efter princippet i § 26 sammenholdt med **EMRK artikel 13**. Højesteret anvendte konstruktionen i [BS-25262/2021-HJR](#) (30.000 kr. for retsstridige person- og

celleundersøgelser), og Rigsadvokaten har opsummeret retstilstanden i [Rigsadvokatmeddelelsen om erstatning i henhold til retsplejelovens kapitel 93 a](#):

Det følger af Højesterets praksis, at Den Europæiske Menneskerettighedskonvention (EMRK) artikel 13 (om effektive retsmidler) sammenholdt med princippet i erstatningsansvarslovens § 26 (om godtgørelse for tort) indebærer, at der er krav på en godtgørelse, hvis der som følge af en krænkelse af EMRK i henhold til Den Europæiske Menneskerettighedsdomstols praksis er ret til godtgørelse efter EMRK artikel 41.

I [BS-53777/2023-VIB](#) forfulgte sagsøgerne alle tre spor samtidigt – artikel 82, § 26 og EMRK artikel 8.

Retten fandt, at Civilstyrelsen havde et legitimt og lovhjemlet grundlag for at videregive oplysninger til brug for regreskravet, men at videregivelsen gik videre end **strengt nødvendigt**: fraværsrapporter og konkluderende psykologudtalelser ville have været tilstrækkelige, mens de intime beskrivelser fra fortrolige psykologsamtaler ikke var proportionale, jf. **EMRK artikel 8, stk. 2**. Det er en sund erindring om, at nødvendighedsprøvelsen ofte afgør sagen længe før udmålingen.

Om afgrænsningen mellem sporene henvises til [tortgodtgoerelse](#), [emrk-artikel-8-privatliv-familieliv](#) og – for krav mod myndigheder på andet grundlag – [erstatningsansvar-ulovlige-myndighedsafgoerelser](#).

LOV	Databeskyttelsesforordningen § 82	Erstatningsansvarsloven § 26, stk. 1
PRAKSIS	Højesteret · Højesteret fastslår, at systematiske daglige person- og celleundersøgelser af terrørsigtet var retsstridige og krænkede menneskerettighederne 22.06.2022 Landsretten · Erstatning for immateriel skade efter databeskyttelsesforordningen ved ulovlig videregivelse af følsomme helbredsoplysninger 21.08.2025 Byretten · Civilstyrelsen dømt til at betale 112.500 kr. for videregivelse af følsomme oplysninger om voldtægtsoffer til gerningsmand 12.01.2026	

§ 12 Hvor kravet skal rejses – artikel 82, stk. 6, og myndighedernes manglende kompetence

Erstatningskravet efter artikel 82 er **udelukkende et domstolskrav**. Det følger af [artikel 82, stk. 6](#):

Retssager med henblik på udøvelse af retten til at modtage erstatning anlægges ved de domstole, der er kompetente i henhold til national ret i den medlemsstat, der er omhandlet i artikel 79, stk. 2.

Datatilsynet kan ikke tilkende erstatning. Kompetencefordelingen er ikke ny – den gjaldt allerede under persondataloven, hvor [Betænkning nr. 1483/2006, s. 73](#) konstaterede:

Krav om erstatning efter bestemmelsen skal indbringes for domstolene, og kan således ikke behandles af tilsynsmyndigheden.

Datatilsynets beføjelser er tilsynsmæssige – kritik, påbud, forbud og indstilling til bøde. EU-Domstolen bekræftede i [C-768/21](#), at tilsynsmyndigheden har et skøn med hensyn til, om og hvordan korrigerende beføjelser skal anvendes ved brud på persondatasikkerheden. En registreret, der klager til Datatilsynet og får medhold, står derfor stadig uden erstatning – kravet må anlægges særskilt ved retten. Tilsynssporet behandles i [datatilsynet-afgoerelser](#).

Ombudsmanden kan heller ikke. Folketingets Ombudsmand har fast afvist at afgøre erstatningsspørgsmål og henviser dem til domstolene – fx i udtalelsen om [hjemmel for påbud om opgravning af olietank](#):

Det bemærkes, at erstatningsspørgsmål henhører under domstolenes afgørelse.

Processuelle spor i praksis. To iagttagelser fra de fundne sager:

- **Principielle sager kan henvises til landsretten.** [BS-27044/2020-OLR](#) blev behandlet af Østre Landsret i første instans efter [retsplejelovens § 226, stk. 1](#), og [BS-53777/2023-VIB](#) blev behandlet af tre dommere i byretten. Artikel 82-sager har ofte principiel karakter.
- **Vejen til Højesteret går gennem Procesbevillingsnævnet.** Gladsaxe-sagen nåede kun tredje instans, fordi nævnet den [4. marts 2025](#) meddelte 3.-instansbevilling efter [retsplejelovens § 371](#) i sagen om immateriel skade efter artikel 82 ved databrud med 20.000 borgeres CPR-numre.

Det strafferetlige spor ligger helt uden for artikel 82 og reguleres bl.a. af [Rigsadvokatmeddelelsen om databeskyttelse i straffesager](#), hvorefter Datatilsynet skal høres, inden der træffes afgørelse om tiltale.

Endelig gælder de almindelige forældelsesregler for kravet – se [forældelse-erstatnings-og-godtgoerelseskrav](#).

LOV	Databeskyttelsesforordningen § 79, stk. 2	Databeskyttelsesforordningen § 82, stk. 6
	Retsplejeloven § 226, stk. 1	Retsplejeloven § 371
PRAKSIS	EU-Domstolen · Tilsynsmyndigheders skønsebeføjelse ved brud på persondatasikkerheden under GDPR 26.09.2024 Landsretten · Erstatning for immateriel skade efter databeskyttelsesforordningen ved ulovlig videregivelse af følsomme helbredsoplysninger 21.08.2025 Byretten · Civilstyrelsen dømt til at betale 112.500 kr. for videregivelse af følsomme oplysninger om voldtægtsoffer til gerningsmand 12.01.2026 Procesbevillingsnævnet · Procesbevillingsnævnet: 3.-instansbevilling om immateriel skade efter GDPR artikel 82 ved databrud med 20.000 borgeres CPR-numre 04.03.2025	

§ 13 Sammenfatning: hvad skal den registrerede løfte – og hvad kan den dataansvarlige stille op?

Retstilstanden efter Højesterets dom af 19. december 2025 kan sammenfattes i fire bevægelser.

For det første er ansvarstærsklen lav, men beviskravet højt. Der er ingen bagatelgrænse for immateriel skade, jf. [C-456/22](#) og [C-590/22](#), og ansvaret er et præsumptionsansvar, jf. [C-667/21](#). Alligevel taber den registrerede, hvis skaden og årsagssammenhængen ikke bevises. Det er ikke et paradoks – det er arbejdsdelingen mellem betingelse 1 (som er let) og betingelse 2 og 3 (som er svære).

For det andet skal frygt-argumentet bygges konkret. Efter [BS-14485/2025-HJR m.fl.](#) skal en påstand om frygt for fremtidigt misbrug underbygges ad to spor: at frygten er **velbegrundet** under de specifikke omstændigheder og for netop den pågældende person, og at frygten **og dens negative konsekvenser** er behørigt bevist. Generisk uro over et databrud rækker ikke – og selv et faktisk indtruffet databedrageri hjælper ikke, hvis det ikke kan føres tilbage til overtrædelsen.

For det tredje er beløbsniveauet i dansk ret moderat. Erstatningen er rent kompenserende og må ikke tillægges pønale elementer, jf. [C-667/21](#). Bødekriterierne i [artikel 83](#) og overtrædelsens grovhed er irrelevante

for udmålingen, og skyldgraden ligeledes. Referencepunktet er de **2.500 kr.**, Østre Landsret tilkendte i [BS-27044/2020-OLR](#) for en lækket helbredsdiagnose. Vil man højere op, skal krænkelsen kunne bære [erstatningsansvarslovens § 26](#) eller **EMRK artikel 8** – og dermed opfylde kravet om kvalificeret grovhed.

For det fjerde er den dataansvarliges forsvar snævert. Fritagelsen i [artikel 82, stk. 3](#) kan ikke bæres af, at en medarbejder handlede i strid med instruksen, jf. [C-741/21](#) og [artikel 29](#), og en undskyldning er ikke en gyldig godtgørelsesform i dansk ret. Er flere aktører involveret i samme behandling, hæfter de solidarisk, jf. [artikel 82, stk. 4](#). Det reelle forsvar ligger derfor **ikke** i ansvarsfritagelsen, men i at bestride skaden og årsagssammenhængen – præcis det, der bar Gladsaxe Kommune igennem alle tre instanser.

Den historiske pointe fortjener at stå til sidst. Da [databeskyttelseslovens § 40](#) blev skrevet, antog Justitsministeriets udvalg, at artikel 82 næppe rakte ud over økonomisk skade i en dansk kontekst, jf. [betænkning nr. 1565/2017, s. 267](#). EU-Domstolen har siden gjort bestemmelsen til et selvstændigt, autonomt EU-retligt krav, som dækker frygt, kontroltab og andre negative følelser. Men den samme domstol har fastholdt beviskravet – og det er dér, sagerne afgøres.

LOV	Databeskyttelsesforordningen § 29	Databeskyttelsesforordningen § 82, stk. 3-4
	Databeskyttelsesforordningen § 83	Databeskyttelsesloven § 40
	Erstatningsansvarsloven § 26	
PRAKSIS	Højesteret · Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	19.12.2025
	Højesteret · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	19.12.2025
	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024
	EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024
	EU-Domstolen · Behandling af ansattes helbredsoplysninger og betingelser for erstatning for immateriel skade i henhold til GDPR	21.12.2023
	EU-Domstolen · Ret til erstatning for immateriel skade under GDPR: Ingen bagatelgrænse for skadens alvor	14.12.2023
	Landsretten · Erstatning for immateriel skade efter databeskyttelsesforordningen ved ulovlig videregivelse af følsomme helbredsoplysninger	21.08.2025

REFERENCE Lovgrundlag

5 paragraffer

Databeskyttelsesforordningen § 29	Databeskyttelsesforordningen § 82
Databeskyttelsesforordningen § 83	Databeskyttelsesloven § 40
Erstatningsansvarsloven § 26	stk. 1

MATERIALE Citerede afgørelser

20 afgørelser

HØJESTERET · ØVERSTE INSTANS

3

19.12.2025	Højesteret frifinder Gladsaxe Kommune for godtgørelseskrav efter tyveri af bærbar computer med personoplysninger	10337-12149
19.12.2025	Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	14485-2025-2025-14653-2025-1 og-16195-2025
22.06.2022	Højesteret fastslår, at systematiske daglige person- og celleundersøgelser af terrorsigtet var retsstridige og krænkede menneskerettighederne	1768-2115
EU-DOMSTOLEN · EUROPÆISK DOMSTOL		12
04.09.2025	Erstatning for immateriel skade og forebyggende undladelerspåbud efter databeskyttelsesforordningen (GDPR)	C-655/23
13.02.2025	Beregning af GDPR-bøder: Begrebet "virksomhed" omfatter hele koncernens omsætning	C-383/23
04.10.2024	Beskyttelse af personoplysninger i handelsregistret: Myndighedens ansvar og erstatning for immateriel skade (Sag C-200/23)	C-200/23
04.10.2024	Erstatning for immateriel skade efter GDPR: Undskyldning som godtgørelse og betydningen af den dataansvarliges skyld	C-507/23
26.09.2024	Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	C-768/21
20.06.2024	Retten til erstatning for immateriel skade ved databrud og fortolkningen af identitetstyveri under GDPR	C-182/22
20.06.2024	Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	C-590/22
11.04.2024	Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	C-741/21
05.03.2024	Europol og medlemsstaternes solidariske ansvar ved ulovlig behandling af personoplysninger	C-755/21
21.12.2023	Behandling af ansattes helbredsoplysninger og betingelser for erstatning for immateriel skade i henhold til GDPR	C-667/21
14.12.2023	Ret til erstatning for immateriel skade under GDPR: Ingen bagatelgrænse for skadens alvor	C-456/22
05.12.2023	Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	C-807/21
LANDSRETTEEN · ANKEINSTANS		2
21.08.2025	Erstatning for immateriel skade efter databeskyttelsesforordningen ved ulovlig videregivelse af følsomme helbredsoplysninger	10370-12199
19.11.2024	Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	6704-8053
BYRETTEEN · FØRSTE INSTANS		2

12.01.2026	Civilstyrelsen dømt til at betale 112.500 kr. for videregivelse af følsomme oplysninger om voldtægtsoffer til gerningsmand	10379-12211
11.05.2021	Afgørelse i sag om databrud i Gladsaxe Kommune: Frifindelse for erstatningskrav	3371-4012
PROCESBEVILLINGSNÆVNET · NÆVN / KLAGEINSTANS		1
04.03.2025	Procesbevillingsnævnet: 3.-instansbevilling om immateriel skade efter GDPR artikel 82 ved databrud med 20.000 borgeres CPR-numre	C-590/22

FORARBEJDE Betænkninger

4 referencer

Behandling af personoplysninger - Betænkning afgivet af udvalget om registerlovgivningen

nr. 1345 · 1997 · Justitsministeriet

Betænkning om tv-overvågning (Betænkning nr. 1483/2006)

nr. 1483 · 2006 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 1)

nr. 1565 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 2)

nr. 1565 · 2017 · Justitsministeriet

09

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over hacking og uberettiget adgang til IT-systemer (§ 263, § 263 a)

Strafudmåling og kvalificering efter straffelovens §§ 263 og 263 a

Version 2 · Opdateret 26. jun. 2026 · 12 afgørelser · 2014-2026

[Læs online](#)**INTRODUKTION**

Straffelovens § 263 kriminaliserer uberettiget adgang til en andens datasystem eller data, mens § 263 a retter sig mod den, der uberettiget skaffer sig eller videregiver adgangsmidler til datasystemer. Bestemmelserne udgør det strafferetlige kernegrundlag for hacking-sager i dansk ret og har en normalstrafferamme på bøde eller fængsel indtil 1 år og 6 måneder, med en kvalificeret strafferamme på fængsel indtil 6 år ved særligt skærpende omstændigheder, herunder industrispionage, systematisk karakter eller betydelige skadevirkninger. Retspraksis spænder fra bøder for enkle overtrædelser til straffe på 3½ års fængsel for de groveste angreb mod samfundsvigtig infrastruktur, og der lægges særlig vægt på adgangsens varighed, mængden af kompromitterede data og udnyttelse af betroet stilling.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Uberettiget adgang til et datasystem er fuldbyrdet allerede ved, at gerningsmanden skaffer sig adgang – det er uden betydning, hvad der efterfølgende foretages i systemet.
- 02 Udtrykket 'datasystem' omfatter computere, smartphones, tablets og ethvert elektronisk udstyr med databehandlingsfunktioner, herunder også data på USB-stik der ikke er tilsluttet et system.
- 03 Flere hackerangreb begået inden for kort tid mod samme mål skal bedømmes samlet ved vurderingen af, om der foreligger 'særligt skærpende omstændigheder' efter § 263, stk. 3.
- 04 Den skærpede strafferamme i § 263, stk. 3, på fængsel indtil 6 år finder ikke kun anvendelse ved industrispionage, men også ved angreb der medfører betydelige skadevirkninger for offentlige eller private interesser.
- 05 Udnyttelse af viden fra en tidligere betroet stilling og brug af en kollegas loginoplysninger kan kvalificere forholdet som begået under 'særligt skærpende omstændigheder'.
- 06 Hacking af samfundsvigtige datasystemer med download af store mængder personfølsomme data – f.eks. politiregistre og CPR-data – straffes i niveauet 3-4½ års fængsel.

- 07** Systematisk fjernstyring af 40+ privatcomputere via malware (f.eks. Netwire) straffes med fængsel i 6 måneder, delvist betinget, med vægt på krænkelsens omfang og varighed.
- 08** Hacking kombineret med identitetstyveri, videregivelse af intime billeder og skjulte optagelser udgør selvstændigt strafbare forhold, der straffes i sammenstød med § 263.
- 09** En arbejdsgiver, der tilgår en fratrådt medarbejders private e-mailkonto uden hjemmel, overtræder både databeskyttelsesforordningen og kan gøre sig skyldig i hacking efter § 263.
- 10** Datahærværk i form af sletning af data i virksomheders IT-systemer kvalificeres efter § 291, stk. 2, når udbedringsomkostningerne overstiger ca. 15.000 kr. eller driften lægges ned.
- 11** Strafferammerne i § 263 blev forhøjet ved lovændringen i 2004 for bedre at afspejle det IT-baserede samfunds sårbarhed og for at undergive IT-kriminalitet samme strafmaksimum som traditionelle formueforbrydelser.
- 12** Ved nyaffattelsen i 2019 blev § 263 omstruktureret, så datakriminalitet (adgang til datasystemer) nu er bestemmelsens hovedregel i stk. 1, mens brevfredskrænkelse er flyttet til stk. 2.

Retsgrundlaget: §§ 263 og 263 a om uberettiget adgang til datasystemer

§ 1

Den strafferetlige regulering af hacking og uberettiget adgang til IT-systemer hviler på to bestemmelser i straffelovens kapitel 27 om freds- og ærekrænkelser.

Straffelovens § 263 er bestemmelsens kerneregulering. Efter den gældende affattelse (der trådte i kraft 1. januar 2019) straffes i **stk. 1** med bøde eller fængsel indtil 1 år og 6 måneder den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem. **Stk. 2** vedrører den subsidiære brevfredskrænkelse (åbning af lukkede meddelelser og skjult aflytning). Den kvalificerede strafferamme i **stk. 3** hæver strafmaksimum til fængsel indtil 6 år, når forholdet begås:

- med forsæt til at skaffe sig erhvervshemmeligheder, eller
- under andre *særligt skærpende omstændigheder*, eller
- (for stk. 1-overtrædelser) når der er tale om overtrædelser af *mere systematisk eller organiseret karakter*.

Straffelovens § 263 a kriminaliserer den, der uberettiget sælger, udbreder eller videregiver adgangsmidler (koder, passwords mv.) til datasystemer. Bestemmelsen blev nyaffattet ved freds- og ærekrænkelserloven i 2019 og samler den tidligere § 263 a (ikke-kommercielle systemer) og § 301 a (kommercielle systemer) i én bestemmelse. Stk. 2 indeholder en skærpet strafferamme på fængsel indtil 6 år ved særligt skærpende omstændigheder.

Hacking medfører regelmæssigt samtidig overtrædelse af § 291 om hærværk, når der slettes eller beskadiges data. Angreb på *samfundsvigtige* datasystemer kan desuden rammes af § 193 om omfattende forstyrrelse i driften af offentlige kommunikationsmidler, IT-systemer m.v., med en strafferamme på fængsel indtil 6 år.

Afgrænsning mod beslægtede praksisoversigter: Når den uberettigede adgang bruges til økonomisk udnyttelse (f.eks. pengeoverførsler), overgår forholdet typisk til [databedrageri](#) efter § 279 a. Misbrug af ulovligt opnåede NemID/MitID-legitimationsoplysninger til transaktioner er behandlet i [mitid-nemid-misbrug](#).

LOV

Straffeloven § 193

Straffeloven § 263, stk. 1, 3

Straffeloven § 263a, stk. 1

Straffeloven § 291, stk. 2

§ 2 Lovhistorik: Fra brevhemmelighed til cyberforbrydelse

Straffelovens § 263 har gennemgået en markant udvikling fra sin oprindelse som beskyttelse af brevhemmeligheden til i dag at udgøre det primære strafferetlige værn mod IT-kriminalitet.

Bestemmelsens oprindelse (1930) var knyttet til fredskrænkelser – brud på brevhemmelighed og krænkelse af private gemmer. Hacking var naturligvis ukendt på dette tidspunkt.

1985-lovændringen indførte den daværende § 263, stk. 2, om uberettiget adgang til en andens *oplysninger eller programmer*, der er bestemt til at bruges i et *informationssystem*. Hermed blev datakriminalitet for første gang direkte kriminaliseret i dansk ret.

2004-lovændringen forhøjede strafferammerne markant. Som Højesteret bemærkede i [Sag 219/2017](#):

"Det fremgår af forarbejderne til lovændringen i 2004, hvorved strafferammerne i § 263, stk. 2 og 3, blev forhøjet, at dette skete for bl.a. bedre at afspejle forbrydelsens alvor under hensyn til det it-baserede samfunds sårbarhed og for at undergive kriminalitet rettet mod informationer samme strafmaksimum som kriminalitet rettet mod mere traditionelle værdier i form af penge og ting."

2019-nyaffattelsen – gennemført med baggrund i [Straffelovrådets betænkning nr. 1563/2017 om freds- og ærekrænkelser](#) – omstrukturerede bestemmelsen grundlæggende. Datakriminalitet (adgang til datasystemer) blev rykket fra stk. 2 til stk. 1, mens brevfredskrænkelse blev subsidieret i stk. 2. Terminologien blev moderniseret: "informationssystem" blev til "datasystem", og "oplysninger eller programmer" til "data".

Forarbejderne til nyaffattelsen præciserer udtrykkeligt, at bestemmelsens gerningsindhold er bredt:

"Den foreslåede bestemmelse vil således omfatte meget forskelligartede forhold, herunder at en gerningsmand skaffer sig adgang til en andens computer eller smartphone [...], at en gerningsmand logger på en andens e-mailsystem [...], eller at en gerningsmand skaffer sig adgang til et usb-stik."

Bestemmelsen omfatter også den, der udnytter en svaghed i et datasystem, der giver en videre adgang end tilsigtet – f.eks. URL-manipulation eller udnyttelse af en softwaresårbarhed.

LOV

Straffeloven § 263, stk. 1, 2

PRAKSIS

Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018

§ 3 De groveste sager: Hacking af samfundsvigtig infrastruktur (3-4½ års fængsel)

De strengeste straffe i dansk praksis er idømt for systematisk hacking af samfundsvigtige IT-systemer, hvor store mængder personfølsomme data er blevet kompromitteret.

CSC-hackersagen er den mest alvorlige hackingsag, der har været behandlet ved danske domstole. Sagen vedrørte et omfattende og teknisk kompliceret angreb i 2012 mod en stor IT-virksomheds mainframe, der driftede bl.a. Kriminalregisteret, CPR-registeret, Kørekortregisteret og Schengen Informationssystemet for Rigspolitiet.

Angriberen etablerede tre bagdøre i systemet og downloadede i alt ca. 19 GB data til servere i Iran, Cambodia og Tyskland over en periode fra februar til august 2012. Byretten ([SS-5591/2014-FRB](#)) idømte tiltalte fængsel i 3 år og 6 måneder. Østre Landsret ([SS-3126/2014-OLR](#)) stadfæstede enstemmigt dommen og fastslog:

"Sagen er den hidtil alvorligste af sin karakter, hvor der i forbindelse med angreb, der foregik systematisk og havde en lang tidsmæssig udstrækning, blev downloadet en betydelig mængde stærkt personfølsomme oplysninger til servere i Tyskland, Cambodja og Iran."

Forholdet blev henført under [§ 263, stk. 3](#) (skærpet strafferamme) og [§ 291, stk. 2](#) (hærværk af betydeligt omfang), men retten fandt det ikke godtgjort, at angrebene havde fremkaldt en *omfattende forstyrrelse* i driften, hvorfor tiltalen efter [§ 193](#) ikke førte til domfældelse. Tiltalte blev desuden udvist.

Bevistemaet om fjernstyring er af særlig interesse. Tiltalte forklarede, at hans computere havde været fjernstyret af ukendte tredjeparter. Landsretten fandt, at muligheden for fjernstyring ikke helt kunne udelukkes, men at den samlede bevisførelse – herunder krypterede containere med de stjalne data, chatlogs og personspecifikke søgninger – "samlet set helt oplagt og entydigt" godtgjorde tiltaltes medvirken. Retten bemærkede, at en person med indgående IT-kendskab ikke ville have undladt at opdage en uautoriseret fjernstyring over en periode på 6 måneder.

LOV

[Straffeloven § 193](#)[Straffeloven § 263, stk. 3](#)[Straffeloven § 291, stk. 2](#)

PRAKSIS

Landsretten · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem 17.06.2015

Byretten · Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014) 31.10.2014

§ 4 Hacking mod tidligere arbejdsplads: Udnyttelse af betroet stilling

Højesterets dom i [Sag 219/2017](#) er den ledende afgørelse om hacking begået af en tidligere ansat med udnyttelse af viden fra en betroet IT-stilling.

Tiltalte – en tidligere IT-chef – gennemførte i november 2014 tre målrettede angreb mod sin tidligere arbejdsgivers IT-systemer:

Dato	Angreb	Konsekvens
8. nov. 2014	Sletning af data i SAN-lagringsenhed	Virksomhedens drift lammet
9. nov. 2014	Sletning af indholdsfortegnelse på NAS	Backups ødelagt
16. nov. 2014	Sletning af intranet	Genetableret via papirkurv

Angrebene medførte, at virksomheden reelt blev "lagt ned", medarbejdere hjemsendt og udbedringsomkostninger på over 400.000 kr.

Højesteret fastslog tre afgørende principper:

1. **Samlet bedømmelse:** De tre angreb skal bedømmes samlet – ikke isoleret – ved vurderingen af, om der foreligger "særligt skærpende omstændigheder".
2. **Ikke kun industrispionage:** Udtrykket "andre særligt skærpende omstændigheder" i § 263, stk. 3 rummer også tilfælde, der vanskeligt kan angives mere præcist, herunder tilfælde med betydelige skadevirkninger for private interesser – selv uden formål om erhvervshemmelighedsspionage.
3. **Strafniveau:** Straffen for hackingforholdene og hærværket isoleret set bør ligge omkring **2 års fængsel**. Den samlede straf for alle 81 forhold (herunder 78 bedrageriforhold) blev fastsat til **fængsel i 3 år og 6 måneder**.

Højesteret afviste betinget dom og samfundstjeneste henset til straffens længde og kriminalitetens alvor.

LOV

Straffeloven § 263, stk. 3

Straffeloven § 291, stk. 2

PRAKSIS

Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018

Hacking af private computere og identitetstyveri:

§ 5 Normalstrafniveauet

Under den skærpede strafferamme ligger en betydelig gruppe sager, hvor privatpersoners computere eller konti kompromitteres – typisk via fjernstyringsprogrammer, stjålne passwords eller social engineering. Strafniveauet ligger her i intervallet 3-6 måneders fængsel, ofte delvist betinget.

Netwire-sagen (S-323-15) vedrørte en tiltalte, der over ca. ét år uberettiget skaffede sig adgang til 40 private computere via fjernstyringsprogrammet Netwire. Programmet gav adgang til filkopiering, keylogging, skærbilleder og remote shell. Østre Landsret skærpede byrettens straf fra 4 til **6 måneders fængsel**, hvoraf 3 måneder betinget med 3 års prøvetid:

"Efter arten og omfanget af lovovertrædelserne, der har strakt sig over en periode på omkring 1 år, samt henset til den krænkelse, som lovovertrædelserne har medført for de forurettede, finder landsretten, at straffen [...] bør forhøjes til fængsel i 6 måneder."

Hacking kombineret med seksuelle krænkelser (S-1264-18) viser sammenstødet mellem § 263 og andre bestemmelser. Tiltalte havde over en længere periode udnyttet sin IT-tekniske viden til at hacke flere kvinders konti, videregivet intime billeder og foretaget skjulte videooptagelser af samleje. Østre Landsret skærpede straffen til **5 måneders ubetinget fængsel** med følgende begrundelse:

"Ved straffastsættelsen er der navnlig lagt vægt på sagens karakter og omfang, herunder at der er tale om adskillige og systematiske krænkelser, hvor tiltalte gennem en længere periode har udnyttet og misbrugt sin it-tekniske viden til at begå alvorlige og krænkende lovovertrædelser."

Trods tiltaltes ustraffethed fandt retten ikke grundlag for betinget dom. Der blev desuden tilkendt tortgodtgørelse til de forurettede på 5.000-20.000 kr. pr. person.



LOV	Erstatningsansvarsloven § 26, stk. 1	Straffeloven § 263, stk. 1	Straffeloven § 264d
PRAKSIS	Landsretten · Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje 26.09.2018 Landsretten · Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden 30.03.2015		

§ 6 Gerningsindholdet: Hvad udgør 'uberettiget adgang'?

Et centralt fortolkningsspørgsmål i praksis er, hvornår en adgang er "uberettiget" i bestemmelsens forstand. Forarbejderne til 2019-nyaffattelsen præciserer, at bestemmelsen er formuleret bredt, og at der *regelmæssigt* skal ske en udskillelse af legale handlinger fra det strafbare.

Adgangen er fuldbyrdet ved selve indtrængen. Det er uden betydning, hvad gerningsmanden efterfølgende foretager sig i systemet – om data kopieres, ændres, slettes eller blot betragtes. Allerede det at skaffe sig adgang fuldender gerningen.

Overskridelse af autoriseret adgang kan også være strafbar. Forarbejderne nævner udtrykkeligt:

- En medarbejder, der har berettiget adgang til arbejdsgiverens system, men som tilgår data, der ikke er arbejdsmæssigt behov for – navnlig hvis medarbejderen har videregående forsæt til at videregive data.
- En kunde, der har berettiget adgang til en brugerflade, men som udnytter en fejl eller svaghed i systemet til at kopiere, ændre eller slette data.

URL-manipulation er et særligt relevant eksempel. Datatilsynet har i flere afgørelser fastslået, at "Broken Access Control" via URL-manipulation er en velkendt sårbarhed – klassificeret som A5:2017 på OWASP Top 10-listen – og at systemer, der tillader uberettiget adgang via URL-ændringer, ikke opfylder kravene til behandlingssikkerhed efter [GDPR art. 32](#).

Adgang til private e-mailkonti er behandlet i Datatilsynets afgørelse [2024-31-0529](#), hvor en virksomhed tilgik en fratrådt medarbejders personlige e-mailkonto, som stod åben i en webbrowser på en afleveret arbejdscomputer. Datatilsynet udtalte alvorlig kritik og bemærkede, at spørgsmålet om en eventuel overtrædelse af [§ 263](#) ikke henhørte under Datatilsynets kompetence – hvilket antyder, at forholdet efter omstændighederne også kan være strafbart.

I sagen om [Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser](#) (2024-32-0482) fandt Datatilsynet, at en offentlig myndighed lovligt kan inddrage oplysninger, der er skaffet i strid med [§ 263, stk. 2](#), af en privat tredjepart – men kun fordi myndigheden selv ikke havde medvirket til den ulovlige handling, og fordi hensynet til barnets bedste og officialpligten vejede tungere.

LOV	Databeskyttelsesforordningen § 32, stk. 1	Straffeloven § 263, stk. 1
PRAKSIS	Datatilsynet · Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer 25.10.2024 Datatilsynet · Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag 13.09.2024	

§ 7 Samspillet med GDPR-håndhævelse og datasikkerhed

Hacking-sager har en vigtig pendant i databeskyttelsesretten. Mens straffeloven retter sig mod gerningsmanden, kan den dataansvarlige organisation – der har undladt at sikre sine systemer tilstrækkeligt – også drages til ansvar efter [GDPR art. 32](#) om behandlingssikkerhed.

Bødestraf til dataansvarlige for utilstrækkelig IT-sikkerhed er blevet en fast del af praksis:

- Vestre Landsret idømte i [SS-113/2025-VLR](#) en region en bøde på **500.000 kr.** for en URL-sårbarhed i en spørgeskemadatabase, der eksponerede 23.000 borgeres helbredsoplysninger i over halvandet år.
- Østre Landsret stadfæstede i [S-2302-23](#) en **bøde på 50.000 kr.** til en kommune for manglende adgangskontrol i et tandplejesystem, der risikerede at afsløre adressebeskyttede borgeres oplysninger.
- Datatilsynet politianmeldte [Lyngby-Taarbæk Kommune](#) og indstillede til en bøde på 350.000-400.000 kr. for manglende flerfaktorautentifikation og brugerrevokation, efter at en uvedkommende tredjepart udnyttede svage loginoplysninger til at tilgå 5.000 borgeres data.

Erstatning for immateriel skade efter databrud er fortsat svær at opnå. I sagen om Gladsaxe Kommunes databrud ([BS-19616/2021-OLR](#)) fastslog Østre Landsret, at kommunen havde overtrådt [GDPR art. 32](#), men at de seks sagsøgende borgere ikke havde godtgjort at have lidt immateriel skade efter [GDPR art. 82](#). Retten lagde bl.a. vægt på, at computeren var stjålet sammen med andre genstande og pantflasker, at der ikke var bevis for, at uvedkommende faktisk havde tilgået dataene, og at to borgeres efterfølgende identitetstyverier ikke var dokumenteret at have årsagssammenhæng med det konkrete databrud.

LOV	Databeskyttelsesforordningen § 32, stk. 1	Databeskyttelsesforordningen § 82, stk. 1
	Databeskyttelsesforordningen § 83, stk. 2	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Landsretten · Region idømt bøde på 500.000 kr. for brud på datasikkerhed – URL-sårbarhed i CBCL-database	23.03.2026
	Landsretten · Kommune idømt bøde på 50.000 kr. for utilstrækkelig IT-sikkerhed i tandpleje-system, der risikerede at afsløre beskyttede adresser	19.02.2025
	Landsretten · Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	19.11.2024
	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024

§ 8 Strafudmålingens centrale momenter

På tværs af den foreliggende praksis kan følgende momenter identificeres som afgørende for strafudmålingen:

Skærpende omstændigheder:

- Angreb på samfundsvigtige systemer (politiregistre, sundhedsdata, CPR)
- Stor datamængde kompromitteret (tusindvis eller millioner af personers data)
- Lang varighed – systematisk angreb over uger eller måneder
- Udnyttelse af betroet stilling eller insiderviden
- Betydelige skadevirkninger (driftsstans, udbedringsomkostninger over 400.000 kr.)
- Anvendelse af sofistikerede metoder (bagdøre, kryptering, scripts)
- Videre salg eller videregivelse af kompromitterede data

Formildende omstændigheder:

- Tilståelse og samarbejde med myndigheder
- Ung alder eller gode personlige forhold
- Begrænset varighed eller omfang af det uberettigede adgang
- Ingen videregivelse af opnåede data

Oversigt over straffniveauer i praksis:

Sagstype	Typisk straf	Eksempel
Hacking af samfundsvigtig infrastruktur med datanedlastning	3-4½ års fængsel	CSC-sagen (3½ år)
Groft datahærværk mod arbejdsgivers IT-system med bedrageri	2-3½ års fængsel	Sag 219/2017 (3½ år samlet)
Systematisk fjernstyring af mange private computere	4-6 måneders fængsel, delvist betinget	Netwire-sagen (6 mdr.)
Hacking + identitetstyveri + digitale sexkrænkelser	5-8 måneders fængsel	S-1264-18 (5 mdr.)

Det er værd at bemærke, at de mest alvorlige sager – CSC og Sag 219/2017 – begge resulterede i præcis 3 år og 6 måneders fængsel, hvilket i praksis synes at udgøre det øverste straffniveau for hackingsager i dansk ret. Strafferammens maksimum på 6 år er endnu ikke nået.

LOV

Straffeloven § 263, stk. 3

PRAKSIS

- Højesteret** · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018
- Landsretten** · Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje 26.09.2018
- Landsretten** · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem 17.06.2015
- Landsretten** · Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden 30.03.2015

§ 9 Sammenfatning og udviklingstendenser

Retspraksis om hacking og uberettiget adgang til IT-systemer viser en klar udvikling i retning af strengere sanktioner og en bredere forståelse af gerningsindholdet.

Straffniveauet er steget markant siden bestemmelsens indførelse. De to ledende afgørelser – CSC-hackersagen og Sag 219/2017 – ligger begge på 3½ års fængsel og markerer den øvre grænse i praksis. For mindre alvorlige overtrædelser ligger straffniveauet typisk i intervallet 3-6 måneders fængsel, delvist betinget.

Gerningsindholdet er blevet udvidet ved 2019-nyaffattelsen, der moderniserede terminologien og placerede datakriminalitet som bestemmelsens hovedregel. Forarbejderne understreger den brede forståelse af "uberettiget adgang", der også omfatter overskridelse af autoriseret adgang.

Samspillet med databeskyttelsesretten er et centralt træk ved moderne hackingsager. Hvor straffeloven retter sig mod angriberen, kan den utilstrækkelig sikre dataansvarlige nu også bødestraffes – med bøder der i praksis

kan nå 500.000 kr. for offentlige myndigheder. De to regelsæt supplerer hinanden og skaber samlet set et stærkere sanktionssystem.

Kritisk infrastruktur nyder en særlig beskyttelse. NIS-direktivet og den danske implementering i [NIS-bekendtgørelsen](#) stiller krav om, at operatører af væsentlige tjenester indfører passende sikkerhedsforanstaltninger. Angreb på sådanne systemer kvalificeres regelmæssigt under den skærpede strafferamme i § 263, stk. 3.

Bevissspørgsmål står centralt i hackingsager. CSC-sagen illustrerer, at forsvarets typiske indvending – at computeren var fjernstyret – kræver stærk teknisk dokumentation for at bære igennem. Domstolene lægger vægt på den samlede bevissituation, herunder digitale spor som krypterede containere, chatlogs, IP-adresser og tidsmæssig sammenhæng mellem aktivitet og anholdelse.

Der er ingen vedtagne men endnu ikke konsoliderede ændringer til [§ 263](#) pr. juni 2026.

LOV	Straffeloven § 263, stk. 1, 3	Straffeloven § 263a	
PRAKSIS	Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads		27.02.2018
	Landsretten · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem		17.06.2015
	Byretten · Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014)		31.10.2014

REFERENCE Lovgrundlag

4 paragraffer

Straffeloven § 193		Straffeloven § 263	stk. 1, 3
Straffeloven § 263a	stk. 1, 2	Straffeloven § 291	stk. 2

MATERIALE Citerede afgørelser

11 afgørelser

HØJESTERET · ØVERSTE INSTANS		1
27.02.2018	Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads	219-2017
LANDSRETTEEN · ANKEINSTANS		6
23.03.2026	Region idømt bøde på 500.000 kr. for brud på datasikkerhed – URL-sårbarhed i CBCL-database	10573-12480
19.02.2025	Kommune idømt bøde på 50.000 kr. for utilstrækkelig IT-sikkerhed i tandpleje-system, der risikerede at afsløre beskyttede adresser	S-2302-23
19.11.2024	Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	6704-8053
26.09.2018	Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje	S-1264-18

17.06.2015 Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem 10786-13836

30.03.2015 Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden S-323-15

BYRET TEN · FØRSTE INSTANS 1

31.10.2014 Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014) 10740-12764

DATATILSYNET · NÆVN / KLAGEINSTANS 3

27.11.2024 Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb

25.10.2024 Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer 2024-31-0529

13.09.2024 Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag 2024-32-0482

FORARBEJDE Betænkninger

1 reference

Straffelovrådets betænkning om freds- og ærekrænkelser

nr. 1563 · 2017 · Justitsministeriet

10

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over IT-leverancekontrakter – forsinkelse, mangler og ophævelse

Forsinkelse, mangler, ophævelse og ansvarsbegrænsning i kommercielle og offentlige it-projekter

Version 2 · Opdateret 3. sep. 2026 · 41 afgørelser · 2002-2026

[Læs online](#)

INTRODUKTION

Tvister om levering, udvikling og drift af it-systemer afgøres i Danmark uden en speciallov: aftalegrundlaget, købelovens analoge anvendelse og de almindelige obligationsretlige grundsætninger bærer afgørelserne. Praksis er koncentreret i Sø- og Handelsretten, suppleret af landsretterne, byretterne, Klagenævnet for Udbud og – på forbrugersiden – Forbrugerklagenævnet, mens de allerstørste leverancetvister typisk afgøres ved fortrolig voldgift. De offentligt tilgængelige domme viser et gennemgående mønster: væsentlighedstærsklen for ophævelse af et it-projekt er høj, kundens egen medvirken og uklarhed i kravgrundlaget slår tilbage på kunden, og tabsopgørelsen skæres kraftigt ned, når den ikke er nøje dokumenteret. På forbrugersiden er retstilstanden derimod lovfæstet efter implementeringen af varedirektivet og direktivet om digitalt indhold i købelovens §§ 3 a, 4 a og 75 a-78 e.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Der findes ingen speciallov om it-leverancer; retsstillingen fastlægges af aftalen, købelovens analoge anvendelse og almindelige obligationsretlige grundsætninger, og domstolene undlader ofte at tage endelig stilling til, om købeloven eller værkslejeretten er rammen.
- 02 En milepælsprøves retlige karakter – stop-test eller ren fremdriftsprøve – afgøres af kontraktens ordlyd og parternes adfærd; kvalificeres prøven som fremdriftsprøve, kan kunden ikke hæve alene på det manglende testresultat.
- 03 Kunden bærer bevisbyrden for, at fejlniveauet ved en overtagelses- eller driftsprøve overskrider kontraktens grænser; er fejlklassifikationen ikke sket i fællesskab som aftalt, falder bevisbyrden typisk ud til leverandørens fordel.
- 04 Uklarhed om kravspecifikationens indhold, som begge parter har bidraget til, kan ikke ensidigt lægges leverandøren til last og udelukker som udgangspunkt ophævelse på det pågældende punkt.

- 05** En uberettiget ophævelse af en it-kontrakt er en dyr fejl: leverandøren kan kræve erstatning opgjort som negativ kontraktinteresse, og domstolene nedsætter ikke beløbet skønsmæssigt, når det er dokumenteret ved bogføringsudtræk.
- 06** Giver samarbejdsaftalen kun adgang til at ophæve hele kontrakten ved væsentlig misligholdelse, er delvis ophævelse af enkeltrettigheder – fx brugsretten til et fællesudviklet it-system – ikke hjemlet.
- 07** Kundens egen skyld kan reducere eller helt bortfælde leverandørens ansvar, selv når leverandøren som professionel it-leverandør har handlet ansvarspådragende ved mangelfuld vejledning.
- 08** Skønsmæssig nedsættelse er hovedreglen ved udokumenterede tabsopgørelser i it-sager; krav på tocifrede millionbeløb reduceres rutinemæssigt til en brøkdel.
- 09** Aftalte ansvarsbegrænsninger tilsidesættes ikke rutinemæssigt mellem erhvervsdrivende, men rækker ikke til misligholdelse, der samtidig indebærer lovovertrædelser eller går ud over kontraktens rammer.
- 10** Ophavsretten til software følger ophavsmanden, medmindre programmet er frembragt under udførelsen af et ansættelsesforhold eller efter arbejdsgiverens anvisninger; betaling af et engangshonorar dokumenterer ikke i sig selv en rettighedsoverdragelse.
- 11** Ideer og ønsker til nye funktioner fra kundens eller arbejdsgiverens medarbejdere kan ikke sidestilles med »anvisninger« efter ophavsretslovens § 59.
- 12** Løbende it-ydelser til en ikke-erhvervsdrivende part kan opsiges efter forbrugeraftalelovens § 28 uanset aftalt uopsigelighed; leverandøren bærer bevisbyrden for, at aftalen ikke er en forbrugeraftale.
- 13** Manglende dokumentation for udført arbejde under en løbende digital serviceaftale er i sig selv væsentlig misligholdelse, der berettiger kunden til at ophæve og kræve det betalte tilbage.
- 14** I forbrugerkøb er digitalt indhold og digitale tjenester ligestillet med varer, og softwarefejl, manglende opdateringer og manglende medfølgende dokumentation udgør mangler efter købelovens §§ 75 b-75 d.
- 15** I offentlige it-anskaffelser er udskydelse af ibrugtagningsdagen og midlertidig videreførelse af det gamle system ikke uden videre en ændring af et grundlæggende element, men lempelse af mindstekrav og prisforhøjelser er det.

Retsgrundlaget: aftalen, købeloven analogt og de obligationsretlige grundsætninger

§ 1

IT-leverancekontrakter er ikke reguleret af en speciallov. Retsstillingen fastlægges derfor af tre lag: parternes eget aftalegrundlag (herunder standardkontrakter og standardbetingelser), købelovens regler anvendt analogt på blandede leverancer af hardware, standardprogrammel og individuel udvikling, samt de almindelige obligationsretlige grundsætninger om væsentlig misligholdelse, loyal samarbejdsplicht, reklamation og tabsbegrænsning.

Denne uafklarethed slår igennem i praksis. I **BS-475/2010-ARH** om udvikling af en hjemmeside gjorde kunden gældende, at ophævelse kunne ske efter [købelovens § 42, stk. 1](#), mens leverandøren bestred, at købeloven overhovedet fandt anvendelse, fordi leverancen var en tjenesteydelse. Retten i Aarhus tog ikke stilling til spørgsmålet, men afgjorde sagen efter en samlet vurdering af forløbet og nedsatte skønsmæssigt vederlaget. Kunden havde i den sag anført, at »IT-ydelsers kompleksitet indebærer, at der indgår både køberetlige og entreprise/værkslejlignende momenter« – en formulering, der rammer kernen i det danske retsgrundlag på området.

For forsinkelse er købelovens udgangspunkt strengt: efter [købelovens § 21, stk. 1](#) har køberen valget mellem at kræve levering og at hæve, og efter [§ 21, stk. 3](#) anses enhver forsinkelse i handelskøb for væsentlig, medmindre kun en ringe del af det solgte er forsinket. I praksis fraviges dette udgangspunkt næsten altid ved aftale i it-kontrakter, hvor parterne i stedet fastsætter dagbod, karenperioder og konkrete ophævelsestærskler.

For mangler leverer købelovens forbrugerkøbsregler i dag den mest udbyggede begrebsramme, og de anvendes ofte som fortolkningsinspiration også uden for forbrugerforhold. Efter [købelovens § 75 b](#) skal ydelsen svare til den aftalte beskrivelse og have den aftalte funktionalitet, kompatibilitet og interoperabilitet, være egnet til køberens særlige formål, som sælgeren har accepteret, og »opdateres som fastsat i aftalen«. Efter [§ 75 c, stk. 1, nr. 1](#) skal ydelsen være egnet til de formål, genstande af samme type normalt anvendes til – den danske udmøntning af »fit for purpose«.

Standardkontrakterne udgør et fjerde, faktisk retskildelag. Allerede [betænkning nr. 1227/1991 om udlicitering af offentlige drifts- og anlægsopgaver](#) beskrev »Statens standardkontrakt for EDB-totalleverancer« som normalgrundlaget ved køb af en totalløsning omfattende »såvel edb-udstyr, standardprogramprodukter og individuelt udviklede systemer«, og [Delbetænkning IV fra EDB-Samordningsudvalget \(nr. 867/1979\)](#) fremhævede allerede dengang, at kontraktforhold var »et fælles problem«, og at de offentlige datacentraler burde søge standardkontrakten anvendt i størst muligt omfang.

LOV

Købeloven § 21, stk. 1-3

Købeloven § 42, stk. 1

Købeloven § 75b

Købeloven § 75c, stk. 1

PRAKSIS · Byretten · Sag om honorar for hjemmesideudvikling

07.02.2011

Milepæle, overtagelsesprøve og driftsprøve som forsinkelsens juridiske omdrejningspunkt

I it-kontrakter er leveringsbegrebet erstattet af et prøveregime. [Vejledningen om Statens standardkontrakt for standardiserede edb-systemer](#) beskriver den arketypiske model, som stort set alle senere danske it-standardkontrakter bygger videre på:

Afprøvning af systemet samt af den dertil hørende dokumentation sker ved en overtagelsesprøve før overtagelsesdagen samt en driftsprøve i tiden derefter.

Overtagelsesprøven er en [funktionsprøve](#), hvor udstyrs- og programprodukterne kontrolleres enkeltvis og [integreret](#), og består den ikke, er leverandøren berettiget til at gentage prøven, »indtil kunden måtte hæve kontrakten efter bestemmelserne herom«. [Driftsprøven](#) måler derimod driftseffektivitet og svartider på systemet som helhed over mindst 20 sammenhængende arbejdsdage.

Det er afgørende, at kundens beføjelser er knyttet til prøverne. Standardkontrakten opstiller derfor en objektiv ophævelsestærskel:

Følgende forhold anses altid for væsentlig misligholdelse, der berettiger kunden til straks at hæve kontrakten helt eller delvis efter kundens valg: Overskridelse af den aftalte overtagelsesdag eller af fristen for tilfredsstillende afslutning af driftsprøve med mere end 30 arbejdsdage.

Vejledningen forklarer samtidig, hvorfor bod og ophævelsesadgang overhovedet er med:

»Misligholdelsesbeføjelserne er ikke primært begrundet i kundens interesse i f.eks. at kunne oppebære bod, men formålet er at give leverandøren et incitament til at sætte alle kræfter ind på at opfylde kontrakten.«

Ved **faseopdelte leverancer** anbefales det udtrykkeligt at sikre, »at leverandørens totalansvar bibeholdes, og at kunden kan påberåbe sig kontraktens retsvirkninger helt eller delvist i forbindelse med hver enkelt fase« – en pointe, der bliver central for spørgsmålet om delvis ophævelse.

Mønsteret i praksis er, at domstolene håndhæver de aftalte tærskler, men kun når de er klart formuleret. I **H-23-05** om levering af interiør til 60 togsæt – en leverancesag med samme struktur som en it-leverance – indeholdt kontraktens art. 26.1.c en ubetinget hæveadgang ved overskridelse af en »fatal date« med mere end fire måneder uanset skyld, og Sø- og Handelsretten anvendte den efter at have rensset de forsinkelser ud, som kunden selv havde forårsaget:

Herefter har Bombardier været berettiget til at ophæve aftalen som sket i medfør af kontraktens art. 26.1.c.

At tidsfrister i it-kontrakter derimod ikke uden videre er ufravigelige mindstekrav, fremgår af Klagenævnet for Udbuds kendelse i **20/00982** om Region Hovedstadens vagtplanlægningssystem Optima. Nævnet fastslog, at ibrugtagningssagen den 1. januar 2020 ikke var et mindstekrav, men et konkurrenceparameter, og at kontraktens bestemmelse om leverandørens ret til at udskyde frister med højst 30 arbejdsdage ikke var en udtømmende regulering af forsinkelser – parterne kunne gensidigt aftale yderligere ændringer af tidsplanen.

LOV

[Købeloven § 21, stk. 3](#)

PRAKSIS

Sø- og Handelsretten · Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler 01.12.2008

Klagenævnet for Udbud · Ændring af kontrakt om IT-system til vagtplanlægning udgjorde ikke en ulovlig direkte tildeling 23.06.2020

§ 3 DACCIS-dommen: prøvens retlige karakter og prisen for en uberettiget ophævelse

Den centrale offentligt tilgængelige danske dom om ophævelse af et stort it-udviklingsprojekt er Sø- og Handelsrettens dom i **H-94-08** om Forsvarets kommando- og kontrolsystem DACCIS. Forsvarets Materieltjeneste (FMT) havde indgået en fastpriskontrakt på 40 mio. kr. med Saab AB med tre milepæle – Initial Capability, Operational Capability (OC) og Full Capability – og kontraktens § 9 gav FMT en udtrykkelig hæveadgang med fuld tilbagebetalingspligt, hvis den aftalte dato for godkendelse af milepæl OC blev overskredet.

Efter en afbrudt OC-test i uge 51/2007 og mislykkede forhandlinger hævede FMT kontrakten den 25. februar 2008. Sø- og Handelsretten frifandt Saab og gav leverandøren fuldt medhold i modkravet. Dommen fastlægger fire principper, der er gennemgående for hele området.

1. Prøvens retlige karakter er et fortolkningsspørgsmål. FMT gjorde gældende, at OC-testen var en stop-test og en delleverance med objektive beståelseskrav. Saab gjorde gældende, at der alene var tale om en fremdriftsprøve med vejledende fejlgrænser. Retten fulgte i realiteten Saab: bilagets fejlkriterier var formuleret som anbefalinger (»no more than 20 are recommended«), og fejlklassifikationen skulle efter aftalen ske i fællesskab.

2. Bevisbyrden for fejlniveauet påhviler den, der hæver.

Efter bevisførelsen finder retten, at FMT ikke har godtgjort, at det antal fejl, som blev observeret under testen i uge 51 ikke levede op til kontraktens bilag 6, punkt 3.5.2.b.

3. Uklarhed, som begge parter har skabt, kan ikke lægges leverandøren til last. Kernen i FMT's ophævelse var, at systemets MIP-interoperabilitet og Basis Data Manager ikke var testet. Retten fandt, at der ikke var stillet krav til, hvordan BDM skulle testes, og at parterne i fællesskab havde skabt uklarhed om MIP-standarden:

Efter forløbet findes begge parter har været med til at skabe uklarhed om, hvorvidt der skulle arbejdes videre med MIP BL 2 eller 3, således at det ikke kan komme Saab til skade, at MIP BL 2 ikke forelå færdig til OC.

Retten lagde tillige vægt på proportionaliteten: BDM og MIP vedrørte kun 7 ud af i alt 181 krav, og den manglende test af disse to dele medførte derfor ikke, at prøven ikke opfyldte kravene til en OC-test.

4. En hensigtserklæring om at forhandle i god tro afskærer ikke hæveadgangen – men beskytter heller ikke den, der hæver. Retten fandt, at hensigtserklæringen af 21. december 2007 pålagde parterne at forhandle i god tro, men ikke afskar FMT fra at gøre kontraktens ophævelsesbeføjelser gældende, hvis enighed ikke kunne opnås:

Parterne grundlæggende ikke var enige om, hvilket fundament der skulle til, for at der kunne indgås det aftalte kontrakttillæg. [...] FMT var dermed ikke den 25. februar 2008 afskåret fra at ophæve alene på grund af forløbet omkring hensigtserklæringen.

Resultatet blev alligevel, at ophævelsen var uberettiget, og FMT blev dømt til at betale 31.947.511,30 kr. – mere end kontraktsummen – plus 5.150.000 kr. i sagsomkostninger. Dommen er den tydeligste illustration af, at det for en it-kunde er en betydelig procesrisiko at hæve på et testresultat, som ikke entydigt kan henføres til leverandørens forhold.

§ 4 Manglers indhold: afvigelse fra kravspecifikation, manglende funktionalitet og manglende leverance

Mangelsbegrebet i it-leverancer spænder fra klassiske funktionsfejl til fravær af den aftalte ydelse overhovedet. Praksis skelner reelt mellem tre situationer.

Afvigelse fra kravspecifikation og garanti. Statens standardkontrakt indeholder en generel leverandørgaranti, hvorefter leverandøren garanterer, at de i bilagene anførte leverancer »er tilstrækkelige til at opfylde alle de i nærværende kontrakt stillede krav«, og at udviklings- og tilpasningsarbejde er udført »i overensstemmelse med god programmeringsskik«, jf. [vejledningens punkt 13.1](#). Er kravene ikke opfyldt, skal leverandøren uden merbetaling og inden for de aftalte frister levere det yderligere udstyr og programmel, der er nødvendigt. Hertil kommer i standardmodellen en selvstændig garanti for [driftseffektivitet og svartider](#), der løber i hele vedligeholdelsesperioden – altså en ydelses- og ikke kun en funktionsgaranti.

Manglende eller mangelfuld leverance. Hvor leverandøren slet ikke kan dokumentere at have leveret den aftalte digitale ydelse, er retsfølgen ikke afslag, men ophævelse. I **BS-46631/2023-OLR** havde en virksomhed betalt 129.950 kr. for en 24-måneders pakke »sociale medier, platin«. Awork A/S kunne hverken over for skønsmanden eller i retten fremlægge logs, timesedler eller andet materiale, og kontaktpersonen kunne ikke beskrive nogen konkret udført opgave. Østre Landsret konkluderede:

Landsretten finder på den baggrund, at der foreligger en væsentlig misligholdelse af aftalen, og at Virksomheden således har været berettiget til at have aftalen som sket ved mail af 31. januar 2022.

Dommen er en vigtig påmindelse om, at dokumentationsbyrden for udført arbejde i løbende digitale serviceaftaler i praksis ligger hos leverandøren, og at fravær af dokumentation i sig selv kan konstituere væsentlig misligholdelse.

Forsinket og forringet delleverance. I **BS-475/2010-ARH** fandt Retten i Aarhus, at en brugbar betaversion af en hjemmeside først forelå halvandet år efter aftalens indgåelse, og at leverandøren derfor ikke kunne kræve honorar for sitehosting og telefonsupport i nogen del af den aftalte etårige periode. Udviklingshonoraret på 34.000 kr. blev skønsmæssigt halveret:

Efter sagens oplysninger finder retten [...] at en regning på 34.000 kr. ekskl. moms er en for stor regning, henset til den begrænsede og forsinkede ydelse, som sagsøgte leverede, og retten nedsætter skønsmæssigt beløbet med halvdelen til 17.000 kr.

Afgrænsningen til scope og ændringsønsker. Grænsen mellem mangel og ændringsønske er notorisk vanskelig at trække, og den vanskelighed slår igennem procesretligt. I **BS-55788/2024-SHR** afviste Sø- og Handelsretten samtlige seks alternative forbudspåstande fra Estatetool A/S mod Mindworking A/S, fordi centrale begreber som »projektsalgs- og udlejningsløsning« og »understøtter« ikke var tilstrækkeligt afgrænset til at kunne indgå i en eksigibel konklusion, jf. [retsplejelovens § 411](#). Kendelsen viser, at en upræcis funktionsbeskrivelse ikke blot skaber materiel usikkerhed om, hvad der er aftalt, men også kan gøre kravet uegnet til retlig håndhævelse. Beslægtet hermed er **BS-21360/2022-SHR**, hvor en systemleverandør ikke kunne få nedlagt forbud mod, at tidligere ansatte solgte service- og vedligeholdelsesaftaler på leverandørens eget alarmmonitoreringssystem – retten lagde bl.a. vægt på, at de sagsøgte i deres aftalevilkår anerkendte leverandørens rettigheder til systemet.

LOV

[Købeloven § 75b](#)[Retsplejeloven § 411](#)

PRAKSIS

Landsretten · Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse

18.03.2025

Sø- og Handelsretten · Afvisning af midlertidigt forbud og påbud i softwarekonflikt grundet upræcise påstande

10.04.2025

Sø- og Handelsretten · Sag om midlertidigt forbud og påbud vedrørende overtrædelse af lov om forretningshemmeligheder og markedsføringsloven i forbindelse med salg og markedsføring af service- og vedligeholdelsesaftaler for software.	06.10.2023
Byretten · Sag om honorar for hjemmesideudvikling	07.02.2011

§ 5 Kundens medvirakenspligt, loyal samarbejdspligt og egen skyld

IT-projekter er samarbejdsprojekter, og praksis lader konsekvent kundens egne forsømmelser slå igennem på leverandørens ansvar.

Det tydeligste eksempel er **H-112-05**, hvor Sø- og Handelsretten frifandt Lundberg Data A/S for et krav på 574.475 kr. efter fejlagtig opsætning af regnskabsprogrammet Navision C5 håndværk. Retten fandt først, at leverandøren havde begået en ansvarspådragende fejl:

Lundberg Data var som IT-leverandør undergivet et skærpet ansvarsgrundlag, og undladelsen af særligt at fremhæve valgmuligheden mellem de to forskellige beregningsgrundlag udgjorde derfor en ansvarspådragende fejl.

Erstatningsansvaret bortfaldt ikke desto mindre helt på grund af kundens egen skyld:

Da en medarbejder hos BVS på baggrund af programmets opbygning aktivt valgte at foretage efterberegningen på grundlag af kostpriser i stedet for standardkostpriser uden at søge nærmere afklaring af konsekvensen af dette valg, og da BVS efter installeringen af det nye program undlod at foretage en manuel fakturakontrol, har BVS imidlertid udvist en sådan grad af egen skyld, at Lundberg Datas erstatningsansvar bortfald.

Dommen fastslår altså to ting samtidig: it-leverandøren er undergivet et skærpet ansvarsgrundlag for vejledning om væsentlige valg i systemopsætningen, men kunden har en tilsvarende egenkontrolpligt, og forsømmes den, kan hele ansvaret bortfalde.

Samme mekanisme viser sig i **BS-475/2010-ARH**, hvor leverandøren gjorde gældende, at hjemmesiden var værdiløs uden kundens tekstindhold, som først blev leveret halvanden måned efter aftalen. Retten nedsatte vederlaget skønsmæssigt uden at afgøre, hvor stor betydning kundens egenlevering havde – men netop ved at udmåle skønsmæssigt tog retten højde for det delte ansvar. Og i **H-94-08** gjorde Saab gældende, at FMT ikke havde leveret de kontraktkrævede *Operational Scenarios*, hvilket indgik i rettens samlede vurdering af, at ansvaret for testens ufuldstændighed ikke alene lå hos leverandøren.

Endelig kan kunden ikke hæve på et faktuel grundlag, som ikke er forelagt leverandøren. I **BS-43688/2021-SON** havde Haderslev Kommune ophævet en driftskontrakt med øjeblikkelig virkning på grundlag af en dataanalyse af registreringsmønstre i fagsystemet KMD Nexus. Retten fandt, at kommunen ikke havde godtgjort væsentlig misligholdelse, netop fordi analysen hverken var forelagt leverandøren eller fulgt op med konkrete undersøgelser – kommunen blev dømt til at betale 771.560 kr. for udført arbejde. Dommen er et konkret udslag af den loyale samarbejdspligt: systemgenererede indikationer skal konfronteres med modparten, før de kan bære en ophævelse.

LOV	Købeloven § 76, stk. 1	
PRAKSIS	Sø- og Handelsretten · Sag om uberettiget ophævelse af IT-kontrakt vedrørende Forsvarets DACCIS-system	10.09.2010
	Sø- og Handelsretten · Mangelfuld undervisning i regnskabsprogram – Egen skyld medfører bortfald af erstatningsansvar	21.06.2007

Byretten · Sag om uberettiget ophævelse af kontrakt om hjemmepleje

16.01.2023

Byretten · Sag om honorar for hjemmesideudvikling

07.02.2011

§ 6 Ophævelse: væsentlighedstærsklen og spørgsmålet om delvis ophævelse

Ophævelse forudsætter væsentlig misligholdelse, og i it-projekter er tærsklen høj, fordi projekterne er langvarige, gensidigt afhængige og typisk har passeret betydelige investeringer på begge sider.

Praksis viser tre typiske grundlag, som holder:

Grundlag	Illustrerende afgørelse	Udfald
Kontraktuelt fastsat tidsoverskridelse	H-23-05 (art. 26.1.c, over 4 måneder)	Ophævelse berettiget
Væsentlige mangler efter afhjælpningsfrist	H-23-05 (art. 26.1.e, skrivelse af 9. marts 2004)	Ophævelse berettiget
Manglende dokumenteret leverance af løbende ydelse	BS-46631/2023-OLR	Ophævelse berettiget, fuld tilbagebetaling

Og tre, som ikke holder: ophævelse på en fremdriftsprøve med vejledende fejlgrænser (**H-94-08**), ophævelse på uafklarede systemgenererede indikationer (**BS-43688/2021-SON**), og ophævelse på en misligholdelse, der ikke er væsentlig i det konkrete aftaleforhold – jf. **H-34-04**, hvor Telelet A/S' ophævelse af otte aftaler om levering af internetforbindelser var uberettiget, fordi det ikke var godtgjort, at leverandøren faktisk sendte ulovligt på de relevante frekvenser, og fordi Telelet ikke havde undersøgt leverandørens muligheder for fortsat levering. Til sammenligning var ophævelse berettiget i **BS-8688/2022-SHR**, hvor en samarbejdspartners betalingsstop over for branchens leverandører skadede modpartens omdømme i en tillidsbaseret branche – et eksempel på, at også ikke-økonomiske følgevirkninger kan bære væsentlighedsvurderingen.

Delvis ophævelse. Et selvstændigt og undervurderet spørgsmål er, om kunden kan hæve en enkelt del af aftalen – fx brugsretten til et fællesudviklet it-system – uden at hæve hele kontrakten. Det spørgsmål besvarede Sø- og Handelsretten benægtende i **BS-51216/2022-SHR m.fl.** af 7. februar 2025 mellem Dansk Boligforsikring A/S og WIA I/S. Samarbejdsaftalens pkt. 3.2 og 3.5 gav parterne lige rettigheder til det fælles it-system og ret til ved ophør at udtage en selvstændig licens til fortsat brug; pkt. 6.2 gav ret til at ophæve kontrakten ved væsentlig misligholdelse efter 30 dages varsel. Da DBF ophævede WIA's brugsret til systemet under henvisning til WIA's misligholdelse, afviste retten dette:

Retten afviste dette, da samarbejdsaftalen kun tillod ophævelse af hele kontrakten ved væsentlig misligholdelse, jf. pkt. 6.2. En delvis ophævelse af enkelte rettigheder var ikke hjemlet og ville forrykke aftalens forudsætninger urimeligt.

Afgørelsen har betydelig praktisk rækkevidde: i fælles udviklings- og platformssamarbejder skal adgangen til at hæve delvist – eller til at suspendere enkeltrettigheder – skrives udtrykkeligt ind i aftalen. Statens standardkontrakt løser problemet i den modsatte retning ved udtrykkeligt at give kunden ret til at »hæve kontrakten helt eller delvis efter kundens valg«, jf. [vejledningens punkt 15.2](#), og ved i faseopdelte leverancer at anbefale, at kunden kan påberåbe sig retsvirkningerne »helt eller delvist i forbindelse med hver enkelt fase«.

LOV

Købeloven § 21, stk. 1

Købeloven § 78b, stk. 2

PRAKSIS

Landsretten · Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse	18.03.2025
Sø- og Handelsretten · Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikringsamarbejde	07.02.2025
Sø- og Handelsretten · Berettiget ophævelse af konsulentaftale grundet skade på omdømme i bunker trader-branchen	22.02.2024
Sø- og Handelsretten · Sag om uberettiget ophævelse af IT-kontrakt vedrørende Forsvarets DACCIS-system	10.09.2010
Sø- og Handelsretten · Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler	01.12.2008
Sø- og Handelsretten · Sag om berettigelsen af ophævelse af aftaler om levering af internetforbindelser grundet påstået misligholdelse	20.12.2006
Byretten · Sag om uberettiget ophævelse af kontrakt om hjemmepleje	16.01.2023

§ 7 Afhjælpning og omlevering før afslag og ophævelse

Både standardkontrakterne og købelovens systematik bygger på et trinvist beføjelsessystem: afhjælpning eller omlevering først, derefter forholdsmæssigt afslag eller ophævelse.

Statens standardkontrakt fastsætter en meget konkret afhjælpningspligt: leverandøren skal i garantiperioden afhjælpe mangler »uden ugrundet ophold efter modtagelse af reklamation [...] i overensstemmelse med god leverandørskik«, og afhjælpning af programmelmangler omfatter udtrykkeligt tre elementer – [identifikation af fejlen, anvisning til kunden om mulighed for omgåelse af fejlen, således at driften forstyrres mindst muligt, samt rettelse af fejlen uden ugrundet ophold](#). Kontrakten indeholder tillige en fejlfrekvensregel: overstiger antallet af driftsforstyrrelser pr. måned pr. enhed en fastsat grænse, kan kunden kræve enheden udskiftet inden 10 arbejdsdage.

I forbrugerkøb er trinfølgen lovfæstet. Efter [købelovens § 78 a, stk. 4](#) skal afhjælpning eller omlevering ske gratis, inden for rimelig tid fra underretningen om manglen og uden væsentlig ulempe for køberen – og for digitalt indhold og digitale tjenester er det efter [§ 78 a, stk. 2](#) sælgeren, der vælger mellem afhjælpning og omlevering. Først derefter indtræder retten til afslag eller ophævelse efter [købelovens § 78 b, stk. 1](#), som opregner fire adgange: manglende eller mangelfuld afhjælpning, fortsat mangelfuldhed trods forsøg, mangler af »så alvorlig karakter«, at omgående afslag eller ophævelse er berettiget, og tilkendegivelse fra sælgeren om, at afhjælpning ikke vil ske inden for rimelig tid. Systemet svarer til [artikel 14 i direktiv \(EU\) 2019/770](#).

Forbrugerklagenævnets praksis er streng over for leverandører, der trækker afhjælpningen. I **18/11728** om en iPhone 8 Plus, hvor synkronisering af billeder konsekvent gik i stå, konstaterede den sagkyndige, at »den konstaterede fejl skyldes en materiale- eller fabrikationsfejl i telefonens software«. Selskabet henviste til, at fejlen ville blive udbedret i en kommende softwareopdatering, men nævnet fandt efter flere måneders forløb, at afhjælpning ikke var tilbudt inden for rimelig tid, og gav forbrugeren ret til at hæve købet. Tilsvarende i **13/12569**, hvor et tilbud om undersøgelse betinget af, at forbrugeren accepterede at betale for en eventuel reparation, ikke blev anset for »et korrekt tilbud om vederlagsfri afhjælpning«, og i **2006-4051/7-849**, hvor gentagelse af den samme softwarefejl efter én afhjælpning, kombineret med to måneders svartid, berettigede ophævelse af både telefonkøbet og det accessoriske abonnement.

I erhvervsforhold gælder de samme grundtanker uden lovfæstelse. **H-23-05** illustrerer, at en afhjælpningsfrist ikke behøver være lang, når forløbet i forvejen har været langtrukket:

Ved skrivelse af 9. marts 2004 havde Bombardier givet Bonansea en frist til at opfylde sine forpligtelser, hvilken frist der efter det forudgående forløb må anses for tilstrækkelig, da Bombardier flere gange har gjort opmærksom på såvel forsinkelserne som manglerne.

LOV	Købeloven § 78a, stk. 2, 4	Købeloven § 78b, stk. 1	
PRAKSIS	Sø- og Handelsretten · Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler		01.12.2008
	Forbrugerklagenævnet · Ophævelse af køb af iPhone 8 Plus efter manglende afhjælpning af softwarefejl		04.12.2018
	Forbrugerklagenævnet · Manglende skrue og defekt gevind i computer – spørgsmål om berettigelse til ophævelse af køb og fradrag for brug		07.10.2014
	Forbrugerklagenævnet · Ophævelse af køb af mobiltelefon og abonnement grundet mangel		17.10.2006

§ 8 Erstatningsopgørelsen: negativ og positiv kontraktinteresse, dagbod og påregnelighed

Erstatningsspørgsmålet i it-sager afgøres i praksis oftere på bevis end på jus. Mønsteret er, at retten anerkender ansvarsgrundlaget, men skærer kravet drastisk ned.

Negativ kontraktinteresse ved uberettiget ophævelse. I **H-94-08** opgjorde Saab sit tab som negativ kontraktinteresse – de omkostninger, der var afholdt i tillid til kontrakten. Retten accepterede opgørelsen fuldt ud, netop fordi den var underbygget:

Saab har nøje redegjort for, hvorledes de enkelte beløb er fremkommet ved udtræk fra selskabets bogføring. [...] Retten finder, at der efter forklaringerne ikke er grundlag for skønsmæssigt at nedsætte det krævede beløb.

Retten afviste endda at udskille omkostningerne til selve kontraktforhandlingerne, da disse ikke ville være afholdt uden kontrakten.

Bod og erstatning kan kumuleres. I **H-23-05** fastslog Sø- og Handelsretten, at kontraktens art. 22.1.1 ikke udelukkede, at der kunne kræves både bod og erstatning, og tilkendte boden på 229.774 € fuldt ud. Erstatningskravet gik det derimod anderledes med: af 1.117.581 € i ekstra lønudgifter blev der tilkendt 250.000 € skønsmæssigt, fordi indlæringskurven var behæftet med usikkerhed, og det ikke var godtgjort, at hele merudgiften skyldtes leverandøren. Krav på glasskillevægge, transportkasser og rejseomkostninger blev afvist som udokumenterede. Netop denne dom er også relevant for påregneligheden af følgeskader, jf. [købelovens § 25](#), der ved ophævelse i mangel af bevis for anden skade fastsætter erstatningen til prisforskellen, subsidiært til den ved et forsvarligt og rettidigt dækningskøb opnåede pris.

Skønsmæssig nedsættelse er hovedreglen ved udokumenterede tab. Det klareste eksempel er **BS-51216/2022-SHR m.fl.**, hvor Dansk Boligforsikring krævede 49,6 mio. kr. i erstatning for uberettiget brug af brugerdata og misligholdelse af aftalens ophørsbestemmelser. Retten fandt ansvarsgrundlaget opfyldt, men fandt tabet »langt fra dokumenteret« – bl.a. manglede konkrete tal for tilbudsforespørgsler, og den anvendte combined ratio var ikke retvisende – og fastsatte erstatningen skønsmæssigt til 3.000.000 kr., dvs. ca. 6 % af det påstævnte.

Tabsbegrænsningspligt og fradrag for opnået forbedring. I **P-0012-00** om sletning af data i konkursramte selskabers edb-system nedsatte Sø- og Handelsretten erstatningen for genopretningsudgifter fra ca. 234.000

kr. til 180.000 kr., fordi boet ved genopretningen opnåede en væsentlig forbedring af det i forvejen mangelfulde bogholderi. Samme princip om tabsbegrænsning styrede Højesterets udmåling af driftstab i **BS-225/2006-HJR**, hvor en uberettiget ophævelse af en forhandlerkontrakt udløste 7,8 mio. kr. i driftstab, men hvor krav om goodwill blev afvist, og hvor forhandlerens tabsbegrænsningspligt i opsigelsesperioden indgik i udmålingen.

Positiv opfyldelsesinteresse. I det udbudsretlige spor kan tabt fortjeneste tilkendes. I **20/05568** tilkendte Klagenævnet for Udbud Eksponent ApS erstatning i form af positiv opfyldelsesinteresse efter Gentofte Kommunes ulovlige tildeling af en it-kontrakt, men nedsatte kravet fra 2.233.670 kr. til skønsmæssigt 1.200.000 kr. under hensyn til usikkerheden ved indtægter og udgifter over en seksårig kontraktperiode.

LOV	KøbeLoven § 25	
PRAKSIS	Højesteret · Højesterets dom om uberettiget ophævelse af forhandlerkontrakt og erstatning for driftstab	24.10.2008
	Sø- og Handelsretten · Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikrings samarbejde	07.02.2025
	Sø- og Handelsretten · Sag om uberettiget ophævelse af IT-kontrakt vedrørende Forsvarets DACCIS-system	10.09.2010
	Sø- og Handelsretten · Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler	01.12.2008
	Sø- og Handelsretten · Erstatningsansvar for IT-hærværk og sletning af data i konkursramte virksomheder	17.02.2003
	Klagenævnet for Udbud · Erstatning for tabt fortjeneste efter ulovlig tildeling af kontrakt	10.02.2021

§ 9 Ansvarsbegrænsning, konventionalbod og rimelighedscensur efter aftaleloven § 36

It-kontrakter indeholder næsten uden undtagelse beløbscaps og fraskrivelse af indirekte tab og driftstab. Praksis viser, at sådanne klausuler som udgangspunkt respekteres mellem professionelle parter, men har to markante grænser.

Grænse 1 – misligholdelse uden for kontraktens rammer. I **BS-51216/2022-SHR m.fl.** indeholdt samarbejdsaftalens pkt. 6.4 en klassisk begrænsning: kun dokumenteret direkte tab kunne kræves, og kun ved grov uagtsomhed eller forsæt; indirekte tab var udelukket. Sø- og Handelsretten fandt bestemmelsen uanvendelig, fordi overtrædelserne »gik ud over kontraktens rammer og tillige indebar lovovertrædelser« – konkret uberettiget brug af den anden parts brugerdata i strid med [lov om forretningshemmeligheder § 4, stk. 2](#) og [markedsføringslovens § 3](#). Ansvarsbegrænsninger dækker med andre ord den kontraktuelle risiko, ikke retsstridige handlinger, der ligger uden for den.

Grænse 2 – rimelighedscensur efter [aftalelovens § 36](#). Bestemmelsen giver adgang til at ændre eller tilsidesætte en aftale helt eller delvis, hvis det vil være urimeligt eller i strid med redelig handlemåde at gøre den gældende, under hensyn til forholdene ved aftalens indgåelse, aftalens indhold og senere indtrufne omstændigheder. Efter forarbejderne bygger bestemmelsen på redegørelsen fra Justitsministeriets sagkyndige vedrørende formuerettens generalklausuler, professor, dr.jur. Stig Jørgensen.

I it-relaterede sager anvendes § 36 i praksis mest på konventionalbod og på finansieringsaftaler, ikke på selve ansvarsbegrænsningen:

- I **H-66-05** mellem WM-data Danmark A/S og Neoprocess A/S om overtrædelse af et ansættelsesforbud i en it-konsulentrammeaftale nedsatte flertallet konventionalbøden fra 750.000 kr. pr. overtrædelse til 250.000 kr. i medfør af [aftalelovens § 36](#).
- I Højesterets dom i **Sag 109/2011** blev en leasingtagers forpligtelser under en leasingaftale om en farveprinter halveret efter § 36 på grund af et ekstremt misforhold mellem ydelsen og udstyrets værdi kombineret med mellemmandens ulovlige salgsmetoder.

Omvendt er tærsklen høj mellem erhvervsdrivende. I **BS-46631/2023-OLR** afviste Østre Landsret at tilsidesætte en abonnementsaftale om annoncering, selv om leverandøren ikke havde leveret:

Der findes ikke tilstrækkelig grundlag for at anse det for urimelig eller i strid med redelig handlemåde at gøre aftalen gældende over for Virksomheden og dermed at tilsidesætte aftalen helt eller delvist i medfør af aftalelovens § 36. Landsretten har herved lagt vægt på, at aftalen ubestridt er indgået mellem to erhvervsdrivende.

Sagen blev i stedet afgjort på misligholdelsesgrundlaget. Samme resultat i **BS-24164/2023-OLR**, hvor Østre Landsret afviste at tilsidesætte to finansielle leasingaftaler om udstyr efter § 36.

Standardkontrakternes betydning ved § 36-vurderingen er velbeskrevet i [betænkning nr. 1480/2006 om revision af ophavsretslovens kapitel 3](#), som netop fremhæver, at kompleksiteten »præger også f.eks. it-kontrakt- og entrepriseretten«, og at eksistensen og indholdet af standardkontrakter på et område er af væsentlig betydning for domstolens bedømmelse, idet »afvigelser kan, hvis de er urimelige, tilsidesættes efter aftalelovens § 36«. På it-området peger dette på, at markante afvigelser fra statens standardkontrakter eller branchens almindelige betingelser til den ene parts fordel har en forhøjet censurrisiko.

LOV	Aftaleloven § 36, stk. 1-2	Markedsføringsloven § 3
PRAKSIS		
	Højesteret · Nedsættelse af leasingydelser efter aftalelovens § 36 grundet ekstremt misforhold mellem ydelse og værdi	12.04.2013
	Landsretten · Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse	18.03.2025
	Landsretten · Landsret stadfæster krav mod sagsøgte for misligholdelse af leasingaftaler og afviser tilsidesættelse efter Aftaleloven	21.02.2025
	Sø- og Handelsretten · Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikringsamarbejde	07.02.2025
	Sø- og Handelsretten · Overtrædelse af ansættelsesforbud i IT-konsulentbranchen efter virksomhedsoverdragelse	28.07.2006

§ 10 Rettigheder til udviklet software: ophavsret, brugsret og kildekode

Hvem der ejer det udviklede, er ofte den reelle kerne i en it-tvist – særligt ved samarbejdets ophør. Udgangspunktet er, at ophavsretten tilkommer ophavsmanden, og at overdragelse kræver aftale. Den vigtigste undtagelse er [ophavsretslovens § 59](#):

Ophavsretten til et edb-program, der er frembragt af en arbejdstager under udførelsen af dennes arbejde eller efter arbejdsgiverens anvisninger, overgår til arbejdsgiveren.

Bestemmelsen viderefører efter forarbejderne til 1995-loven den tidligere § 42 b, som blev indsat ved ændringslovene af 1989 og 1992.

Sø- og Handelsrettens dom i **BS-17826/2022-SHR** af 18. november 2024 om klokkespilsprogrammer er den mest detaljerede danske afgørelse om rækkevidden af § 59. Thubalka A/S havde gennem årtier betalt for udvikling af tre generationer af styringsprogrammet (DOS-programmet fra 1988/89, VB6-version 2009 og VB-version 2018) og påstod eneret til alle tre. Retten frifandt udvikleren på alle punkter og fastslog fire ting:

- **Betaling er ikke overdragelse.** Om DOS-programmet, som Thubalka havde betalt 120.650 kr. for og afskrevet som et aktiv, udtalte retten: »Retten finder dog, at det ikke giver fornødne sikre holdepunkter for, at det var ophavsrettighederne til programmet, som Jansson overdrog til Thubalka, og der er heller ikke i øvrigt sådanne holdepunkter.« Køberen havde erhvervet brugsret, ikke ophavsret.
- **Konvertering til nyt styresystem og programmeringssprog skaber et nyt værk** med selvstændig ophavsret.
- **Bevisbyrden efter § 59 påhviler arbejdsgiveren**, og den løftes ikke af, at programmøren var ansat: »Thubalka har ikke godtgjort, at Jørn Nielsen frembragte programmet VB6-version 2009 under udførelsen af sit arbejde for Thubalka eller efter Thubalkas anvisninger, hvorved bemærkes, at ideer til nye funktioner fra andre medarbejdere hos Thubalka ikke kan sidestilles med anvisninger.«
- **Vederlagsformen er et tungtvejende indicium.** Engangshonorarer, der ikke var ferieberettiget løn, og betalinger betegnet »aftalt ydelse« understøttede, at arbejdet ikke var udført som led i ansættelsen.

Billedet suppleres af **V 37/05** om softwareprogrammet MediBOX, hvor Sø- og Handelsretten fandt, at programmet var blevet til i et ligeværdigt samarbejde med fælles ophav, og at parternes adfærd viste en underforstået aftale om, at modparten kunne sælge programmet mod at betale for opdateringer – hvorfor udvikleren ikke ensidigt kunne indføre en royalty. Og af **V-9-15** om en GIS-applikation til ledningsregistrering, hvor rettighedshaverens krav var bortfaldet ved passivitet efter mere end syv års inaktivitet, selv om kopiering var dokumenteret ved syn og skøn.

Adgang til data og kildekode ved exit. Praksis om exit og transition er sparsom, men to afgørelser er retningsgivende. I **BS-2394/2024-SHR** nedlagde Sø- og Handelsretten midlertidigt forbud og påbud vedrørende softwareplatformen Bio+ og pålagde begge modparter at udlevere data, idet det var sandsynliggjort, at kunden havde rettighederne til de indtastede data og sammensætningen heraf – men afviste et krav om genaktivering af adgang som for uklart. I **BS-51216/2022-SHR m.fl.** var det fælles it-system reguleret ved en udtrykkelig licensret ved ophør, og netop den udtrykkelige regulering blev afgørende for, at brugsretten ikke kunne ophæves delvist.

At kildekoden i sig selv er et retligt følsomt aktiv, understreges af EU-Domstolens dom i **C-353/24**, hvor et nationalt krav om udlevering af softwarens kildekode til myndighedskontrol blev anset for en teknisk forskrift efter direktiv (EU) 2015/1535. Dommen angår ikke kontraktforhold, men illustrerer, at kildekodeadgang behandles som et selvstændigt reguleringsobjekt – hvilket taler for, at escrow- og deponeringsordninger reguleres udtrykkeligt i leverancekontrakten frem for at hvile på almindelige fortolkningsprincipper.

LOV

Ophavsretsloven § 1

Ophavsretsloven § 59

PRAKSIS

EU-Domstolen · Krav om udlevering af software-kildekode til skattekontrol udgør en teknisk forskrift i henhold til direktiv 2015/1535 18.12.2025

Sø- og Handelsretten · Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikringsamarbejde 07.02.2025

Sø- og Handelsretten · Sag om ophavsret til klokkespilsprogrammer – Udviklet før og under ansættelse 18.11.2024

Sø- og Handelsretten · Midlertidigt forbud vedrørende krænkelse af rettigheder til softwareplatform (Bio+)	17.04.2024
Sø- og Handelsretten · Tvist om ophavsret til GIS-applikation og tegnestandarder til ledningsregistrering	07.04.2017
Sø- og Handelsretten · Sag om ophavsret til softwareprogrammet MediBOX og krav om royalti	21.08.2007

It-as-a-service, abonnementer og leasing af udstyr: opsigelsesadgang ved løbende ydelser

Overgangen fra engangsleverance til abonnement flytter tyngdepunktet fra mangelsbeføjelser til opsigelses- og bindingsregler.

Den mest markante afgørelse er Østre Landsrets dom i **BS-4980/2023-OLR** af 8. oktober 2024, hvor Køge Svømmeklub havde leaset to ladestandere af Grenkeleasing ApS på en standardformular med fem års uopsigelighed. Landsretten fandt efter en samlet vurdering, at svømmeklubben var »en almenyttig forening uden kommercielle eller erhvervsmæssige interesser« og dermed forbruger – med henvisning til bevisbyrdereglen i [forbrugeraftalelovens § 2, stk. 2](#):

Grenkeleasing har ikke godtgjort, at svømmeklubben havde til hensigt at tjene penge på de to ladestandere.

Dermed fandt [forbrugeraftalelovens § 28](#) anvendelse, hvorefter forbrugeren kan opsig en aftale om løbende levering af varer eller tjenesteydelser med én måneds varsel, når der er gået fem måneder efter aftalens indgåelse, og hvor der efter [§ 28, stk. 5](#) ikke kan aftales et længere opsigelsesvarsel. Aftalens vilkår om femårig uopsigelighed var i direkte strid hermed, og standardformularen manglede tillige den oplysning om opsigelsesretten, som [§ 28, stk. 3](#) kræver. Landsretten anså aftalen for opsagt til udgangen af 2. kvartal 2020, frifandt klubben for kravet på 101.415,88 kr. og tilkendte tilbagebetaling af 170.054,11 kr. Særligt bemærkelsesværdigt er, at leverandøren blev pålagt en aktiv oplysningspligt: da klubben i december 2019 bad om at få aftalen sat i bero, havde Grenkeleasing »en særlig anledning til at oplyse om opsigelsesretten«, men gjorde det ikke.

Afgørelsen skal sammenholdes med **BS-24164/2023-OLR**, hvor en enkeltmandsvirksomhed ikke kunne påberåbe sig hverken omkvalifikation af leasingaftalen til leje/lån eller [aftalelovens § 36](#) – grænsen mellem forbruger og erhvervsdrivende er i praksis afgørende for udfaldet.

På leverancesiden er hovedreglen, at manglende dokumenteret levering af den løbende ydelse er væsentlig misligholdelse, jf. **BS-46631/2023-OLR**. Og i **H-27-04** frifandtes et moderselskab for et krav på 250.761,25 kr. for udført vedligeholdelse af edb-udstyr, fordi parterne efter bevisførelsen havde haft en fælles forståelse om, at aftalen var indgået med det (nu konkursramte) datterselskab – en påmindelse om, at rette kontraktpart i koncernstrukturerede driftsaftaler skal fastlægges udtrykkeligt.

Forbrugerombudsmandens praksis om abonnementsvilkår er relevant for SaaS-udbydere med forbrugerkunder. I **fom-108291** afgav en streamingtjeneste tilsagn efter at have henvist opsigende kunder til telefonisk kontakt; Forbrugerombudsmanden fandt praksissen i strid med reglerne om nem online opsigelse samt god markedsførings- og erhvervsskik. I **fom-80436** blev det indskærpet, at automatisk fornyelse af et abonnement med en ny bindingsperiode efter udløbet af den oprindelige uopsigelsesperiode ikke er tilladt. Og i **fom-90682** vurderede Forbrugerombudsmanden, at et vilkår, der gav udbyderen ubegrænset adgang til ensidigt at ændre aftalevilkårene, ikke opfyldte gennemsigtighedskravet i [aftalelovens § 38 b, stk. 2](#), og at det ville stride

mod § 38 c, jf. § 36, at gøre det gældende. Endelig fastslog Sø- og Handelsretten i **BS-52204/2023-SHR** af 13. januar 2026, at et frikøbsbeløb ved førtidig opsigelse af en løbende leveringsaftale ikke kunne opretholdes som standardiseret erstatning, men var et ulovligt skifterelateret gebyr – et princip med overførselsværdi til exit-gebyrer i abonnementsbaserede it-ydelser.

LOV	Aftaleloven § 36	Aftaleloven § 38b, stk. 2	Forbrugeraftaleloven § 2, stk. 2
	Forbrugeraftaleloven § 28, stk. 1, 3, 5		
PRAKSIS	Landsretten · Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse		18.03.2025
	Landsretten · Landsret stadfæster krav mod sagsøgte for misligholdelse af leasingaftaler og afviser tilsidesættelse efter Aftaleloven		21.02.2025
	Landsretten · Køge Svømmeklub vinder ankesag mod Grenkeleasing: Status som forbruger sikrede opsigelsesret		08.10.2024
	Sø- og Handelsretten · Dom om ulovlige gebyrer ved opsigelse af elaftaler - Forbrugerombudsmanden mod Velkommen A/S		13.01.2026
	Sø- og Handelsretten · Sag om kontraktforpligtelse: Nordic Computer A/S mod BCP A/S vedrørende vedligeholdelsesaftale		14.04.2005
	Forbrugerombudsmanden · Streamingtjeneste tilsidesatte krav om nem online opsigelse af abonnementer		19.12.2023
	Forbrugerombudsmanden · Manglende oplysning om dataindsamling og urimelige vilkår i løbehjulsudlejningsapps		18.10.2022
	Forbrugerombudsmanden · Automatisk fornyelse af abonnement med ny bindingsperiode er i strid med Forbrugeraftaleloven		13.02.2009

Den forbrugerretlige side: digitalt indhold og digitale tjenester i købeloven

Hvor den erhvervsrettede it-kontraktret er ulovbestemt, er forbrugersiden siden 1. januar 2022 detailreguleret. Ved **lov nr. 1173 af 8. juni 2021** om ændring af købeloven og markedsføringsloven blev [Europa-Parlamentets og Rådets direktiv \(EU\) 2019/771 om salg af varer](#) og [direktiv \(EU\) 2019/770 om levering af digitalt indhold og digitale tjenester](#) gennemført i dansk ret. Af lovforslagets almindelige bemærkninger fremgår baggrunden:

Justitsministeren nedsatte i foråret 2020 et udvalg [...] med henblik på, at udvalget skulle overveje og komme med anbefalinger til, hvordan bl.a. varedirektivet og direktivet om digitalt indhold mest hensigtsmæssigt bør gennemføres i dansk ret. [...] Udvalget afgav den 27. januar 2021 Delbetænkning I (nr. 1576/2021) om gennemførelse af varedirektivet og direktivet om digitalt indhold.

De centrale ændringer for it-området er fire.

1. Udvidet forbrugerkøbsbegreb. Efter [købelovens § 4 a, stk. 3](#) anses aftaler om levering af digitalt indhold eller en digital tjeneste for forbrugerkøb, når leveringen sker mod et pengebeløb, et digitalt udtryk for værdi eller mod personoplysninger. Definitionerne i [§ 3 a](#) omfatter bl.a. »digital tjeneste«, »vare med digitale elementer«, funktionalitet, holdbarhed, kompatibilitet, interoperabilitet og »digitalt miljø«. En række ydelser er udtrykkeligt undtaget efter [§ 4 a, stk. 4](#), herunder open source-software uden vederlag og finansielle tjenesteydelser. Af forarbejderne til den nyaffattede [§ 75 a](#) fremgår, at salgsgenstanden »kan være en fysisk løsøregenstand, men også digitalt indhold, fordringer eller rettigheder«, og at det »som noget nyt i forhold til gældende ret« også kan være en digital tjeneste.

2. Todelt mangelsbegreb. Forarbejderne beskriver systematikken direkte: [§ 75 b](#) angår »krav til salgsgenstanden, som følger af den konkrete aftale mellem køberen og sælgeren (subjektive krav)«, mens [§ 75 c](#) og [§ 75 d](#) angår »krav til salgsgenstanden, som følger af købeloven på grundlag af salgsgenstandens art og omstændighederne i øvrigt (objektive krav)«. De objektive krav kan kun fraviges ved en udtrykkelig aftale om specifikke egenskaber, jf. [§ 75 c, stk. 3](#).

3. Opdateringspligt. Efter [§ 75 b, nr. 4](#) skal salgsgenstanden »opdateres som fastsat i aftalen«. Direktiv 2019/770 præciserer i betragtning 44, at manglende opdateringer – og tillige »fejlbehæftede eller ufuldstændige opdateringer« – udgør manglende overensstemmelse.

4. Ændringer af løbende digitale ydelser. [Købelovens § 77 b](#) regulerer, hvornår sælgeren må ændre digitalt indhold eller en digital tjeneste, der leveres løbende, ud over hvad der er nødvendigt for at holde ydelsen mangelfri. Ændringen kræver bl.a. hjemmel og en gyldig grund i aftalen, at den sker uden yderligere omkostninger, og at køberen orienteres klart; har ændringen ikke-uvæsentlig negativ indvirkning, kan køberen efter [§ 77 b, stk. 2](#) ophæve købet gratis inden for 30 dage. Bestemmelsen er den direkte modvægt til SaaS-udbyderes ensidige ændringsklausuler og svarer til [artikel 19 i direktiv \(EU\) 2019/770](#).

Forbrugerklagenævnets ældre praksis er fortsat illustrativ for, hvordan mangelsvurderingen slår ud i it-forhold, selv om den hviler på de tidligere regler: **2002-4031/7-2150**, hvor manglende medfølgende installations-cd med styresystemet udgjorde en mangel, fordi det var normal praksis at levere en sådan; **01-09-6375**, hvor det ikke fremgik tilstrækkelig tydeligt af abonnementsbetingelserne, at opsigelse af abonnementet også afskar brug af satellitboksen til gratis kanaler, hvilket berettigede ophævelse; og **2002-4054-7-168**, hvor teleudbyderens manglende vejledning om nødvendig softwareinstallation ved skift fra ISDN til ADSL førte til nedsættelse af regningen efter [aftalelovens § 38 c](#), jf. [§ 36](#).

LOV	Købeloven § 3a	Købeloven § 4a, stk. 3-4	Købeloven § 75a	Købeloven § 75b
	Købeloven § 75c, stk. 3	Købeloven § 77b, stk. 1-2		
PRAKSIS	Forbrugerklagenævnet · Ophævelse af køb af iPhone 8 Plus efter manglende afhjælpning af softwarefejl			04.12.2018
	Forbrugerklagenævnet · Manglende skrue og defekt gevind i computer – spørgsmål om berettigelse til ophævelse af køb og fradrag for brug			07.10.2014
	Forbrugerklagenævnet · Mangelfuld oplysning ved køb af satellitboks og abonnement			28.10.2010
	Forbrugerklagenævnet · Manglende vejledning om softwareinstallation ved skift til ADSL-forbindelse			31.12.2003
	Forbrugerklagenævnet · Manglende installations-cd udgjorde en mangel			31.12.2002

Offentlige it-anskaffelser: standardkontrakter, kontraktændringer og grænsen til udbudsretten

En stor del af dansk it-leveranceret udspiller sig i offentlige projekter, hvor kontraktretten er indrammet af udbudsretten og af statens interne styringsregler.

Styringsrammen. Efter [cirkulære om Statens It-råd](#) omfatter reguleringen »statslige myndigheders udgifter til it-projekter, it-anskaffelser og til drift og vedligehold af it-systemer«, og cirkulæret uddyber Budgetvejledningens punkt 2.2.18. Ved it-projekter over de fastsatte beløbsgrænser kræves anvendelse af statens it-projektmodel samt risikovurdering i Statens It-råd. Denne styringsramme forklarer, hvorfor offentlige it-kontrakter typisk indeholder detaljerede milepæls-, prøve- og rapporteringsregimer – og dermed hvorfor tvisterne oftere handler om prøveresultater end om selve funktionsbeskrivelsen.

Ændringer i kontraktperioden. Klagenævnet for Udbud har i **20/00982** fastlagt en forholdsvis rummelig ramme for at håndtere it-forsinkelser inden for den eksisterende kontrakt. Region Hovedstaden kunne udskyde ibrugtagningssdagen for det nye vagtplanlægningssystem Optima og samtidig indgå tillæg om midlertidig videreførelse af det gamle system, uden at det udgjorde en ændring af et grundlæggende element efter [udbudslovens § 178](#) – nævnet lagde vægt på, at tillægget var nødvendigt og midlertidigt, ikke ændrede leverandørens grundlæggende forpligtelse og ikke rykkede kontraktens økonomiske balance. Grænsen går derimod ved lempelse af mindstekrav: i **21/10576** fandt nævnet, at et svar om, at tilbudsgiverne skulle »se bort fra krav om maling af master«, udgjorde en væsentlig ændring af et udtrykkeligt mindstekrav, og at bevisbyrden for det modsatte påhvilede ordregiveren.

Direkte tildeling ved leverandørbinding. I **21/10232** havde Det Digitale Folkebibliotek tildelt en kontrakt om udvikling af en basisplatform direkte til den eksisterende leverandør med henvisning til [udbudslovens § 80, stk. 3, nr. 2](#) om tekniske årsager. Klagenævnet fandt bevisbyrden uløftet – en konkurrent havde sandsynliggjort at besidde de nødvendige kompetencer – og annullerede tildelingsbeslutningen, men erklærede ikke kontrakten uden virkning, da profylaksebekendtgørelse og standstill var overholdt, og ordregiveren havde udvist fornøden omhu. Afgørelsen viser, at teknisk leverandørbinding i it-porteføljer sjældent i sig selv legitimerer direkte tildeling.

Transition og exit som konkurrenceparameter. I **2014-0038026** afviste Klagenævnet at tillægge en klage opsættende virkning, hvor en konkurrent gjorde gældende, at 90 arbejdsdage til transitionsfase T1 gav den eksisterende leverandør en utilbørlig fordel. Nævnet henviste til, at en ordregiver ikke er forpligtet til fuldstændigt at udligne alle fordele hos en eksisterende leverandør. Tilsvarende i **2014-8323**, hvor SKATs høje vægtning af transition (35 %) ikke blev anset for at favorisere den siddende leverandør, selv om nævnet kritiserede begrundelsen for tildelingen. Og i **2010-0022970** om Aarhus Kommunes it-løsning til Socialforvaltningen accepterede nævnet, at bod blev fastsat ensartet for alle tilbudsgivere, og at tidsplanen blev udskudt som følge af overgangen til udbud med forhandling – begge dele uden at udgøre væsentlige ændringer.

Leverandørskifte under kontrakten. I **23/06414** afviste Klagenævnet en klage over tildelingen af en syvårig kontrakt om drift og vedligehold af Forsvarets sags- og dokumenthåndteringssystem, selv om den vindende tilbudsgiver kort efter prækvalifikationen havde frasolgt sin it-infrastrukturforretning til et nyt selskab, der herefter optrådte som underleverandør. Afgørelsen har praktisk betydning for outsourcing- og carve-out-scenarier i lange driftskontrakter.

Endelig knytter sanktionssiden an til kontraktretten: i **20/05568** blev en ordregiver pålagt at betale positiv opfyldelsesinteresse efter en ulovlig tildeling af en it-kontrakt – dvs. samme tabsbegreb som ved uberettiget ophævelse i det kontraktretlige spor, men med skønsmæssig reduktion under hensyn til usikkerheden over en lang kontraktperiode.

LOV	Udbudsloven § 2	Udbudsloven § 80, stk. 3	Udbudsloven § 178
PRAKSIS	Klagenævnet for Udbud · Klage over tildeling af IT-driftskontrakt efter vindende tilbudsgivers omstrukturering afvist 24.01.2025 Klagenævnet for Udbud · Direkte tildeling af IT-kontrakt på grund af tekniske årsager var uberettiget, men kontrakten blev ikke erklæret uden virkning 21.06.2022 Klagenævnet for Udbud · Ændring af mindstekrav under udbudsproces førte til opsættende virkning 15.10.2021 Klagenævnet for Udbud · Erstatning for tabt fortjeneste efter ulovlig tildeling af kontrakt 10.02.2021 Klagenævnet for Udbud · Ændring af kontrakt om IT-system til vagtplanlægning udgjorde ikke en ulovlig direkte tildeling 23.06.2020 Klagenævnet for Udbud · Afvisning af tilbud og mangelfuld begrundelse i SKATs IT-udbud 23.06.2015 Klagenævnet for Udbud · Afslag på opsættende virkning i sag om IT-udbud grundet manglende bevis for utilbørlig fordel til eksisterende leverandør 13.08.2014 Klagenævnet for Udbud · Afvisning af klage over udbud af IT-løsning efter ændring af udbudsform 16.08.2011		

§ 14 Sammenfatning: de bærende mønstre i dansk it-leverancepraksis

På tværs af de offentligt tilgængelige afgørelser tegner der sig syv mønstre, som en rådgiver kan bygge på.

- 1. Kontrakten er næsten hele retskilden.** Uden speciallov afgøres sagerne af, hvad parterne har skrevet – og af, hvor præcist de har skrevet det. Både **H-94-08**, **H-23-05** og **BS-51216/2022-SHR m.fl.** blev afgjort på fortolkning af konkrete kontraktbestemmelser om prøver, fatale datoer og ophævelsesadgang, ikke på almindelige grundsætninger.
- 2. Prøvedesignet bestemmer misligholdelsesretten.** Om en milepælstest er en stop-test eller en fremdriftsprøve, om fejlgrænserne er bindende eller vejledende, og om fejlklassifikationen skal ske i fællesskab, afgør reelt, om kunden kan hæve. Statens standardkontrakts model med en funktionsbaseret [overtagelsesprøve](#) efterfulgt af en måleorienteret [driftsprøve](#) og en objektiv 30-dages ophævelsestærskel er stadig den mest gennemarbejdede danske skabelon.
- 3. Væsentlighedstærsklen er høj, og bevisbyrden ligger hos den, der hæver.** Kunden skal godtgøre både misligholdelsens omfang og dens væsentlighed. Uklarhed, som kunden selv har bidraget til, tæller ikke med.
- 4. Delvis ophævelse skal aftales.** Er hæveadgangen formuleret som en ret til at ophæve kontrakten, kan enkeltrettigheder – brugsret, licens, adgang til data – ikke ophæves isoleret, jf. **BS-51216/2022-SHR m.fl.**
- 5. Tabsopgørelsen er sagens reelle slagmark.** Dokumenteret negativ kontraktinteresse gennemføres fuldt ud (**H-94-08**: 31,9 mio. kr.), mens skønspregede tabsberegninger skæres ned til en brøkdel (**BS-51216/2022-SHR m.fl.**: 3 mio. kr. af 49,6 mio. kr.; **H-23-05**: 250.000 € af 1.117.581 €).
- 6. Ansvarsbegrænsninger holder mellem professionelle – indtil misligholdelsen forlader kontraktens rammer.** [Aftalelovens § 36](#) anvendes tilbageholdende mellem erhvervsdrivende (**BS-46631/2023-OLR**, **BS-24164/2023-OLR**), men bruges aktivt på konventionalbod (**H-66-05**) og på finansieringskonstruktioner med ekstremt misforhold (**Sag 109/2011**).

7. Rettigheder og exit skal reguleres udtrykkeligt. Ophavsretten følger ophavsmanden, medmindre [ophavsretslovens § 59](#) er opfyldt, og bevisbyrden derfor påhviler arbejds- eller hvervgiveren (- **BS-17826/2022-SHR**). Betaling giver brugsret, ikke ejendomsret. Adgang til data og kildekode ved ophør skal fremgå af aftalen – også fordi selv velformulerede krav om genaktivering af adgang kan blive afvist som for uklare (**BS-2394/2024-SHR**).

Endelig gælder som praktisk forbehold, at de fleste store danske it-leverancetvister afgøres ved fortrolig voldgift. Den offentligt tilgængelige praksis er derfor ikke repræsentativ for områdets fulde volumen, og standardkontrakterne – statens K-kontrakter, kontrakten for agil softwareudvikling og branchens almindelige betingelser – udgør i praksis en selvstændig og tungtvejende fortolkningsfaktor, hvis afvigelser efter omstændighederne kan censureres efter [aftalelovens § 36](#).

LOV	Aftaleloven § 36	Ophavsretsloven § 59	
PRAKSIS	Højesteret · Nedsættelse af leasingydelser efter aftalelovens § 36 grundet ekstremt misforhold mellem ydelse og værdi		12.04.2013
	Landsretten · Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse		18.03.2025
	Landsretten · Landsret stadfæster krav mod sagsøgte for misligholdelse af leasingaftaler og afviser tilsidesættelse efter Aftaleloven		21.02.2025
	Sø- og Handelsretten · Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikringssamarbejde		07.02.2025
	Sø- og Handelsretten · Sag om ophavsret til klokkespilsprogrammer – Udviklet før og under ansættelse		18.11.2024
	Sø- og Handelsretten · Midlertidigt forbud vedrørende krænkelse af rettigheder til softwareplatform (Bio+)		17.04.2024
	Sø- og Handelsretten · Sag om uberettiget ophævelse af IT-kontrakt vedrørende Forsvarets DACCIS-system		10.09.2010
	Sø- og Handelsretten · Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler		01.12.2008
	Sø- og Handelsretten · Overtrædelse af ansættelsesforbud i IT-konsulentbranchen efter virksomhedsoverdragelse		28.07.2006

REFERENCE Lovgrundlag 8 paragraffer

Aftaleloven § 36	stk. 1-2	Forbrugeraftaleloven § 28	stk. 1
Købeloven § 4a	stk. 3	Købeloven § 21	stk. 1-3
Købeloven § 25		Købeloven § 75b	
Købeloven § 78b	stk. 1-2	Ophavsretsloven § 59	

MATERIALE Citerede afgørelser 41 afgørelser

HØJESTERET · ØVERSTE INSTANS		2
12.04.2013	Nedsættelse af leasingydelser efter aftalelovens § 36 grundet ekstremt misforhold mellem ydelse og værdi	109-2011

24.10.2008	Højesterets dom om uberettiget ophævelse af forhandlerkontrakt og erstatning for driftstab	4845-5840
------------	--	-----------

EU-DOMSTOLEN · EUROPÆISK DOMSTOL	1
----------------------------------	---

18.12.2025	Krav om udlevering af software-kildekode til skattekontrol udgør en teknisk forskrift i henhold til direktiv 2015/1535	C-353/24
------------	--	----------

LANDSRETTE · ANKEINSTANS	3
--------------------------	---

18.03.2025	Virksomhed frifundet for betaling for social media-abonnement på grund af leverandørens væsentlige misligholdelse	9809-11467
------------	---	------------

21.02.2025	Landsret stadfæster krav mod sagsøgte for misligholdelse af leasingaftaler og afviser tilsidesættelse efter Aftaleloven	10244-12026
------------	---	-------------

08.10.2024	Køge Svømmeklub vinder ankesag mod Grenkeleasing: Status som forbruger sikrede opsigelsesret	9512-11078
------------	--	------------

SØ- OG HANDELSRETTE · SPECIALRET	16
----------------------------------	----

13.01.2026	Dom om ulovlige gebyrer ved opsigelse af elaftaler - Forbrugerombudsmanden mod Velkommen A/S	
------------	--	--

10.04.2025	Afvisning af midlertidigt forbud og påbud i softwarekonflikt grundet upræcise påstande	BS-55788/2024-SHR
------------	--	-------------------

07.02.2025	Strid om brugerdata og IT-rettigheder efter ophør af mangeårigt forsikringssamarbejde	BS-51216/2022-SHR, BS-51220/2022-SHR, BS-51218/2022-SHR, BS-26811/2023-SHR
------------	---	---

18.11.2024	Sag om ophavsret til klokkespilsprogrammer – Udviklet før og under ansættelse	BS-17826/2022-SHR
------------	---	-------------------

17.04.2024	Midlertidigt forbud vedrørende krænkelse af rettigheder til softwareplatform (Bio+)	BS-2394/2024-SHR
------------	---	------------------

22.02.2024	Berettiget ophævelse af konsulentaftale grundet skade på omdømme i bunker trader-branchen	BS-8688/2022-SHR
------------	---	------------------

06.10.2023	Sag om midlertidigt forbud og påbud vedrørende overtrædelse af lov om forretningshemmeligheder og markedsføringsloven i forbindelse med salg og markedsføring af service- og vedligeholdelsesaftaler for software.	BS-21360/2022-SHR
------------	--	-------------------

07.04.2017	Tvist om ophavsret til GIS-applikation og tegnestandarder til ledningsregistrering	V-9-15
------------	--	--------

10.09.2010	Sag om uberettiget ophævelse af IT-kontrakt vedrørende Forsvarets DACCIS-system	H-94-08
------------	---	---------

01.12.2008	Sag om ophævelse af kontrakt om levering af interiør til tog på grund af forsinkelse og mangler	H-23-05
------------	---	---------

21.08.2007	Sag om ophavsret til softwareprogrammet MediBOX og krav om royalty	V 37/05
------------	--	---------

21.06.2007	Mangelfuld undervisning i regnskabsprogram – Egen skyld medfører bortfald af erstatningsansvar	H-112-05
------------	--	----------

20.12.2006	Sag om berettigelsen af ophævelse af aftaler om levering af internetforbindelser grundet påstået misligholdelse	H-34-04
------------	---	---------

28.07.2006	Overtrædelse af ansættelsesforbud i IT-konsulentbranchen efter virksomhedsoverdragelse	H-66-05
14.04.2005	Sag om kontraktforpligtelse: Nordic Computer A/S mod BCP A/S vedrørende vedligeholdelsesaftale	H-27-04
17.02.2003	Erstatningsansvar for IT-hærværk og sletning af data i konkursramte virksomheder	P-0012-00
BYRET TEN · FØRSTE INSTANS		2
16.01.2023	Sag om uberettiget ophævelse af kontrakt om hjemmepleje	5605-6705
07.02.2011	Sag om honorar for hjemmesideudvikling	3436-4095
KLAGENÆVNET FOR UDBUD · NÆVN / KLAGEINSTANS		8
24.01.2025	Klage over tildeling af IT-driftskontrakt efter vindende tilbudsgivers omstrukturering afvist	23/06414
21.06.2022	Direkte tildeling af IT-kontrakt på grund af tekniske årsager var uberettiget, men kontrakten blev ikke erklæret uden virkning	21/10232
15.10.2021	Ændring af mindstekrav under udbudsproces førte til opsættende virkning	21/10576
10.02.2021	Erstatning for tabt fortjeneste efter ulovlig tildeling af kontrakt	20/05568
23.06.2020	Ændring af kontrakt om IT-system til vagtplanlægning udgjorde ikke en ulovlig direkte tildeling	20/00982
23.06.2015	Afvisning af tilbud og mangelfuld begrundelse i SKATs IT-udbud	2014-8323
13.08.2014	Afslag på opsættende virkning i sag om IT-udbud grundet manglende bevis for utilbørlig fordel til eksisterende leverandør	2014-0038026
16.08.2011	Afvisning af klage over udbud af IT-løsning efter ændring af udbudsform	2010-0022970
FORBRUGERKLAGENÆVNET · NÆVN / KLAGEINSTANS		6
04.12.2018	Ophævelse af køb af iPhone 8 Plus efter manglende afhjælpning af softwarefejl	18/11728
07.10.2014	Manglende skrue og defekt gevind i computer – spørgsmål om berettigelse til ophævelse af køb og fradrag for brug	13/12569
28.10.2010	Mangelfuld oplysning ved køb af satellitboks og abonnement	01-09-6375
17.10.2006	Ophævelse af køb af mobiltelefon og abonnement grundet mangel	2006-4051/7-849
31.12.2003	Manglende vejledning om softwareinstallation ved skift til ADSL-forbindelse	2002-4054-7-168
31.12.2002	Manglende installations-cd udgjorde en mangel	2002-4031/7-2150
FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS		3
19.12.2023	Streamingtjeneste tilsidesatte krav om nem online opsigelse af abonnementer	
18.10.2022	Manglende oplysning om dataindsamling og urimelige vilkår i løbehjulsudlejningsapps	

13.02.2009 · Automatisk fornyelse af abonnement med ny bindingsperiode er i strid med Forbrugeraftaleloven

FORARBEJDE Betænkninger

3 referencer

Udlicitering af offentlige drifts- og anlægsopgaver

nr. 1227 · 1991 · Finansministeriet

Betænkning om revision af ophavsretslovens kapitel 3

nr. 1480 · 2006 · Kulturministeriet

Delbetænkning IV fra EDB-Samordningsudvalget om forvaltningens konsulent- og planlægningsfunktioner samt edb-efteruddannelse og om samarbejde mellem Datacentralen og Kommunedata

nr. 867 · 1979 · Finansministeriet

11

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over MitID / NemID-misbrug og digital identitetstyveri

Strafferetlig kvalificering, strafudmåling og ofrets hæftelse ved misbrug af digital identitet

Version 2 · Opdateret 24. jun. 2026 · 34 afgørelser · 2016-2026

[Læs online](#)

INTRODUKTION

Misbrug af MitID og NemID udgør en central og voksende del af dansk berigelseskriminalitet. Gerningsindholdet spænder fra uberettiget lånoptagelse i andres navn via databedrageri (straffeloven § 279 a) over dokumentfalsk med elektroniske dokumenter (§ 171) til selvstændigt identitetsmisbrug (§ 264 e). Parallelt hermed rejser misbruget civile retlige spørgsmål om ofrets hæftelse over for sin bank efter betalingslovens § 100, hvor Finansielle Ankenævn har udviklet en konsekvent – men omstridt – praksis for vurderingen af "groft uforsvarlig adfærd" ved social engineering. Praksisoversigten gennemgår den strafferetlige kvalificering, strafudmålingsniveauerne og den civile retlige ansvarsfordeling, som den tegner sig i domspraksis og nævnsafgørelser.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Uberettiget lånoptagelse via en andens NemID/MitID kvalificeres som databedrageri efter straffeloven § 279 a – ikke som simpelt bedrageri efter § 279 – fordi den tabsforvoldende disposition (lånudbetaling) sker ved automatiseret databehandling.
- 02 Brug af en andens NemID/MitID til at underskrive en digital låneaftale kan samtidig udgøre dokumentfalsk efter straffeloven § 171, idet et elektronisk dokument forsynet med en digital signatur opfylder dokumentbegrebet i § 171, stk. 2.
- 03 Identitetsmisbrug efter straffeloven § 264 e straffes i sammenstød med bedrageri og databedrageri; bestemmelsen kræver ikke et berigelsesformål og rammer dermed tilfælde, der falder uden for formueforbrydelserne.
- 04 Strafudmålingen ved systematisk NemID/MitID-lånebedrageri afhænger især af det samlede beløb, antallet af forhold og gerningsperiodens længde: 24 forhold for over 400.000 kr. udmåles typisk til 1 års fængsel, mens beløb over 1 mio. kr. medfører fængsel i 2 år eller mere.
- 05 Overlader en person sit NemID/MitID til tredjemand mod betaling i bevidstheden om, at det bruges til lånoptagelse, dømmes vedkommende for medvirken til hvidvask (§ 290 a) – ikke for selve databedrageriet.

- 06** Ved 'muldyr'-sager (bankkonto stillet til rådighed) er forsætsvurderingen central: retten finder typisk acceptforsæt opfyldt, når kontohaveren ikke reagerer på advarsler eller umiddelbart hæver og videregiver indbetalte beløb.
- 07** Betalingslovens § 100 fordeler hæftelsen ved uautoriserede transaktioner i en trappestige: 375 kr. (stk. 3) ved simpel brug af sikkerhedsforanstaltning, op til 8.000 kr. (stk. 4, nr. 3) ved groft uforsvarlig adfærd, og ubegrænset (stk. 5) ved forsætlig videregivelse med indsigt i misbrugsrisiko.
- 08** Finansielle Ankenævn finder konsekvent med 3-2 flertal, at godkendelse af en MitID-handling med tekst om profilændring eller betaling – som kunden burde have læst – udgør 'groft uforsvarlig adfærd' efter betalingslovens § 100, stk. 4, nr. 3, med en selvrisko på 8.000 kr.
- 09** Mindretallet i Finansielle Ankenævn argumenterer lige så konsekvent for, at professionel og organiseret svindel ikke bør føre til, at forbrugeren kvalificeres som groft uforsvarlig – og at banken bærer systemrisikoen.
- 10** Udbyderen (banken) hæfter uanset kundens adfærd, hvis udbyderen ikke har krævet stærk kundeautentifikation, medmindre kunden har handlet svigagtigt, jf. betalingslovens § 100, stk. 7.
- 11** Betalingslovens § 100, stk. 8, fritager kunden helt for hæftelse, hvis tabet, tyveriet eller den uberettigede tilegnelse af sikkerhedsforanstaltningen ikke kunne opdages forud for misbruget.
- 12** Østre Landsret har i en fogsagsag nægtet at fremme tvangsfuldbyrdelse af et NemID-baseret lån, hvor låntageren var franarret sine NemID-oplysninger af en bedrager – den aftaleretlige forpligtelse beror på en konkret helhedsvurdering af hændelsesforløbet, jf. U.2019.1192H og U.2019.1197H.
- 13** Overførsler foretaget af kunden selv under social engineering (vishing) er autoriserede betalingstransaktioner, som falder uden for betalingslovens § 100 – kunden bærer det fulde tab.
- 14** Rigsadvokatmeddelelsen om freds- og ærekrænkelser fastsætter udgangspunktet for strafpåstand ved identitetsmisbrug til en bøde på 10.000 kr. i førstegangstilfælde med en enkelt overtrædelse.

Strafferetlig kvalificering: Bedrageri, databedrageri og dokumentfalsk

§ 1

Misbrug af MitID/NemID til uberettigede transaktioner berører flere bestemmelser i straffeloven, og den korrekte kvalificering afhænger af, hvordan den tabsforvoldende disposition sker.

Bedrageri (straffeloven § 279) forudsætter, at gerningsmanden retsstridigt fremkalder, bestyrker eller udnytter en vildfarelse hos en *person*, som herved bestemmes til en handling, der medfører et formuetab. Bestemmelsen finder anvendelse, hvor en menneskelig beslutningstager – fx en bankrådgiver ved skranken – narres til at godkende en transaktion.

Databedrageri (straffeloven § 279 a) finder derimod anvendelse, hvor den tabsforvoldende disposition sker via automatiseret elektronisk databehandling. Bestemmelsen rammer den, der retsstridigt ændrer, tilføjer eller

sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt søger at påvirke resultatet af en sådan databehandling. Når en gerningsmand logger ind med en andens NemID/MitID på en online låneportal og ansøger om et kviklån, der automatisk godkendes og udbetales, foreligger databedrageri – ikke simpelt bedrageri – fordi vildfarelsen opstår i et datasystem, ikke hos en person.

Sondringen er illustreret i [S-2360-16](#), hvor Østre Landsret domfældte for både bedrageri (§ 279) for de personlige kontaktsituationer og databedrageri (§ 279 a) for de elektroniske kreditanmodninger, med et samlet beløb på ca. 1,3 mio. kr.

Dokumentfalsk (straffeloven § 171) kan foreligge sideløbende, når gerningsmanden benytter en andens digitale signatur til at underskrive en låneaftale eller kontrakt. Bestemmelsens dokumentbegreb omfatter udtrykkeligt elektroniske dokumenter forsynet med en betegnelse af udstederen ([straffeloven § 171, stk. 2](#)). Et digitalt underskrevet lånedokument opfylder dette krav, og dokumentet er falsk efter stk. 3, fordi det ikke hidrører fra den angivne udsteder. I [AM2018.04.3002](#) domfældte Østre Landsret for forsøg på bedrageri og dokumentfalsk, da tiltalte signerede en digital låneansøgning med sit eget NemID og vedhæftede falske lønsedler.

Der straffes typisk i konkurrence, jf. [straffeloven § 89](#), når databedrageri og dokumentfalsk foreligger i den samme handling – fx NemID-signering af en elektronisk låneaftale med falske oplysninger.

LOV	Straffeloven § 89	Straffeloven § 171, stk. 2-3	Straffeloven § 279	Straffeloven § 279a
PRAKSIS				
	Landsretten · Dokumentfalsk og forsøg på bedrageri med falske lønsedler til låneansøgning – Stadfæstelse af 9 måneders fængsel			17.08.2018
	Landsretten · Domfældelse for forsøg på bedrageri og dokumentfalsk i forbindelse med digital låneansøgning			30.04.2018
	Landsretten · Fængsel i 2 år for omfattende bedrageri, databedrageri og dokumentfalsk for ca. 1,3 mio. kr.			15.08.2017

§ 2 Identitetsmisbrug som selvstændigt gerningsindhold (§ 264 e)

Ved lov nr. 292 af 8. marts 2022 blev [straffeloven § 264 e](#) indført som et selvstændigt forbud mod identitetsmisbrug. Bestemmelsen kriminaliserer den, der uberettiget anvender oplysninger om en anden person – herunder CPR-nummer, navn og billede – til på utilbørlig vis at udgive sig for at være denne person (stk. 1, nr. 1). Der kræves *ikke* et berigelsesformål; bestemmelsen rammer dermed tilfælde, der falder uden for bedrageri og databedrageri.

Ifølge [Rigsadvokatmeddelelsen om freds- og ærekrænkelser](#) er udgangspunktet en bøde på 10.000 kr. i førstegangstilfælde med en enkelt overtrædelse. I gentagelsestilfælde fastsættes markant højere bødestrafte, og ved groft identitetsmisbrug kan der idømmes fængsel op til 6 måneder.

Rigsadvokatmeddelelsen fastslår, at der straffes i *sammenstød* med bl.a. § 171 (dokumentfalsk), § 279 (bedrageri) og § 279 a (databedrageri), når identitetsmisbruget er led i en berigelsesforbrydelse. I [S-1647-24](#) domfældte Vestre Landsret for bedrageri og identitetsmisbrug, hvor tiltalte fremsendte fotos af andres ID-kort til købere for at skabe troværdighed ved Facebook Marketplace-svindel. Landsretten præciserede kvalifikationen:

Da tiltalte ikke påvirkede eller ændrede de personlige oplysninger, som han sendte til Forurettede3 og Forurettede8, kan han ikke anses for at have manipuleret en anden persons fremtræden. Der er derfor ikke grundlag for at anvende bestemmelsen i straffelovens § 264 e, nr. 2.

Derimod fandtes tiltalte skyldig i nr. 1, da han utilbørligt udgav sig for at være i familie med den person, hvis personalekort han fremviste.

LOV

[Straffeloven § 264e, stk. 1](#)

PRAKSIS

Landsretten · Bedrageri og Identitetsmisbrug: Ubetinget fængsel for salg af ikke-eksisterende varer på Facebook Marketplace 04.12.2024

§ 3 Strafadmåling ved NemID/MitID-baseret lånebedrageri

Strafadmålingen ved NemID/MitID-baseret lånebedrageri afhænger af det samlede beløb, antallet af forhold, gerningsperiodens længde og tiltaltes personlige forhold. Straffelovrådets betænkning nr. 1581/2023 om strafudmåling (bind III) gennemgår praksis systematisk og identificerer følgende niveauer for databedrageri:

Beløbsramme	Antal forhold	Typisk straf	Eksempler
Ca. 400.000 kr.	24	1 års fængsel	NemID-misbrug af samlevers identitet
700.000 – 1,3 mio. kr.	Mange	1-2 års fængsel	Misbrug af stilling, systematisk over længere periode
Over 3 mio. kr.	Talrige	2-2,5 års fængsel	Kommunal leder, 713 tilfælde
Over 6 mio. kr.	79+	1 år 9 mdr. – 6 år	Callcenter-bedrageri, NemKonto-ændring

Formildende omstændigheder: I [S-0564-21](#) idømte Vestre Landsret 1 års fængsel for 24 tilfælde af databedrageri (over 400.000 kr.) med misbrug af samleverens NemID. Straffen blev udmålt som en kombinationsdom – 3 måneder ubetinget og 9 måneder betinget – under vægt på frivillig tilmelding, fuld tilståelse, behandling for ludomani og en ekstraordinært lang sagsbehandlingstid.

Skærpende omstændigheder: I [SS-2891/2022-KBH](#) blev tiltalte idømt 1 år og 9 måneders fængsel for 79 forhold af databedrageri for over 6 mio. kr. begået via ændring af forurettedes NemKonto og efterfølgende lånoptagelse. I [SS-10613/2022-ARH](#) – et callcenter-bedrageri rettet mod ældre, der blev lokket til at afgive NemID-oplysninger – udmåltes straffen til 5,5-6 års fængsel for et samlet beløb på ca. 15 mio. kr.

Højesterets praksis: I [Sag 219/2017](#) stadfæstede Højesteret en straf på 3 år og 6 måneders fængsel for en IT-chef, der begik 78 tilfælde af bedrageri og dokumentfalsk for ca. 740.000 kr. mod to arbejdsgivere, kombineret med tre hackerangreb. Sagen illustrerer den skærpende virkning af betroet stilling og tilbagefald.

Kvalificeres forholdet som af *særlig grov beskaffenhed* efter [straffeloven § 286, stk. 2](#), hæves strafmaksimum til fængsel i 8 år. Bestemmelsen finder navnlig anvendelse ved systematiske forhold over en længere periode med et samlet beløb i millionklassen.

LOV

[Straffeloven § 279a](#)[Straffeloven § 286, stk. 2](#)

PRAKSIS

Højesteret · IT-chef idømt 3 år og 6 måneders fængsel for omfattende bedrageri, dokumentfalsk og groft datahærværk mod to arbejdsgivere 27.02.2018

Landsretten · Systematisk databedrageri gennem misbrug af samlevers NemID medførte delvist betinget fængselsstraf	13.09.2021
Landsretten · Fængsel i 2 år for omfattende bedrageri, databedrageri og dokumentfalsk for ca. 1,3 mio. kr.	15.08.2017
Byretten · Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe	15.12.2023
Byretten · Omfattende databedrageri med uretmæssig ændring af Nemkonti og efterfølgende låneoptagelser	12.05.2022

§ 4 "Muldyr"-problematikken: Hvidvask og medvirken ved kontooverdragelse

En særlig type MitID/NemID-misbrug involverer personer, der – frivilligt eller under pres – stiller deres bankkonto eller NemID-oplysninger til rådighed for ukendte tredjemænd, som bruger kontoen til at modtage og videresende bedrageriske midler. Disse "muldyr"-sager kvalificeres typisk som hvidvask efter [straffeloven § 290 a](#) og ikke som databedrageri.

I [S-0889-22](#) havde tiltalte bevidst overladt sine NemID-oplysninger til to personer mod et mindre beløb. Lån på 45.000 kr. blev optaget og indsat på kontoen, hvorefter 33.300 kr. blev overført videre. Vestre Landsret differentierede den juridiske kvalifikation:

Tiltalte har således gjort sig skyldig i hvidvask, jf. den nugældende bestemmelse i straffelovens § 290 a, for så vidt angår de 33.300 kr., som blev overført til konti tilhørende andre personer, og hæleri, jf. straffelovens § 290 vedrørende de 11.700 kr., som blev stående på tiltaltes konto.

Forsætsvurderingen er det centrale stridspunkt i muldyr-sager. I [99-1800/2023](#) fandt Retten i Herning, at tiltalte – der havde udleveret alle sine personlige oplysninger og NemID-koder til en ukendt Facebook-låneprofil – måtte have indset muligheden for misbrug og forholdt sig accepterende hertil:

Under de foreliggende omstændigheder, hvor tiltalte havde givet alle sine personlige oplysninger til sin konto i Bank 1 til en ukendt person, som stod bag en låneprofil på Facebook [...] finder retten det bevist, at tiltalte må have indset muligheden for, at hans konto kunne blive og rent faktisk blev brugt til modtagelse og videreoverførsel af udbytte fra strafbare lovovertrædelser.

Samme tiltalte blev dog frifundet for de sideløbende bedrageriforhold, fordi identitetsmisbruget (tiltaltes pas var stjålet) skabte rimelig tvivl om hans personlige medvirken i bedrageriet som sådant. Sagen illustrerer den vigtige skelnen mellem *kontotilrådighedsstillelse* (hvidvask) og *selve bedrageriet* (databedrageri/bedrageri).

LOV	Straffeloven § 290a, stk. 1	Straffeloven § 290, stk. 1	
PRAKSIS	Landsretten · Dømt for medvirken til hvidvask og hæleri efter NemID-misbrug – Idømt psykiatrisk behandling		15.02.2023
	Byretten · Dom for hvidvask: Modtagelse og hævnning af 25.000 kr. fra bedrageri		01.05.2024
	Byretten · Dom for grov hvidvask som "muldyr" via bankkonto og frifindelse for bedrageri pga. identitetsmisbrug		06.09.2023

§ 5 Ofrets aftaleretlige stilling: Hæfter man for et NemID-signeret lån?

Når en tredjemand optager et lån i en persons navn ved at misbruge dennes NemID, opstår spørgsmålet, om det digitale lånedokument binder den forurettede aftaleretligt. Højesteret har i **U.2019.1192H** og **U.2019.1197H** fastslået, at afgørelsen af, om NemID-indehaveren bliver forpligtet, må træffes på grundlag af en *konkret vurdering af det samlede hændelsesforløb*.

I denne vurdering indgår bl.a.:

- Under hvilke omstændigheder tredjemand er kommet i besiddelse af NemID-oplysningerne
- Om indehaveren har haft kendskab til, at tredjemand er i besiddelse af oplysningerne
- Om indehaveren har gjort, hvad der var muligt for at forhindre misbrug, fx ved at spærre sit NemID hurtigst muligt

I **BS-445/2020-OLR** nægtede Østre Landsret at fremme en fogedsag om tvangsfuldbyrdelse af et NemID-lån på 62.000 kr. hos Basisbank. De kærrende var franarret deres NemID-oplysninger af en bedrager, der udgav sig for politimand. Landsretten fandt det betænkeligt at fremme sagen:

Landsretten finder under disse omstændigheder efter en samlet vurdering, at det er betænkeligt at fremme fogedsagen.

Sagen viser, at der ikke gælder en automatisk bundethed ved digital signatur – den forurettede kan bestride sin forpligtelse, hvis NemID-oplysningerne er franarret under svindelagtige omstændigheder, og vedkommende har reageret hurtigt.

LOV

Retsplejeloven § 478, stk. 1, 4

PRAKSIS

Landsretten · Kære af fogedrettens afgørelse om fremme af fogedsag - identitetstyveri og NemID

10.09.2020

§ 6 Betalingslovens hæftelsestrappe: Ofrets ansvar over for banken ved uautoriserede MitID-transaktioner

Betalingslovens § 100 fastlægger en gradueret ansvarsfordeling mellem kunden ("betaleren") og banken ("udbyderen") ved uautoriserede betalingstransaktioner. Bestemmelsen gennemfører artikel 74 i 2. betalingstjenestedirektiv og opretholder følgende trappestige:

- **Stk. 1:** Udgangspunktet er, at *udbyderen hæfter* for tab ved andres uberettigede anvendelse.
- **Stk. 3:** Betaleren hæfter med op til **375 kr.**, hvis den personlige sikkerhedsforanstaltning (fx MitID) har været anvendt – den "simple" selvrisko.
- **Stk. 4, nr. 3:** Betaleren hæfter med op til **8.000 kr.**, hvis udbyderen godtgør, at betaleren ved *groft uforsvarlig adfærd* har muliggjort den uberettigede anvendelse.
- **Stk. 5:** Betaleren hæfter *uden beløbsbegrænsning*, hvis udbyderen godtgør, at betaleren med forsæt har oplyst sikkerhedsforanstaltningen under omstændigheder, hvor betaleren indså eller burde have indset misbrugsrisikoen.

Forarbejderne til § 100 (L 157, 2016-17) præciserer, at i phishing-tilfælde – hvor betaleren *uforsvarende* har overladt sin sikkerhedsforanstaltning – finder stk. 5 *ikke* anvendelse, fordi betaleren ikke overdrog oplysningerne med forsæt til, at der skulle foretages uberettiget anvendelse:

I tilfælde, hvor betaler uforvarende har overladt den personlige sikkerhedsforanstaltning til andre, eksempelvis i forbindelse med phishing, hæfter betaler ikke efter forslaget til stk. 5, idet betaler ikke overdrog den personlige sikkerhedsforanstaltning med forsæt på at der skal foretages den uberettigede anvendelse.

Et centralt modstykke er [§ 100, stk. 7](#): Udbyderen hæfter *uanset* stk. 3-5, hvis udbyderen ikke har krævet stærk kundeautentifikation, medmindre kunden har handlet svigagtigt. Denne bestemmelse presser banker og kortudstedere til at anvende 3D Secure og MitID-godkendelse ved alle fjernbetalinger.

Hertil kommer [§ 100, stk. 8](#), der fritager kunden helt, hvis tabet eller den uberettigede tilegnelse af sikkerhedsforanstaltningen *ikke kunne opdages* forud for misbruget – fx hvor kortoplysninger kompromitteres via et databrud hos en internetforretning.

Der er ingen vedtagne, men endnu ikke konsoliderede ændringer til betalingslovens § 100 (seneste konsolidering: 20. maj 2026).

LOV

Betalingsloven § 82

Betalingsloven § 93

Betalingsloven § 100, stk. 1-8

§ 7 Groft uforsvarlig adfærd ved MitID-godkendelse: Det centrale stridspunkt i Finansielle Ankenævn

Størstedelen af de civilretlige MitID-misbrugssager afgøres af Finansielle Ankenævn og drejer sig om, hvorvidt kundens godkendelse af en MitID-handling – typisk under social engineering via DBA, Facebook Marketplace, Tise eller falske GLS/DAO-henvendelser – udgør "groft uforsvarlig adfærd" efter [betalingslovens § 100, stk. 4, nr. 3](#).

Ankenævnet træffer konsekvent afgørelse med **stemmeflertallet 3-2**, hvor:

Flertallet (3 medlemmer) finder groft uforsvarlig adfærd og en selvrisko på 8.000 kr., med følgende kerneargumenter:

- Kunden har godkendt (swipet) en MitID-anmodning med klar tekst om fx "Log på hos MitID.dk for at se eller ændre i din MitID profil" eller "Betal [beløb] til [modtager]"
- Der var ingen logisk sammenhæng mellem den påståede aktivitet (modtagelse af betaling for en vare) og den godkendte handling (profilændring/betaling)
- Kunden burde have læst teksten og reageret på uoverensstemmelsen

Mindretallet (2 medlemmer) finder alene simpel selvrisko på 375 kr. og argumenterer:

- Der er tale om professionel, organiseret svindel, som en almindelig forbruger ikke kan forventes at gennemskue
- Banken bærer systemrisikoen for betalingssystemets sikkerhed
- Social engineering-teknikker udnytter kognitive bias, der rammer også påpasselige forbrugere

Dette mønster ses tydeligt i en lang række afgørelser:

Sag	Svindelmetode	Beløb	Afgørelse
327/2023	DBA-salg, MitID-indrullering	14.000 kr.	8.000 kr. selvrisko (3-2)

627/2023	Falsk GLS-henvendelse, MitID-indrullering	7.415 kr.	Fuld hæftelse op til 8.000 kr. (3-2)
120/2024	DBA phishing, MitID	–	8.000 kr. selvrisko (3-2)
265/2025	MitID phishing	–	8.000 kr. selvrisko (3-2)
304/2024	Facebook Marketplace	–	Groft uforsvarlig (3-2)

I enkelte sager **afviser** ankenævnet at behandle klagen, fordi sagen forudsætter parts- og vidneforklaringer under ed. I [5/2023](#) var der direkte modstrid mellem kundens forklaring (at hun ikke udleverede koder) og bankens tekniske logs (der viste aktiv indrullering). Ankenævnet kunne ikke afklare konflikten uden mundtlig bevisførelse og afviste sagen.

For SMS-baserede phishing-sager (smishing), hvor offeret lokkes til at afgive MitID-oplysninger via et link i en SMS, henvises til den beslægtede praksisoversigt om [SMS-phishing \(smishing\)](#).

LOV [Betalingsloven § 100, stk. 3-4](#)

PRAKSIS	Det finansielle ankenævn · Klager hæfter for 7.006 DKK efter godkendelse af svindeltransaktion med MitID	22.01.2026
	Det finansielle ankenævn · Indsigelse mod selvrisko på 8.000 kr. efter svindel-SMS og MitID-godkendelse af transaktion i indonesiske rupiah	10.10.2025
	Det finansielle ankenævn · Afvisning af sag om indsigelse mod korttransaktioner godkendt med MitID grundet behov for bevisførelse	27.05.2025
	Det finansielle ankenævn · Indsigelse mod hæftelse for svindeltransaktion godkendt med MitID efter falsk henvendelse på Facebook Marketplace	19.12.2024
	Det finansielle ankenævn · Kundes hæftelse for misbrug efter udlevering af MitID-oplysninger til svindler ved falsk GLS-henvendelse	15.10.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved misbrug af betalingskort godkendt med MitID efter phishing-mail	25.09.2024
	Det finansielle ankenævn · Afvisning af klage over hæftelse for 8.000 kr. ved MitID-misbrug grundet behov for bevisførelse	25.09.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved uautoriseret korttransaktion godkendt med MitID afvises grundet bevisusikkerhed	30.08.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved uautoriserede korttransaktioner efter misbrug af MitID	19.03.2024
	Det finansielle ankenævn · Afvisning af sag om misbrug af betalingskort godkendt med MitID grundet behov for bevisførelse	19.03.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for kortmisbrug efter svindel via Tise og indrullering af MitID på fremmed enhed	28.02.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved MitID-svindel i forbindelse med DBA-salg	06.02.2024
	Det finansielle ankenævn · Afvisning af sag om misbrug af MitID og betalingskort grundet behov for bevisførelse	06.02.2024

§ 8 Autoriserede overførsler under social engineering: Uden for betalingslovens dækning

Et vigtigt afgrænsningsspørgsmål er sondringen mellem *uautoriserede* og *autoriserede* betalingstransaktioner. Når kunden selv logger ind i sin netbank med sit eget MitID og foretager overførsler – typisk under telefonisk

manipulation ("vishing") af en bedrager, der udgiver sig for at være bankens medarbejder – er der tale om *autoriserede* transaktioner, som falder *uden for* [betalingslovens § 100](#).

I [100/2023](#) blev en kunde telefonisk overbevist om, at hendes konti var under hacking-angreb. Hun foretog selv fire overførsler for i alt 251.000 kr. via MitID-login og bekræftede hver overførsel ved at svare "JA" på en kontrol-SMS fra banken. Finansielle Ankenævn afviste klagen:

Da klageren selv har iværksat overførslerne ved at logge ind i netbanken med sit MitID [...] er der tale om autoriserede betalingstransaktioner.

Denne sontring har stor praktisk betydning: Ved uautoriserede transaktioner hæfter kunden som udgangspunkt kun for 375 kr. eller 8.000 kr., mens kunden ved autoriserede transaktioner under social engineering bærer hele tabet. I [72/2024](#) kombinerede svindleren vishing og kortmisbrug: De overførsler, kunden selv foretog, var autoriserede (fuldt tab), mens de kortbetalinger, svindleren foretog med de franarrede kortoplysninger, var uautoriserede (selvrisko).

LOV	Betalingsloven § 82	Betalingsloven § 100	
PRAKSIS	Det finansielle ankenævn · Hæftelse for kontooverførsler og kortmisbrug efter vishing-opkald og spørgsmål om dobbelt selvrisko		04.12.2024
	Det finansielle ankenævn · Afvisning af erstatningskrav for autoriserede netbankoverførsler foretaget under social engineering-svindel		18.09.2023

§ 9 Datatilsynets tilsyn med MitID/NemID-infrastrukturens sikkerhed

Datatilsynet har i flere sager udtalt alvorlig kritik af sikkerhedsbrister i MitID- og NemID-infrastrukturen, som har muliggjort eller forværret misbrug.

I [afgørelse 2022-432-0079](#) udtalte Datatilsynet **alvorlig kritik** af Digitaliseringsstyrelsen for en race condition i MitID-systemet. Fejlen betød, at en brugers identitet under visse omstændigheder kunne kompromitteres, uden at brugeren havde mulighed for at opdage det. Tilsynet lagde vægt på, at MitID udgør en central national infrastruktur, og at sikkerhedsniveauet derfor skal være proportionalt med risikoen.

I [afgørelse 2023-432-0017](#) rettede tilsynet alvorlig kritik mod Nets DanID for et NemID-nedbrud, der efterlod brugerne uden sikker digital identifikation. Tilsynet vurderede, at nedbruddet skyldtes utilstrækkelige tekniske og organisatoriske foranstaltninger.

I [afgørelse 2023-432-0025](#) kritiserede Datatilsynet Digitaliseringsstyrelsen for en utilstrækkelig JavaScript-risikovurdering i MitID, der potentielt kunne udnyttes til at omgå sikkerhedsforanstaltninger.

Disse afgørelser understreger, at ansvaret for MitID/NemID-sikkerheden ikke alene hviler på brugerne. Systemfejl og infrastrukturens svigt kan udgøre en selvstændig årsag til misbrug, og Datatilsynets kritik kan have afledt betydning for bedømmelsen af brugerens hæftelse efter [betalingslovens § 100, stk. 6, nr. 3](#) – udbyderen hæfter, hvis denne ikke har truffet egnede foranstaltninger til at beskytte betalingsinstrumentet.

LOV	Betalingsloven § 100, stk. 6	
PRAKSIS	Datatilsynet · Alvorlig kritik af Nets DanID for utilstrækkelig behandlingssikkerhed ved omfattende NemID-nedbrud	02.05.2024

Datatilsynet · Digitaliseringsstyrelsen får kritik for utilstrækkelig risikovurdering af borgeres rettigheder	09.11.2023
Datatilsynet · Alvorlig kritik af Digitaliseringsstyrelsen for brister i MitID-sikkerheden	23.06.2023

§ 10 Sammenfatning og hovedtendenser

Praksis vedrørende MitID/NemID-misbrug og digital identitetstyveri tegner følgende hovedtendenser:

Strafferetligt:

- Uberettiget lånoptagelse via andres digitale identitet kvalificeres som databedrageri (§ 279 a) – typisk i konkurrence med dokumentfalsk (§ 171) og eventuelt identitetsmisbrug (§ 264 e)
- Strafmålingen er primært styret af det samlede bedragne beløb og antallet af forhold; systematisk NemID-misbrug for mere end 400.000 kr. medfører ubetinget fængsel
- "Muldyr", der stiller konto eller NemID til rådighed, dømmes for hvidvask (§ 290 a); forsætsvurderingen baseres på acceptforsæt – det er tilstrækkeligt, at kontohaveren indså muligheden for misbrug og forholdt sig accepterende
- Identitetsmisbrug (§ 264 e) straffes i sammenstød med bedrageri og giver et selvstændigt grundlag, der ikke forudsætter berigelsesformål

Civilretligt (betalingsloven):

- Finansielle Ankenævn fastholder konsekvent (med 3-2 flertal), at MitID-godkendelse trods klar advarseltekst udgør groft uforsvarlig adfærd → selvrisiko 8.000 kr.
- Mindretallet argumenterer for, at professionel svindel ikke bør belaste forbrugeren → selvrisiko 375 kr.
- Overførsler foretaget af kunden selv under social engineering (vishing) er autoriserede og falder *uden for* § 100 – kunden bærer det fulde tab
- Aftaleretligt kan den forurettede bestride sin bundethed af et NemID-signeret lånedokument, hvis NemID-oplysningerne er franarret under svindelforhold – vurderingen beror på en helhedsbedømmelse efter Højesterets praksis

Systemisk:

- Datatilsynet har udtalt alvorlig kritik af tekniske sikkerhedsbrister i MitID/NemID-infrastrukturen, hvilket understreger, at ansvaret for digital identitetssikkerhed ikke alene påhviler den enkelte bruger
- Betalingslovens § 100, stk. 7, lægger et betydeligt pres på udbydere for at anvende stærk kundeautentifikation – undladelse heraf medfører, at udbyderen selv hæfter

Retsstillingen er kendetegnet ved en spænding mellem hensynet til at beskytte forbrugere mod professionel digital svindel og hensynet til at opretholde tilliden til digital signatur som legitimationsgrundlag. Den vedvarende 3-2 splittelse i Finansielle Ankenævn signalerer, at grænsen for "groft uforsvarlig adfærd" ved social engineering fortsat er retspolitisk omstridt.

LOV

Betalingsloven § 100, stk. 4

Straffeloven § 279a

REFERENCE Lovgrundlag

6 paragraffer

Betalingsloven § 100	stk. 3-5	Straffeloven § 171	
Straffeloven § 264e	stk. 1	Straffeloven § 279	
Straffeloven § 279a		Straffeloven § 286	stk. 2

MATERIALE Citerede afgørelser

34 afgørelser

HØJESTERET · ØVERSTE INSTANS

1

27.02.2018	IT-chef idømt 3 år og 6 måneders fængsel for omfattende bedrageri, dokumentfalsk og groft datahærværk mod to arbejdsgivere	Sag 219/2017
------------	--	--------------

LANDSRETTEEN · ANKEINSTANS

8

04.12.2024	Bedrageri og Identitetsmisbrug: Ubetinget fængsel for salg af ikke-eksisterende varer på Facebook Marketplace	S-1647-24
15.02.2023	Dømt for medvirken til hvidvask og hæleri efter NemID-misbrug – Idømt psykiatrisk behandling	S-0889-22
31.01.2023	Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn	S-0930-22
13.09.2021	Systematisk databedrageri gennem misbrug af samlevers NemID medførte delvist betinget fængselsstraf	S-0564-21
10.09.2020	Kære af fogedrettens afgørelse om fremme af fogedsag - identitetstyveri og NemID	1251-1509
17.08.2018	Dokumentfalsk og forsøg på bedrageri med falske lønsedler til låneansøgning – Stadfæstelse af 9 måneders fængsel	AM2018.08.170
30.04.2018	Domfældelse for forsøg på bedrageri og dokumentfalsk i forbindelse med digital låneansøgning	AM2018.04.3002
15.08.2017	Fængsel i 2 år for omfattende bedrageri, databedrageri og dokumentfalsk for ca. 1,3 mio. kr.	S-2360-16

BYRETTEEN · FØRSTE INSTANS

5

01.05.2024	Dom for hvidvask: Modtagelse og hævnning af 25.000 kr. fra bedrageri	3-8847/2023
15.12.2023	Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe	6497-7797
06.09.2023	Dom for grov hvidvask som "muldyr" via bankkonto og frifindelse for bedrageri pga. identitetsmisbrug	99-1800/2023
12.05.2022	Omfattende databedrageri med uretmæssig ændring af Nemkonti og efterfølgende låneoptagelser	1525-1841
18.10.2016	Dom for 28 forhold af bedrageri og omfattende databedrageri ved brug af stjålne kreditkortoplysninger	10-4468/2016

DET FINANSIELLE ANKENÆVN · NÆVN / KLAGEINSTANS		17
22.01.2026	Klager hæfter for 7.006 DKK efter godkendelse af svindeltransaktion med MitID	491/2025
10.10.2025	Indsigelse mod selvrisko på 8.000 kr. efter svindel-SMS og MitID-godkendelse af transaktion i indonesiske rupiah	265/2025
27.05.2025	Afvisning af sag om indsigelse mod korttransaktioner godkendt med MitID grundet behov for bevisførelse	14/2025
19.12.2024	Indsigelse mod hæftelse for svindeltransaktion godkendt med MitID efter falsk henvendelse på Facebook Marketplace	304/2024
04.12.2024	Hæftelse for kontooverførsler og kortmisbrug efter vishing-opkald og spørgsmål om dobbelt selvrisko	72/2024
15.10.2024	Kundes hæftelse for misbrug efter udlevering af MitID-oplysninger til svindler ved falsk GLS-henvendelse	627/2023
25.09.2024	Indsigelse mod hæftelse for 8.000 kr. ved misbrug af betalingskort godkendt med MitID efter phishing-mail	120/2024
25.09.2024	Afvisning af klage over hæftelse for 8.000 kr. ved MitID-misbrug grundet behov for bevisførelse	529/2023
30.08.2024	Indsigelse mod hæftelse for 8.000 kr. ved uautoriseret korttransaktion godkendt med MitID afvises grundet bevisusikkerhed	14/2024
19.03.2024	Indsigelse mod hæftelse for 8.000 kr. ved uautoriserede korttransaktioner efter misbrug af MitID	447/2023
19.03.2024	Afvisning af sag om misbrug af betalingskort godkendt med MitID grundet behov for bevisførelse	495/2023
28.02.2024	Indsigelse mod hæftelse for kortmisbrug efter svindel via Tise og indrullering af MitID på fremmed enhed	5/2023
06.02.2024	Indsigelse mod hæftelse for 8.000 kr. ved MitID-svindel i forbindelse med DBA-salg	327/2023
06.02.2024	Afvisning af sag om misbrug af MitID og betalingskort grundet behov for bevisførelse	364/2023
18.09.2023	Afvisning af erstatningskrav for autoriserede netbankoverførsler foretaget under social engineering-svindel	100/2023
30.03.2023	Indsigelse mod 3D Secure-betaling godkendt via NemID afvist af Ankenævnet grundet behov for bevisførelse	360/2022
24.05.2022	Spørgsmål om 13-måneders frist for indsigelse mod uautoriserede transaktioner fra 2016 i Nordea Bank	346/2021
DATATILSYNET · NÆVN / KLAGEINSTANS		3
02.05.2024	Alvorlig kritik af Nets DanID for utilstrækkelig behandlingssikkerhed ved omfattende NemID-nedbrud	2023-432-0017
09.11.2023	Digitaliseringsstyrelsen får kritik for utilstrækkelig risikovurdering af borgeres rettigheder	2023-432-0025

23.06.2023 Alvorlig kritik af Digitaliseringsstyrelsen for brister i MitID-sikkerheden

2022-432-0079

FORARBEJDE Betænkninger

1 reference

Betænkning om strafudmåling – Bind III

nr. 1581 · 2023 · Justitsministeriet

12

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over MobilePay og betalingstjeneste-bedrageri

Bedrageri, databedrageri og hvidvask via MobilePay, Apple Pay og lignende tjenester

Version 2 · Opdateret 24. jun. 2026 · 18 afgørelser · 2018-2025

[Læs online](#)

INTRODUKTION

Denne praksisoversigt behandler strafferetlig og civilretlig praksis vedrørende misbrug af MobilePay, Apple Pay og lignende betalingstjenester. De typiske gerningsformer omfatter salg af varer på DBA eller Facebook Marketplace uden levering, telefonsvindel (vishing) hvor gerningsmænd udgiver sig for bankpersonale, og hvidvask via MobilePay-overførsler. Sondringen mellem bedrageri (straffelovens § 279) og databedrageri (§ 279 a) beror på, om en person villedes eller en elektronisk dataproces manipuleres – ved online salgsbedrageri, hvor forurettede frivilligt betaler, er § 279 typisk det rette subsumtionsgrundlag. Strafniveauet spænder fra betinget fængsel i enkeltstående tilfælde til flere års ubetinget fængsel ved systematisk kriminalitet med mange forurettede og store beløb. På civilretssiden regulerer betalingslovens § 100 fordelingen af tab ved uautoriserede transaktioner mellem betaler og betalingsudbyder.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Salg af varer på DBA eller Facebook Marketplace uden intention om levering udgør bedrageri efter straffelovens § 279, idet sælgeren fremkalder en vildfarelse om, at varen vil blive leveret, og derved skaffer sig uberettiget vinding.
- 02** Sondringen mellem bedrageri (§ 279) og databedrageri (§ 279 a) beror på, om det er en person, der villedes (§ 279), eller en elektronisk dataproces, der manipuleres uden direkte personkontakt (§ 279 a) – ved online salgsbedrageri, hvor offeret frivilligt betaler, er § 279 det rette grundlag.
- 03** Modtagelse og videreoverførsel af penge via MobilePay, der stammer fra svindel, kan udgøre hvidvask efter § 290 a, stk. 1, når modtageren vidste eller bestemt formodede, at pengene stammede fra en strafbar lovovertrædelse.
- 04** Ved forsætsvurderingen for hvidvask via MobilePay lægger domstolene vægt på, om modtageren fik overført et højere beløb end aftalt fra en ukendt afsender, idet dette indikerer viden om den strafbare oprindelse.

- 05** Ved systematisk online salgsbedrageri med mange forurettede fastsættes straffen navnlig under hensyn til antallet af forhold og det samlede formuetaf – 38 bedragerier for over 400.000 kr. udmåltes til fængsel i 1 år.
- 06** Ubetinget fængsel er udgangspunktet ved et større antal bedrageriforhold, men straffen kan gøres betinget med vilkår om samfundstjeneste, særligt for ustraffede gerningsmænd med gode personlige forhold.
- 07** Tilståelse i sager om omfattende bedrageri anerkendes som formildende omstændighed efter straffelovens § 82, stk. 1, nr. 9, navnlig når den medfører en ikke ubetydelig ressourcebesparelse.
- 08** Enkeltstående DBA-bedrageri for et mindre beløb (under ca. 2.000 kr.) udmåles typisk til 14 dages betinget fængsel – lang sagsbehandlingstid kan føre til, at vilkår om samfundstjeneste bortfalder.
- 09** Bedrageri af særligt grov beskaffenhed (§ 286, stk. 2) med strafferamme op til 8 år kan foreligge ved professionel eller erhvervsmæssig karakter eller et stort antal forhold.
- 10** Efter betalingslovens § 100 hæfter betalerens udbyder som udgangspunkt for uautoriserede betalingstransaktioner via MobilePay, men betaleren kan pålægges en selvrisiko på op til 8.000 kr. ved groft uforsvarlig adfærd.
- 11** Krav mod banken om tilbagebetaling af uautoriserede MobilePay-transaktioner forældes efter tre år fra transaktionens gennemførelse, jf. forældelseslovens § 3.

Sondringen mellem bedrageri og databedrageri ved misbrug af betalingstjenester

§ 1

Den strafferetlige behandling af misbrug af MobilePay og lignende betalingstjenester hviler på to centrale bestemmelser i straffeloven:

- **Bedrageri** efter [straffelovens § 279](#) rammer den, som for derigennem at skaffe sig uberettiget vinding retsstridigt fremkalder, bestyrker eller udnytter en vildfarelse og derved bestemmer en anden til en handling, der påfører denne et formuetaf. Bestemmelsen forudsætter, at det er en *person*, der villedes.
- **Databedrageri** efter [straffelovens § 279 a](#) rammer den, som retsstridigt ændrer, tilføjer eller sletter oplysninger til elektronisk databehandling eller i øvrigt søger at påvirke resultatet af en sådan databehandling. Her er det ikke en person, men et *elektronisk system*, der manipuleres.

Sondringen har afgørende betydning for subsumtionen af MobilePay-bedrageri. Når en gerningsmand sælger en vare på DBA eller Facebook Marketplace, modtager betaling via MobilePay og aldrig leverer varen, er det køberen – en person – der villedes om, at varen vil blive leveret. Forholdet subsumeres derfor under § 279. Omvendt foreligger databedrageri efter § 279 a, når gerningsmanden uden offerets medvirken direkte manipulerer det elektroniske betalingssystem, fx ved at bruge stjålne kortoplysninger til at gennemføre transaktioner i MobilePay eller Apple Pay.

Strafferammen for begge forbrydelser er fængsel indtil 1 år og 6 måneder, jf. [straffelovens § 285, stk. 1](#). Straffen kan stige til fængsel i 8 år, hvis forbrydelsen er af *særligt grov beskaffenhed*, jf. [straffelovens § 286, stk. 2](#), navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter, størrelsen af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

[Rigsadvokatmeddelelsen om formueforbrydelser](#) indeholder retningslinjer for anklagepraksis ved bedrageri og databedrageri, herunder vejledning om subsumtion og strafpåstande.

Der er ingen vedtagne, ikke-konsoliderede ændringer af §§ 279 eller 279 a pr. juni 2026.

For MitID-baseret indlogging på MobilePay-appen, se praksisoversigten om [MitID/NemID-misbrug](#). For fysisk korttyveri og kortskimming, se praksisoversigterne om [bedrageri](#) og [databedrageri](#).

LOV

[Straffeloven § 279](#)[Straffeloven § 279a](#)[Straffeloven § 285, stk. 1](#)[Straffeloven § 286, stk. 2](#)

Online salgsbedrageri via DBA og Facebook Marketplace – typiske gerningsformer

Den hyppigste gerningsform ved MobilePay-relateret bedrageri er online salgsbedrageri, hvor gerningsmanden opretter en annonce for en vare – typisk elektronik som smartphones, spillekonsoller eller Lego – på DBA.dk, Facebook Marketplace, Reshopper eller lignende platforme, modtager betaling via MobilePay eller straksoverførsel og aldrig leverer varen.

Gerningsformen følger et typisk mønster:

1. Gerningsmanden opretter en annonce med billeder (ofte kopieret fra andre annoncer) til en attraktiv pris
2. Køber tager kontakt og aftaler køb
3. Betaling sker via MobilePay, bankoverførsel eller straksoverførsel
4. Gerningsmanden undlader at sende varen og afbryder kontakten

I sagen [S-2932-20](#) havde tiltalte annonceret en Samsung Galaxy S7 på DBA til 1.300 kr. Forurettede betalte via MobilePay, men modtog aldrig telefonen. Tiltalte undveg herefter al kontakt og nægtede at åbne døren, da forurettede opsøgte ham personligt. Østre Landsret fandt det bevist, at tiltalte fra starten manglede vilje til at levere varen. Tiltalte havde tidligere domme for mandatsvig og bedrageri.

I en mere omfattende sag, [S-2725-19](#), blev tiltalte fundet skyldig i 37 fuldbyrdede bedragerier og ét forsøg – i alt 38 forhold – begået i perioden juli til november 2018 via DBA. Tiltalte udgav sig for at sælge elektronik og andre varer mod forudbetaling, men leverede aldrig. Det samlede formuetab for de 40 forurettede beløb sig til 403.957 kr.

I byretten ([SS-1460/2023-HEL](#)) blev en tiltalt dømt for systematisk bedrageri via DBA, Facebook Marketplace og Reshopper, hvor betaling blev modtaget via MobilePay. I en anden byretsdom ([SS-4447/2022-ALB](#)) var DBA-bedrageri via MobilePay og straksoverførsel kombineret med trusler mod forurettede, der forsøgte at få pengene tilbage.

I sagen [SS 2-16817/2023](#) blev to tiltalte dømt for en lang række forhold, herunder internetbedrageri med salg af iPhones, Lego og spillekonsoller på nettet, hvor betaling blev modtaget til tiltaltes bankkonto uden

levering, samt misbrugelse af andres identitetsoplysninger til at oprette mobilabonnementer og købe telefoner i forretninger.

LOV [Straffeloven § 279](#)

PRAKSIS	Landsretten · Dom for omfattende bedrageri begået via DBA og NemID-svindel: Landsretten ændrer delvist ubetinget fængsel til betinget straf med samfundstjeneste	13.12.2021
	Landsretten · Bedrageri ved salg af mobiltelefon via DBA - Betaling modtaget, men vare aldrig leveret	09.03.2021
	Byretten · Omfattende sag om systematisk bedrageri, identitetsmisbrug og tyveri fører til fængselsstraffe	10.07.2025
	Byretten · Dom for bedrageri og chikane: Fængselsstraf og erstatningskrav	04.10.2023
	Byretten · Anbringelsesdom for omfattende internetbedrageri, vidnetrusler og forsøg på ulovlig tvang	13.03.2023

§ 3 Telefonsvindel (vishing) og misbrug af betalingstjenester ved identitetssvig

En voksende gerningstype involverer telefonsvindel (vishing), hvor gerningsmænd ringer til ofre og udgiver sig for at være fra offerets bank eller politiet. Formålet er at få offeret til at udlevere betalingskort, PIN-koder eller NemID/MitID-oplysninger, som derefter bruges til hævnninger og betalinger via MobilePay, Apple Pay eller netbank.

I sagen [S-0009-25](#) blev tiltalte fundet skyldig i 42 tilfælde af bedrageri og databedrageri rettet mod primært ældre borgere. Gerningsmændene kontaktede ofrene telefonisk og udgav sig for bankrådgivere under påskud af at afværge misbrug. Ofrene blev manipuleret til at modtage gerningsmændene på deres bopæl og udlevere betalingskort og PIN-koder, hvorefter der hurtigt blev foretaget omfattende hævnninger og køb. Vestre Landsret fastsatte straffen med henvisning til tilståelsens formildende virkning:

Efter en samlet vurdering af karakteren, grovheden og omstændighederne vedrørende de forhold, som tiltalte er fundet skyldig i, sammenholdt med omfanget af den ikke ubetydelige ressourcebesparelse i retsid, som tiltaltes tilståelse har medført, finder landsretten, at hensynet til tilståelsen som formildende omstændighed, jf. [straffelovens § 82, stk. 1, nr. 9](#), skal føre til, at fælles og tillægsstraffen fastsættes til fængsel i 1 år og 9 måneder.

Ved kvalifikationen af telefonsvindel er det afgørende, om det er offeret selv, der foretager transaktionen (§ 279, bedrageri), eller om gerningsmanden ved brug af de indhentede oplysninger selv gennemfører betalinger i offerets navn (§ 279 a, databedrageri). Ofte foreligger begge gerningsformer i samme sagskompleks.

I en særskilt sagskategori kombineres online salgsbedrageri med identitetsmisbrug, fx når gerningsmanden bruger en anden persons identitet i forbindelse med svindlen. I sagen [S-1647-24](#) ved Vestre Landsret blev tiltalte dømt for Facebook Marketplace-bedrageri kombineret med identitetsmisbrug efter [straffelovens § 264 e](#).

LOV [Straffeloven § 82, stk. 1](#)

[Straffeloven § 264e](#)

[Straffeloven § 279](#)

[Straffeloven § 279a](#)

PRAKSIS	Landsretten · Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold)	11.04.2025
	Landsretten · Bedrageri og Identitetsmisbrug: Ubetinget fængsel for salg af ikke-eksisterende varer på Facebook Marketplace	04.12.2024

§ 4 Databedrageri ved misbrug af stjålne kortoplysninger i MobilePay og Apple Pay

Databedrageri efter [straffelovens § 279 a](#) foreligger, når gerningsmanden retsstridigt bruger stjålne eller uretmæssigt erhvervede kortoplysninger til at gennemføre transaktioner i MobilePay, Apple Pay eller andre digitale tegnebøger. Her er det ikke en person, der villedes, men det elektroniske betalingssystem, der manipuleres med urigtige data.

I sagen **S-1842-17** ved Østre Landsret blev tiltalte dømt for 92 forhold om databedrageri begået via MobilePay og stjålne kortoplysninger. Gerningsformen illustrerer den systematiske karakter, som databedrageri via betalingstjenester kan antage, når gerningsmanden har adgang til mange kortoplysninger.

I sagen **S-0930-22** ved Landsretten blev tiltalte fundet skyldig i bedrageri for et iPhone-salg, men frifundet for et tilknyttet databedrageri-forhold. Afgørelsen illustrerer den praktiske sondring mellem de to bestemmelser – bedrageri (§ 279) blev stadfæstet for det forhold, hvor forurettede selv betalte i tillid til levering, mens databedrageri-tiltalen (§ 279 a) ikke kunne bevises.

Højesteret har i kendelse **AM2023.06.28H** taget stilling til varetægtsfængsling i en sag om databedrageri, hvilket understreger, at der ved omfattende databedrageri kan foreligge en styrke af mistanke og en kriminalitetens alvor, der begrunder frihedsberøvelse under efterforskningen.

Også ved røverier kan databedrageri via betalingstjenester indgå som sekundært forhold, fx når gerningsmænd efter et røveri bruger offerets betalingskort til at forsøge hævnninger via MobilePay eller hæveautomater.

LOV

[Straffeloven § 279a](#)
[Straffeloven § 279](#)

PRAKSIS

Højesteret · Højesterets vurdering af varetægtsfængsling ved omfattende databedrageri og påvirkningsrisiko 28.06.2023

Landsretten · Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn 31.01.2023

Landsretten · Databedrageri og medvirken til omfattende misbrug af stjålne kreditkort via MobilePay – Frifindelse for medvirkende kontoindehaver 21.02.2018

§ 5 Hvidvask via MobilePay efter straffelovens § 290 a

MobilePay bruges i stigende grad som kanal for hvidvask, typisk ved at en person stiller sin konto til rådighed for overførsel og videreformidling af penge, der stammer fra svindel. Hvidvask straffes efter [straffelovens § 290 a, stk. 1](#) med bøde eller fængsel indtil 1 år og 6 måneder, og straffen kan stige til fængsel i 8 år ved grov hvidvask, jf. [§ 290 a, stk. 2](#).

I sagen **S-0234-24** blev tiltalte fundet skyldig i hvidvask efter § 290 a, stk. 1. Tiltalte havde efter aftale med en veninde modtaget 17.000 kr. fra en ukendt person på sin bankkonto, hævet 5.000 kr. kontant og overført de resterende 12.000 kr. via MobilePay. Pengene stammede fra NemID-svindel mod en tredjemand.

Forsætsspørgsmålet var afgørende. Vestre Landsret stadfæstede med 4 mod 2 stemmer:

Vi har herved lagt vægt på de samme omstændigheder, som byretten har anført. Vi har tillige lagt vægt på, at tiltalte har forklaret, at hun aftalte med Person2, at hun skulle modtage 5.000 kr. på sin konto fra Person2, som hun herefter

skulle have til hende, og at hun i stedet modtog 17.000 kr. fra en anden person. Vi finder det herefter bevist, at tiltalte havde det fornødne forsæt til at begå hvidvask.

Domstolene lagde ved forsætsvurderingen navnlig vægt på:

- At det overførte beløb var betydeligt højere end det aftalte
- At pengene kom fra en person, tiltalte ikke kendte
- At tiltalte ikke kendte detaljer om venindens private forhold trods det påståede nære venskab

Straffen blev fastsat til betinget fængsel i 14 dage, henset til forholdets karakter og tiltaltes unge alder og ustraffethed.

I byretsdom **SS-3603/2023-HER** blev tiltalte dømt for 5 hvidvask-forhold via MobilePay, hvilket viser det typiske mønster, hvor en person gentagne gange modtager og videregiver svindeludbytte gennem sin MobilePay-konto.

LOV

Straffeloven § 290a, stk. 1, 2

PRAKSIS

Landsretten · Stadfæstelse af dom for hvidvask via MobilePay: Tiltalte modtog 17.000 kr. fra ukendt kilde efter aftale med veninde 02.04.2025

Byretten · Betinget fængselsstraf for fem forhold af hvidvask via MobilePay 11.03.2024

§ 6 Strafadmåling ved betalingstjeneste-bedrageri

Strafadmålingen ved online salgsbedrageri via MobilePay og lignende betalingstjenester afhænger af en række faktorer: antallet af forhold, det samlede formuetab, gerningsmandens personlige forhold, eventuelt recidiv og tilståelsens karakter.

Praksis viser følgende mønstre:

Sag	Antal forhold	Beløb	Straf	Betingelser
S-2932-20 (ØL)	1	1.300 kr.	14 dage	Betinget, prøvetid 1 år
S-2725-19 (ØL)	38	403.957 kr.	1 år	Betinget, 200 timer samfundstjeneste
S-0009-25 (VL)	42	Betydeligt	1 år 9 mdr.	Ubetinget

Formildende omstændigheder i praksis:

- Ustraffethed: I S-2725-19 ændrede landsretten fuldbyrdelsesmåden fra delvist ubetinget til fuldt betinget fængsel med samfundstjeneste, fordi tiltalte var ustraffet og havde gode personlige forhold
- Tilståelse: I S-0009-25 anerkendte landsretten tilståelsens ressourcebesparelse som formildende efter [straffelovens § 82, stk. 1, nr. 9](#)
- Lang sagsbehandlingstid: I S-2932-20 medførte den lange sagsbehandlingstid, at vilkår om samfundstjeneste og tilsyn bortfaldt
- Ung alder: Særligt ved hvidvask via MobilePay ses lave straffe for unge, ustraffede tiltalte (14 dage betinget)

Skærpende omstændigheder i praksis:

- Tidligere bedrageridømme (recidiv)
- Stor professionel organisering og mange ofre
- Særligt sårbare ofre (ældre borgere)
- Kombination med identitetsmisbrug eller dokumentfalsk
- At kriminaliteten er fortsat trods tidligere advarsel

Ved groft bedrageri/databedrageri efter [straffelovens § 286, stk. 2](#) forhøjes strafferammen til 8 år, hvilket typisk aktualiseres ved professionel, erhvervsmæssig svindel med mange forurettede.

LOV	Straffeloven § 82, stk. 1	Straffeloven § 285, stk. 1	Straffeloven § 286, stk. 2
PRAKSIS	Højesteret · Højesteret fastlægger retningslinjer for tilståelsesrabat under den nye straffelov § 82, nr. 9, i sag om omfattende narkotika, databedrageri og hæleri 15.05.2025		
	Landsretten · Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold) 11.04.2025		
	Landsretten · Dom for omfattende bedrageri begået via DBA og NemID-svindel: Landsretten ændrer delvist ubetinget fængsel til betinget straf med samfundstjeneste 13.12.2021		
	Landsretten · Bedrageri ved salg af mobiltelefon via DBA - Betaling modtaget, men vare aldrig leveret 09.03.2021		

Betalingslovens hæftelsesregler ved misbrug af MobilePay og Apple Pay

Betalingslovens regler om hæftelse for uautoriserede betalingstransaktioner har direkte betydning for ofre for MobilePay- og Apple Pay-svindel. Reglerne fordeler tabet mellem betaleren og dennes udbyder (typisk banken) efter en gradueret ansvarsmodel.

Efter [betalingslovens § 100](#) er udgangspunktet, at betalerens udbyder hæfter for uautoriserede transaktioner. Betaleren kan dog pålægges en selvrisiko:

- Op til **375 kr.** ved simpel uagtsom adfærd, jf. [§ 100, stk. 3](#)
- Op til **8.000 kr.** ved groft uforsvarlig adfærd, jf. [§ 100, stk. 4](#)
- **Fuldt tab** ved forsætlig medvirken eller grove tilsidesættelser, jf. [§ 100, stk. 5](#)

I sagen [58/2025](#) hos Det Finansielle Ankenævn var klagerens kort blevet tilknyttet MobilePay af en bekendt via MitID-godkendelse, hvorefter der blev overført i alt 80.000 kr. Sydbank dækkede 72.000 kr. men fastholdt en egenandel på 8.000 kr. med henvisning til groft uforsvarlig adfærd. Ankenævnet afviste at behandle sagen, da den krævede mundtlige parts- og vidneforklaringer.

I sagen [238/2022](#) var en ældre kunde blevet kontaktet af en svindler, der udgav sig for at komme fra IT-support. Kunden udleverede NemID-oplysninger, som svindleren brugte til at oprette et virtuelt kort i Apple Wallet og gennemføre 11 transaktioner for 24.736 kr. Sparekassen tilbageførte 16.736 kr. men fastholdt en selvrisiko på 8.000 kr. efter [§ 100, stk. 4](#). Også denne sag blev afvist af ankenævnet.

Et vigtigt opmærksomhedspunkt er **forældelse**. I sagen [280/2021](#) havde klagerens tidligere samlever uberettiget overført 19.700 kr. via MobilePay i februar 2017. Den tidligere samlever blev senere dømt for databedrageri. Da klageren først genoptog sagen mod banken i 2021, fandt ankenævnet kravet forældet efter [forældelseslovens § 3](#), idet den treårige frist regnes fra transaktionens tidspunkt.

Det er endvidere værd at bemærke, at registreringen af brug af et betalingsinstrument ikke i sig selv er bevis for, at betaleren har autoriseret transaktionen, jf. [betalingslovens § 98, stk. 2](#). Banken bærer bevisbyrden for, at kunden har handlet svigagtigt.

LOV	Betalingsloven § 98, stk. 2	Betalingsloven § 100, stk. 3-5	Forældelsesloven § 3
PRAKSIS	Det finansielle ankenævn · 58/2025: Afvisning af sag om MobilePay-misbrug på 80.000 kr. grundet behov for bevisførelse om MitID-godkendelse 31.10.2025 Det finansielle ankenævn · Afvisning af sag om misbrug via Apple Pay og MobilePay grundet behov for bevisførelse 21.02.2023 Det finansielle ankenævn · Spørgsmål om forældelse af indsigelse mod uautoriserede MobilePay-transaktioner foretaget af tidligere samlever 19.04.2022		

§ 8 Sammenfatning af hovedlinjer i praksis

Praksis om MobilePay- og betalingstjeneste-bedrageri kan opsummeres i følgende hovedlinjer:

Subsumtion: Online salgsbedrageri, hvor køberen frivilligt betaler i tillid til levering, er bedrageri efter [straffelovens § 279](#). Databedrageri efter [§ 279 a](#) kræver, at det er et elektronisk system – ikke en person – der manipuleres, typisk ved brug af stjålne kortoplysninger. De to bestemmelser kan begge være aktuelle i samme sagskompleks, fx ved telefonsvindel kombineret med efterfølgende misbrug af udleverede kort.

Strafniveau: Enkeltstående onlinebedrageri for mindre beløb medfører typisk betinget fængsel i 14 dage. Systematisk bedrageri med mange forurettede og beløb i hundredtusinde-klassen udmåles til fængsel i 1-2 år, som kan gøres betinget med samfundstjeneste for ustraffede gerningsmænd. Grov og professionel svindel mod sårbare ofre kan medføre ubetinget fængsel i op til 1 år og 9 måneder eller mere, med mulighed for udvisning af ikke-danske statsborgere.

Hvidvask: MobilePay bruges som kanal for hvidvask af svindeludbytte. Domstolene stiller ikke høje krav til forsætsbevisbyrden, når modtageren får overført et uventet beløb fra en ukendt person – beløbets afvigelse fra det aftalte indikerer i sig selv viden om den ulovlige oprindelse.

Civilretlig hæftelse: Ofre for MobilePay-misbrug kan kræve tabet dækket af deres betalingsudbyder (bank) efter [betalingslovens § 100](#), men selvrisiko på op til 8.000 kr. kan pålægges ved groft uforsvarlig adfærd, herunder udlevering af NemID/MitID-oplysninger. Kravet forældes tre år fra transaktionens gennemførelse.

Bevistemaer: Kernen i mange sager er forsætsspørgsmålet – havde tiltalte den fornødne vilje til berigelse på transaktionstidspunktet? Domstolene lægger vægt på tiltaltes adfærd efter betalingen (kontaktundvigelse, afvisning af at levere eller tilbagebetale), tidligere bedrageridømme og den samlede omstændigheder ved transaktionsforløbet.

LOV	Betalingsloven § 100	Straffeloven § 279	Straffeloven § 279a
	Straffeloven § 290a, stk. 1		

REFERENCE Lovgrundlag

6 paragraffer

[Betalingsloven § 100](#)

Straffeloven § 279		Straffeloven § 279a	
Straffeloven § 285	stk. 1	Straffeloven § 286	stk. 2
Straffeloven § 290a	stk. 1		

MATERIALE Citerede afgørelser 18 afgørelser

HØJESTERET · ØVERSTE INSTANS 2

15.05.2025	Højesteret fastlægger retningslinjer for tilståelsesrabat under den nye straffelov § 82, nr. 9, i sag om omfattende narkotika, databedrageri og hæleri	AM2025.05.15H
28.06.2023	Højesterets vurdering af varetægtsfængsling ved omfattende databedrageri og påvirkningsrisiko	AM2023.06.28H

LANDSRET TEN · ANKEINSTANS 7

11.04.2025	Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold)	S-0009-25
02.04.2025	Stadfæstelse af dom for hvidvask via MobilePay: Tiltalte modtog 17.000 kr. fra ukendt kilde efter aftale med veninde	S-0234-24
04.12.2024	Bedrageri og Identitetsmisbrug: Ubetinget fængsel for salg af ikke-eksisterende varer på Facebook Marketplace	S-1647-24
31.01.2023	Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn	S-0930-22
13.12.2021	Dom for omfattende bedrageri begået via DBA og NemID-svindel: Landsretten ændrer delvist ubetinget fængsel til betinget straf med samfundstjeneste	S-2725-19
09.03.2021	Bedrageri ved salg af mobiltelefon via DBA - Betaling modtaget, men vare aldrig leveret	S-2932-20
21.02.2018	Databedrageri og medvirken til omfattende misbrug af stjålne kreditkort via MobilePay – Frifindelse for medvirkende kontoindehaver	S-1842-17

BYRET TEN · FØRSTE INSTANS 5

10.07.2025	Omfattende sag om systematisk bedrageri, identitetsmisbrug og tyveri fører til fængselsstraffe	9965-11659
11.03.2024	Betinget fængselsstraf for fem forhold af hvidvask via MobilePay	5932-7086
16.11.2023	Fængsel for gentagen massiv afpresning, bedrageri og databedrageri samt gentagne færdselslovsovertrædelser	RAFD-3300/2023
04.10.2023	Dom for bedrageri og chikane: Fængselsstraf og erstatningskrav	4316-5172
13.03.2023	Anbringelsesdom for omfattende internetbedrageri, vidnetrusler og forsøg på ulovlig tvang	4723-5689

DET FINANSIELLE ANKENÆVN · NÆVN / KLAGEINSTANS 3

31.10.2025	58/2025: Afvisning af sag om MobilePay-misbrug på 80.000 kr. grundet behov for bevisførelse om MitID-godkendelse	58/2025
21.02.2023	Afvisning af sag om misbrug via Apple Pay og MobilePay grundet behov for bevisførelse	238/2022
19.04.2022	Spørgsmål om forældelse af indsigelse mod uautoriserede MobilePay-transaktioner foretaget af tidligere samlever	280/2021
PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS		1
07.12.2021	Kontrolafgift opretholdt for uaflæselig p-skive dækket af logo	park-5172

13

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over obligatorisk digital post, fritagelse og MitID-forvaltning

Fremkomsttidspunkt, risikofordeling og forvaltningen af den digitale adgangsnøgle

Version 2 · Opdateret 21. jul. 2026 · 36 afgørelser · 2013-2026

[Læs online](#)**INTRODUKTION**

Obligatorisk Digital Post og MitID udgør tilsammen den infrastruktur, som næsten al kommunikation mellem det offentlige og borgeren i dag hviler på. Retsvirkningen er skarp: en meddelelse anses for kommet frem, når den er tilgængelig i postløsningen – herunder i en visningsklient – uanset om borgeren har læst den, jf. [lov om Digital Post fra offentlige afsendere § 10](#). Praksis fra Ankestyrelsen, Folketingets Ombudsmand, domstolene og en lang række klagenævn viser et konsekvent mønster: borgeren bærer risikoen for sit eget udstyr, sine koder og sin manglende kontrol af postkassen, mens myndigheden bærer risikoen for driftsforstyrrelser i postløsningen og visningsklienten – og skal kunne dokumentere fremkomsten med forsendelseslog, når modtagelsen bestrides.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 En meddelelse i Digital Post anses for kommet frem, når den er tilgængelig for adressaten i postløsningen, herunder i en visningsklient – kundskab om indholdet er uden betydning.
- 02 Fremkomstreglen svarer efter forarbejderne præcist til, at et papirbrev anses for kommet frem, når det er lagt i adressatens fysiske postkasse.
- 03 Retsvirkningen er den samme, uanset om borgeren tilgår posten i en offentlig visningsklient (borger.dk, Virk) eller i en kommerciel visningsklient (e-Boks, mit.dk).
- 04 Borgeren bærer risikoen for egen internetforbindelse, eget udstyr, mistede koder og manglende opsætning af den valgte kommercielle visningsklient til at vise offentlig post.
- 05 Myndigheden bærer risikoen for driftsforstyrrelser i selve postløsningen eller i visningsklienten; meddelelsen anses da først for kommet frem, når hindringen er ophørt.
- 06 Bestrider borgeren modtagelsen, skal myndigheden kunne dokumentere fremkomsten – typisk ved forsendelseslog der viser levering, ikke blot afsendelse.
- 07 Kommunen har efter Ankestyrelsens principmeddelelse 33-23 en selvstændig undersøgelsespligt for, om driftsforstyrrelser i visningsklienten har afskåret borgeren fra at læse meddelelsen.

- 08** Klagefristen for digitale meddelelser regnes fra den dag, meddelelsen blev tilgængelig – uanset klokkeslæt, og også når det er en lørdag eller helligdag.
- 09** Klagenævnene anvender en restriktiv praksis: at have glemt eller ikke kunnet tjekke sin e-Boks er ikke en "særlig grund" til at se bort fra en fristoverskridelse, når borgeren ikke har søgt fritagelse.
- 10** God forvaltningsskik forpligter ikke myndigheden til at kontrollere, om borgeren har læst sin digitale post, før der sendes rykker eller administrativt bødeforelæg.
- 11** Skifter myndigheden kommunikationsform fra fysisk post til Digital Post, indtræder en særlig vejledningspligt efter forvaltningslovens § 7 – orienteringen kan ikke gyldigt gives alene digitalt.
- 12** Fritagelse efter § 5, stk. 1, træffes af kommunalbestyrelsen ved personligt fremmøde efter ni objektive fritagelsesgrunde, gælder tidsubegrænset og kan ikke indbringes for anden administrativ myndighed.
- 13** Kommunen skal før fritagelse konkret vurdere, om hjælp og vejledning kan sætte borgeren i stand til selv at tilgå posten – og kan alternativt tildele læseadgang eller fuld adgang til en pårørende.
- 14** Fritagelse fra Digital Post giver efter lov om fravigelse fra obligatorisk digital selvbetjening § 2 et objektivet, ubetinget krav på det hjemlede alternativ til enhver obligatorisk selvbetjeningsløsning – men først efter anmodning og inden for den relevante frist.
- 15** Afslag på udstedelse af MitID og myndighedsbestemt spærring eller suspension er forvaltningsretlige afgørelser med begrundelses-, vejlednings- og klageadgang; klage indgives til Digitaliseringsstyrelsen efter genvurdering hos registreringsenheden.
- 16** Myndigheder har pligt til at hjælpe borgere uden MitID til at agere inden for myndighedens område og give dem adgang til samme service som MitID-indehavere.
- 17** Tilknytning af privat MitID til en erhvervsidentitet hviler på et dobbelt frivillighedsprincip – både erhvervsbrugeren og brugerorganisationen skal acceptere det.
- 18** Digital forkyndelse og digitalt fremsendte processkrifter kan efter omstændighederne ikke sidestilles med samtykke til digital kommunikation i retsplejelovens forstand.

Retsgrundlaget: obligatorisk tilslutning, frivillig binding og fremkomstreglen

§ 1

Digital Post hviler på en enkel konstruktion med tre led: en tilslutningspligt, en fritagelsesadgang og en fremkomstregel.

Efter § 3, stk. 1 skal fysiske personer på 15 år eller derover med bopæl eller fast ophold i Danmark tilsluttes Digital Post, medmindre de fritages efter § 5, stk. 1 og 3. Juridiske enheder med cvr-nummer tilsluttes efter § 3, stk. 2. Flytter en tilsluttet person ud af landet, fortsætter tilslutningen uændret, medmindre den pågældende aktivt anmoder om fritagelse, jf. § 3, stk. 4 – et forhold der har fået afgørende betydning i praksis.

Den, der én gang er fritaget, kan efter [§ 4, stk. 1](#) frivilligt tilslutte sig igen med de retsvirkninger, der følger af § 10, og er da **bundet af tilslutningen**, indtil der på ny meddeles fritagelse. Det samme gælder efter [§ 4, stk. 2](#) for personer uden bopæl i Danmark, der frivilligt tilslutter sig.

Offentlige afsendere kan efter [§ 7, stk. 1](#) anvende Digital Post til kommunikation med tilsluttede personer og enheder – og bestemmelsen præciserer udtrykkeligt, at kommunikation omfatter "afsendelse af alle dokumenter og meddelelser m.v., herunder afgørelser". Omvendt har borgere og virksomheder efter [§ 8](#) en **ret** til at anvende postløsningen over for offentlige afsendere. Den ret er ikke symbolsk: Folketingets Ombudsmand fastslog i [FOB 2018-1](#), at det er myndighedens eget ansvar at sikre, at dens it-løsninger kan modtage og håndtere henvendelser sendt via Digital Post, og i [FOB 2015-21](#) behandledes tilsvarende, om kapaciteten i myndighedernes digitale postkasse reelt understøtter denne ret.

Selve kernebestemmelsen er [§ 10](#):

Meddelelser, der sendes under anvendelse af Digital Post, anses for

- 1. at være kommet frem på det tidspunkt, hvor meddelelsen er tilgængelig for adressaten i postløsningen, herunder i en visningsklient, og*
- 2. at være afsendt af den angivne afsender.*

Ordene "herunder i en visningsklient" blev indsat ved **lov nr. 1941 af 15. december 2020** med virkning fra 1. januar 2021, samtidig med at der i [§ 10 a](#) og [§ 10 b](#) blev skabt hjemmel til henholdsvis offentlige og kommercielle visningsklienter. Nummer 2 om autenticitet har den praktiske konsekvens, at modtageren – herunder en myndighed – ikke er forpligtet til på anden måde at sikre sig den angivne afsenders identitet.

Endelig blev der ved en ændringslov af 15. november 2021 indsat en [§ 10 d](#), der giver finansministeren hjemmel til at indføre en omstillingsperiode med ændret, begrænset eller indstillet adgang ved leverandørskift eller systemovergange. Bestemmelsen er trådt i kraft, men er endnu ikke konsolideret ind i lovbekendtgørelsen. Af forarbejderne fremgår udtrykkeligt, at fremkomstreglen ikke fraviges: problemer knyttet til postløsningen, som adressaten ikke har indflydelse på, medfører fortsat, at meddelelsen ikke anses for kommet frem, før forhindringen er ophørt.

LOV

[Lov om Digital Post fra offentlige afsendere § 3, stk. 1](#)[Lov om Digital Post fra offentlige afsendere § 4, stk. 1, 2](#)[Lov om Digital Post fra offentlige afsendere § 7, stk. 1](#)[Lov om Digital Post fra offentlige afsendere § 8](#)[Lov om Digital Post fra offentlige afsendere § 10](#)

Forarbejderne til § 10: papirbrevet i den fysiske postkasse som § 2 fortolkningsanker

Fremkomstreglen kan ikke forstås uden sine forarbejder, der er usædvanligt udførlige. Til den oprindelige bestemmelse i lov nr. 528 af 11. juni 2012 om Offentlig Digital Post anførte lovgiver:

Bestemmelsen i nr. 1 er lovforslagets centrale bestemmelse, der indebærer, at en meddelelse, som sendes i Offentlig Digital Post efter §§ 7 og 8, anses for at være kommet frem til adressaten, når meddelelsen er tilgængelig for

adressaten i Offentlig Digital Post. [...] Dette svarer til, at et papirbrev anses for at være kommet frem, når det pågældende brev er lagt i adressatens fysiske postkasse.

Parallellen til papirbrevet er ikke retorisk pynt. Den bærer hele retsvirkningslæren: forvaltningsakter får de tilsigtede retsvirkninger, når de er kommet frem til adressaten, og det er som udgangspunkt uden betydning, om afgørelsen er kommet til adressatens **kundskab**. Forarbejderne henviser her direkte til Højesterets dom af 9. marts 1989 (**UFR 1989.442/2H**) om tilbudspligt og til ombudsmandens udtalelse i **FOB 2000.320** om, at manglende meddelelse af en afgørelse som udgangspunkt medfører ugyldighed.

Tilgængelighedskriteriet er defineret teknisk-funktionelt:

En meddelelse, der sendes i Offentlig Digital Post, er tilgængelig, når adressaten vil kunne fremkalde meddelelsen på en almindeligt fungerende computer tilsluttet internettet med almindeligt tilgængelige programmer og dermed gøre sig bekendt med meddelelsens indhold.

Derefter følger den passus, der i praksis er blevet den mest citerede:

Det er uden betydning, om adressaten har bragt sig i stand til at logge sig ind i Offentlig Digital Post, herunder om den pågældende har skaffet sig den fornødne offentlige digitale signatur [...] Adressaten bærer således risikoen ved ikke at gøre sig bekendt med indholdet af post i vedkommendes digitale postkasse.

Forarbejderne præciserer samtidig, at reglen ikke ændrer på, **hvornår** en fremkomst er rettidig ved fristberegning – det afgøres fortsat efter de hidtidige principper – og at brug af anbefalet brev eller afleveringsattest, hvor lovgivningen foreskriver det, ikke berøres. Afsenderen må derfor selv vurdere, om Digital Post er en tilstrækkelig fremsendelsesform i den konkrete sag.

Det retspolitiske udgangspunkt for hele denne konstruktion blev lagt i [betænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen](#). Udvalget gennemgik ca. 500 formkravsregler på fire ministerområder og anbefalede en hjemmel i forvaltningsloven til at tillade digital kommunikation **til** myndighederne – men afstod udtrykkeligt fra at foreslå en generel pligt for borgere til at modtage digitale meddelelser **fra** det offentlige på grund af retssikkerhedsmæssige betænkeligheder. Netop det skridt tog lovgiver først med Digital Post-loven i 2012. Udvalgets efterfølgende arbejde i [betænkning nr. 1456/2004 om e-signaturs retsvirkninger](#) og [betænkning nr. 1517/2010 om elektronisk aftaleindgåelse og handel](#) behandlede samme grundproblem – fremkomst- og kundskabstidspunktet ved digitale meddelelser – ud fra et ækvivalens- og teknologineutralitetsprincip.

LOV

[Lov om Digital Post fra offentlige afsendere § 10](#)

Risikofordelingen mellem postløsning, visningsklient og borgerens eget udstyr

Med indførelsen af visningsklienter i 2021 blev risikofordelingen udbygget. Af forarbejderne til **lov nr. 1941 af 15. december 2020** fremgår:

Med den foreslåede ændring videreføres gældende ret. Adressatens retsstilling er den samme uanset om denne tilgår sin digitale post fra offentlige afsendere i en offentlig visningsklient eller i en kommerciel visningsklient. Retsvirkningen for borgeren eller virksomheden er dermed uafhængig af typen af visningsklient, der anvendes. Ved problemer knyttet til postløsningen, som adressaten ikke har indflydelse på (sammenbrud, midlertidig

kapacitetsnedgang m.v.), der indebærer, at en meddelelse ikke er eller kan blive tilgængelig for adressaten, kan en meddelelse til en borger eller virksomhed ikke anses for at være kommet frem, før forhindringen er ophørt.

Omvendt gælder:

Lovforslaget ændrer ikke retsstillingen i de tilfælde, hvor adressaten oplever, at vedkommendes egen internetforbindelse, computer, smartphone eller tablet ikke fungerer, eller at vedkommende har mistet adgang til sin kode til at logge på den digitale postløsning eller oplever lignende hindringer, som det er op til adressaten at overvinde.

Den autoritative udmøntning findes i Ankestyrelsens principmeddelelse [33-23](#), der behandlede tre sygedagpengesager om bortfald efter [sygedagpengelovens § 21, stk. 1, nr. 1](#). Ankestyrelsen fastslog:

Har driftsforstyrrelser påvirket den sygemeldtes mulighed for at tilgå kommunens meddelelser sendt som digital post, kan den sygemeldte have en rimelig grund til ikke at medvirke ved kommunens opfølgning.

Af [Beskæftigelsesministeriets vejledning om obligatorisk digital selvbetjening i sygedagpengesager, pkt. 4.1](#), der refererer principmeddelelsen ordret, fremgår sontringen skarpest:

Den sygemeldte er ikke forpligtet til at tilgå sin digitale post fra offentlige afsendere via en anden visningsklient, når den visningsklient, som den sygemeldte har valgt, er nede eller ude af drift. [...] Den sygemeldte er derimod nærmest til at bære risikoen for hindringen i situationer, hvor eksempelvis den sygemeldtes egen internetforbindelse, computer, smartphone eller tablet ikke fungerer, eller den sygemeldte har mistet adgang til sin kode til at logge på den digitale postløsning.

Og helt konkret om opsætningsfejl i den kommercielle klient:

Det betyder, at hvis den sygemeldte har valgt at benytte en kommerciel visningsklient, men ikke har opsat denne til, at der fortsat kan vises post fra offentlige afsendere, bærer den sygemeldte risikoen for, at pågældende ikke kan gøre sig bekendt med indholdet af den digitale post.

De tre sager i 33-23 illustrerer mønstret præcist: **sag 1** (borger havde ikke opsat sin e-Boks til offentlig post) – bortfald stadfæstet; **sag 3** (kommunen havde undersøgt og udelukket driftsforstyrrelser) – bortfald stadfæstet; **sag 2** (kommunen havde ikke undersøgt, om driftsproblemer i visningsklienten havde afskåret borgeren) – hjemvist.

Et beslægtet princip ses uden for Digital Post-loven i Højesterets kendelse i [BS-42968/2019-HJR](#), hvor et kæreskrift undtagelsesvis kunne anses for gyldigt indgivet pr. e-mail, fordi Domstolsstyrelsens sagsportal på grund af en systemhindring var utilgængelig for advokatkontorets medarbejdere på kærefristens sidste dag:

Det må imidlertid efter de oplysninger, der er fremkommet for Højesteret, anses for godtgjort, at det var særlige tekniske problemer, der forhindrede, at kæreskriftet kunne indgives på sagsportalen den 26. marts 2019 [...] finder Højesteret, at kæreskriftet helt undtagelsesvis kan anses for gyldigt indgivet ved mailen af 26. marts 2019.

Dommen understøtter den grundtanke, at systemfejl på myndighedssiden ikke må komme borgeren til skade – men også, at der skal være tale om en dokumenteret objektiv barriere, ikke blot en påstand.

LOV

[Lov om Digital Post fra offentlige afsendere § 10](#)

[Sygedagpengeloven § 21, stk. 1](#)

PRAKSIS

Højesteret · Kæreskrift indgivet pr. mail pga. tekniske fejl på sagsportalen anset for gyldigt

11.02.2020

Ankestyrelsen · Sygedagpenge – Bortfald ved manglende medvirken i digital post; risikofordeling ved brug af visningsklienter og kommunens undersøgelsespligt

01.01.2023

Myndighedens bevisbyrde: forsendelseslog og undersøgelsespligt når modtagelsen bestrides

Fremkomstreglen fritager ikke myndigheden for at bevise, at meddelelsen faktisk **nåede** postløsningen. Ankestyrelsen fastlagde dokumentationskravet principielt i [26-16](#), der samlede to sygedagpengesager om udeblivelse fra opfølgningssamtaler. Myndigheden bærer bevisbyrden, og beviset kan føres som **systembevis** ved forsendelseslog:

Det er ikke tilstrækkeligt, at dokumentationen alene viser, at brevet er afsendt; den skal bekræfte, at brevet faktisk er leveret til modtagerens digitale postkasse.

Udfaldet fulgte dokumentationen: I den ene sag kunne kommunen trods forespørgsler hos både egen it-afdeling og systemleverandøren ikke fremlægge forsendelsesloggen, og Ankestyrelsen ændrede afgørelsen, fordi det så måtte lægges til grund, at brevet aldrig var kommet frem. I den anden sag forelå en log, der dokumenterede levering "med succes", og bortfaldet blev stadfæstet.

Ankestyrelsen skærpede kravet i [33-23](#) med henvisning til undersøgelsespligten i [retssikkerhedslovens § 10](#):

Kommunen skal kunne dokumentere, at en meddelelse afsendt via den digitale postløsning (Digital Post) er kommet frem til selve postløsningen. Dette kan kommunen gøre ved at fremlægge den forsendelseslog, som knytter sig til den konkrete meddelelse.

Og videre: kommunen skal i **tillæg** til forsendelsesloggen undersøge, om driftsforstyrrelser i den valgte visningsklient har afskåret borgeren fra at tilgå meddelelsen, før der kan træffes afgørelse om bortfald.

Samme bevistema optræder på skatteområdet. I [19-0045533](#) kunne Skattestyrelsen oprindeligt ikke fremlægge en kopi af den konkrete afgørelse om foreløbig momsfastsættelse, men fremskaffede via e-Boks' afsendersupport dokumentation for, at forsendelsen var gjort tilgængelig i virksomhedens e-Boks den 2. april 2015. Landsskatteretten fandt det herefter bevist, at afgørelsen var kommet frem, jf. § 10, at kundskabstidspunktet dermed lå i 2015, og at 6-månedersfristen i [skatteforvaltningslovens § 32, stk. 2](#) var overskredet ved anmodningen i november 2018.

Ankestyrelsens administrative praksis for fristberegning er beskrevet i [Retssikkerhedsvejledningen, pkt. 267](#): digital post antages modtaget samme dag, men "[h]vis du oplyser, at det digitale brev først er kommet til din digitale postkasse senere, undersøger vi det [...]" ved at bede myndigheden dokumentere de digitale registreringer for brevet." I principmeddelelse [7-21](#) har Ankestyrelsen tilsvarende taget stilling til udløbstidspunktet for anmeldelsesfrister ved henholdsvis fysisk og digital post efter [arbejdsskadesikringslovens § 36, stk. 1](#).

LOV [Lov om Digital Post fra offentlige afsendere § 10](#)

[Lov om retssikkerhed og administration på det sociale område § 10](#)

[Skatteforvaltningsloven § 32, stk. 2](#)

PRAKSIS	Landsskatteretten · Afslag på ekstraordinær genoptagelse af momstilsvare vedrørende foreløbig fastsættelse modtaget i e-Boks	03.05.2023
	Ankestyrelsen · Sygedagpenge – Bortfald ved manglende medvirken i digital post; risikofordeling ved brug af visningsklienter og kommunens undersøgelsespligt	01.01.2023
	Ankestyrelsen · Anmeldelsesfrist for arbejdsskadesager: Udløbstidspunkt for fysisk og digital post	01.01.2021
	Ankestyrelsen · Dokumentationskrav for digital post: Myndighedens bevisbyrde for levering i borgernes digitale postkasse	01.01.2016

§ 5 Klagefristens begyndelsestidspunkt ved digitale meddelelser

Justitsministeriets [vejledning om beregning af klagefrister](#) – senest opdateret 3. marts 2026 – indeholder den samlede administrative retningslinje. Om digitale meddelelser hedder det i [pkt. 3.2](#):

En klagefrist bør for så vidt angår digitale meddelelser regnes fra den dato, hvor meddelelsen er tilgængelig for modtageren i postløsningen, uanset hvilket tidspunkt på døgnet, meddelelsen modtages.

Ovenstående gælder også i de tilfælde, hvor en afgørelse måtte gøres tilgængelig en dag, der ikke er en arbejdsdag. Klagefristens begyndelsestidspunkt kan således være en lørdag eller en helligdag, hvis afgørelsen er tilgængelig for modtageren på dette tidspunkt.

Dette har direkte konsekvenser i nævnspraksis. Planklagenævnet afviste i [19/03357](#) en klage over et lovliggørelsespåbud, der var sendt i Digital Post fredag den 14. december 2018 kl. 16.04. Klageren gjorde gældende, at afgørelsen – modtaget efter kontortids ophør – først burde anses for modtaget mandag den 17. december. Nævnet afviste dette: fristen løb fra den 14. december "uanset tidspunktet på dagen", og klagen indgivet 14. januar 2019 var tre dage for sen. Juleferie var ikke en undskyldelig omstændighed, navnlig fordi klagerens repræsentant den 8. januar – altså inden fristens udløb – var vejledt korrekt om at indgive en ny klage.

Vejddirektoratet anlagde samme linje i [EMN-2024-621376](#) under henvisning til netop klagefristvejledningen. Afgørelsen var tilgængelig i e-Boks fredag den 18. oktober 2024; fristen på fire uger udløb fredag den 15. november – ikke dagen efter, og ikke forlænget til førstkommande hverdag, da den 15. november var en almindelig hverdag. Klagen modtaget 17. november var for sen.

En særlig variant ses i Udlændingenævnets afgørelse [W20250952925](#), hvor en udvisningsafgørelse blev leveret digitalt via løsningen "filkassen" med et e-mail-link. Nævnet fastslog, at fristen efter [udlændingelovens § 46 a, stk. 3](#) løb fra det øjeblik, linket blev sendt og dokumentet dermed var tilgængeligt. Klagen var tre dage for sen, og der var ikke anført nogen begrundelse, der kunne begrunde dispensation.

Endelig fastslog Natur- og Miljøklagenævnet i [NMK-33-03220](#) to punkter af generel rækkevidde: adressaten kan ikke udskyde klagefristens udløb ved at undlade at kontrollere sin e-Boks, og kommunen kan ikke forlænge fristen ved efterfølgende at eftersende afgørelsen på anden vis. Grundejerforeningen havde ikke modtaget advisering, fordi kommunens øvrige post gik til formandens personlige e-mail – men fristen løb fra den dag, afgørelsen var tilgængelig i foreningens e-Boks.

LOV

[Lov om Digital Post fra offentlige afsendere § 10](#)
[Planloven § 58, stk. 1](#)
[Udlændingeloven § 46a, stk. 3](#)

PRAKSIS	Planklagenævnet · Afvisning af klage over påbud om lovliggørelse af kvist på grund af overskredet klagefrist	09.05.2019
	Planklagenævnet · Natur- og Miljøklagenævnets afvisning af realitetsbehandling i sag om gyldighed af byplanvedtægt grundet overskredet klagefrist	10.11.2015
	Udlændingenævnet · Afvisning af klage over udvisning grundet overskridelse af klagefrist ved digital forkyndelse	20.06.2025
	Vejddirektoratet · Afvisning af klage over vejvedligeholdelse grundet overskredet klagefrist	20.11.2024

§ 6 Nævnenes restriktive dispensationspraksis: "jeg fik ikke tjekket min e-Boks" er ikke en særlig grund

På tværs af klagenævn og tilsyn er billedet påfaldende ensartet. Manglende kontrol af den digitale postkasse – uanset årsag – anerkendes stort set aldrig som en undskyldelig omstændighed, når borgeren ikke har søgt fritagelse.

Vejdirektoratet har den tydeligste linje. I [21-02975](#) havde en borger begrundet den forsinkede klage med sygdom, der medførte, at hun sjældent tjekkede sin e-Boks. Direktoratet konstaterede, at borgeren var tilsluttet Digital Post, ikke havde søgt om fritagelse – skønt sygdom netop kunne udgøre en fritagelsesgrund – og var bevidst om, at sygdommen forhindrede hyppig kontrol. Genoptagelse blev afvist. I [EMN-2025-11047](#) var begrundelsen, at klageren havde glemt at tjekke sin e-Boks:

Vi må lægge til grund, at på baggrund af det oplyste i sagen, er der ikke tale om forhold af et sådant omfang, at det ikke har været muligt for dig at tjekke din e-Boks og overholde klagefristen.

Tilsvarende i [20-00687](#) (påbud i e-Boks, ingen særlige grunde anført), [23-15241](#) (forvirring om e-Boks ikke en særlig grund) og [EMN-2026-11265](#), hvor klageren aktivt havde valgt at korrespondere videre med kommunen frem for at klage rettidigt – en omstændighed der talte **imod** dispensation.

Planklagenævnet afviste i [20/11016](#) en klage, hvor advokaten netop havde anført, at klienten havde svært ved at anvende e-Boks, og at kommunen var bekendt hermed. Nævnet lagde vægt på, at afgørelsen var korrekt meddelt via Digital Post, at **klageren ikke var fritaget**, at klagevejledningen var korrekt, og at en aktindsigtsanmodning ikke suspenderer klagefristen. I [21/13508](#) afslog nævnet genoptagelse af en sag, hvor klagegebyret var betalt for sent, fordi klageren ikke havde tjekket e-Boks under ferie – og understregede, at det er adressatens ansvar at gøre sig bekendt med indholdet, jf. § 10. Se også [21/04751](#) (én dags overskridelse, ingen dispensation) og [24/06060](#) (ligeledes én dag).

Erhvervsankenævnet har anvendt samme princip i afgiftssager efter årsregnskabsloven. I [2015-8794](#) fastholdt nævnet afgifter på 2.000 kr. pr. bestyrelsesmedlem, selv om hele bestyrelsen påstod ikke at have modtaget påkravsbrevet – Erhvervsstyrelsen fremlagde dokumentation fra eBoks A/S for levering, og det er ledelsens ansvar at tømme selskabets postkasse. I [2016-657](#) kunne end ikke en 90-årig direktørs fire rygoperationer og efterfølgende blodprop føre til fritagelse efter [årsregnskabslovens § 152, stk. 1](#), bl.a. fordi de alvorligste helbredsproblemer indtrådte efter fristens udløb, og fordi de øvrige bestyrelsesmedlemmer ikke var fritaget for deres tilsynspligt. Og i [21/00029](#) afviste nævnet en direktørs proportionalitetsindsigelse – han havde "blot overset det digitale brev" – med henvisning til § 10.

Landsskatteretten følger samme linje. I [22-0074112](#) havde et selskab undladt at opdatere sin e-mailadresse til notifikationer fra e-Boks og reagerede derfor hverken på forslag eller afgørelse:

Landsskatteretten har herved lagt vægt på, at de forhold, at selskabet ikke havde opdateret sin e-mail til modtagelse af notifikationer om modtagelse af breve i e-Boks, og at selskabet derfor ikke modtog besked om, at der i selskabets e-Boks var indgået breve fra Skattestyrelsen [...] ikke kan anses for sådanne særlige omstændigheder.

Udlændingenævnet afviste i **W20171009025** en klage indgivet 14 måneder for sent, hvor udlændingen anførte ikke at have haft adgang til sin e-Boks. Nævnet lagde vægt på den digitale pligt, på at styrelsen havde gjort opmærksom på at tjekke e-Boks og søge hjælp i kommunen, og på klagerens passivitet efter faktisk at have fået kendskab til afslaget. Se tilsvarende **W20190998125**.

Endelig har Rigsadvokaten i **AM2025.03.11RA** anvendt reglen over for en indsat under afsoning. Statsadvokatens afgørelse var sendt via Digital Post den 12. september 2024; klagefristen efter **retsplejelovens § 1018 e, stk. 5** udløb 10. oktober, og klagen kom 29. januar 2025:

Det påhviler således erstatningssøgende, som afsoner, at tjekke sin digitale post eller framelde sig Digital Post.

Bemærk, at bekendtgørelsen om forvaltning af Digital Post netop indeholder en særregel for denne gruppe: efter **§ 9, stk. 5** kan kriminalforsorgen indgive fritagelsesansøgning på vegne af en person, der på grund af ophold i kriminalforsorgens institutioner ikke kan give personligt fremmøde.

LOV

Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 9, stk. 5

Lov om Digital Post fra offentlige afsendere § 10

Retsplejeloven § 1018e, stk. 5

Årsregnskabsloven § 152, stk. 1

PRAKSIS	Landsskatteretten · Afslag på genoptagelse af momstilsvær grundet overskredne frister og manglende tjek af e-Boks	22.11.2023
	Vejdirektoratet · Afvisning af klage over kommunalt beskæringspåbud – klagefrist overskredet (EMN-2026-11265)	21.04.2026
	Vejdirektoratet · Afvisning af klage over nedlæggelse af privat fællesvej på grund af overskredet klagefrist	17.03.2025
	Vejdirektoratet · Afvisning af klage over parasolopstilling: Forvirring om e-boks var ikke en 'særlig grund' til at se bort fra klagefrist	24.11.2023
	Vejdirektoratet · Afvisning af Genoptagelse: Manglende Tjek af e-Boks Grundet Sygdom Ikke Gyldig Grund for Overskredet Klagefrist	15.06.2021
	Vejdirektoratet · Klage over påbud om beskæring afvist på grund af overskredet klagefrist	29.01.2020
	Planklagenævnet · Planklagenævnets afvisning af klage over afslag på lovliggørende landzonetilladelse i Roskilde Kommune grundet fristoverskridelse	07.08.2024
	Planklagenævnet · Planklagenævnets afslag på genoptagelse af klagesag vedrørende dispensation i Herning	10.12.2021
	Planklagenævnet · Afvisning af klage over byggetilladelse grundet overskredet klagefrist	20.05.2021
	Planklagenævnet · Afvisning af klage over påbud om lovliggørelse på grund af overskredet klagefrist	16.12.2020
	Erhvervsankenævnet · Stadfæstelse af lukning for straksregistrering på virk.dk efter manglende dokumentation for ejerændringer	28.09.2021
	Erhvervsankenævnet · Stadfæstelse af ledelsesaftager for for sent indsendt årsrapport trods sygdom og manglende kendskab til Digital Post	14.09.2016
	Erhvervsankenævnet · Stadfæstelse af afgifter for for sent indsendt årsrapport trods påstand om manglende modtagelse af digitalt påkrav	08.02.2016
	Udlændingenævnet · Afvisning af for sent indgivet klage trods betegnelse som ankesag i korrespondance	13.11.2019
	Udlændingenævnet · Afvisning af klage over opholdstilladelse grundet overskredet klagefrist og udvisning med indrejseforbud	11.11.2017
	Rigsadvokaten · Ikke erstatning for mistet jakke under polititransport – Klage afvist grundet overskridelse af klagefrist	11.03.2025

Hvornår giver digitale barrierer alligevel dispensation? Grænserne for borgerens risiko

§ 7

Praksis er restriktiv, men ikke absolut. Der tegner sig tre situationstyper, hvor borgeren alligevel får medhold.

1. Myndigheden har skiftet kommunikationsform uden forudgående vejledning. Ankestyrelsens principmeddelelse [125-13](#) angik to enlige forsørgere, hvis børnetilskud blev standset, fordi de ikke havde bekræftet deres status. Udbetaling Danmark havde skiftet fra fysisk post til Digital Post – og havde givet besked om skiftet **udelukkende via Digital Post**. Ankestyrelsen anerkendte udgangspunktet, men fastslog:

Når en myndighed ændrer den måde, som borgeren er vant til at modtage post fra myndigheden på, så har myndigheden en særlig vejledningsforpligtelse, som betyder, at borgeren på forhånd bør orienteres om ændringen.

Hjemlen er [forvaltningslovens § 7, stk. 1](#). Da vejledningspligten ikke var opfyldt, var det undskyldeligt, at borgerne ikke havde nået fristen, og standsningen var uberettiget.

2. Borgeren er reelt digitalt afskåret, og fristoverskridelsen er minimal. Retten i Kolding tilsidesatte i [BS-27387/2022-KOL](#) en afgørelse fra Ankestyrelsen om sygedagpenge. Borgeren var digitalt uøvet og helt afhængig af sin hustru, der var rejst til Grønland for at pleje en alvorligt syg søster, netop i det vindue hvor kommunens digitale brev med otte dages frist lå i e-Boks. Han modtog ingen SMS-advisering, ansøgte to dage efter fristen – dagen efter hustruens hjemkomst – og blev efterfølgende fritaget for både digital selvbetjening og Digital Post. Retten udtalte:

Uanset Sagsøger ikke var fritaget for digital post og selvbetjening, da han overskred ansøgningsfristen, finder retten under de ovenfor anførte omstændigheder, herunder den meget beskedne fristoverskridelse, sammenhængen mellem sygedagpengelovens § 38, stk. 7, og § 69 a, stk. 2, og de hensyn der ligger bag bestemmelserne, samt efter en helhedsvurdering, at der har foreliget sådanne særlige undskyldende forhold, at betingelserne [...] var opfyldt.

Dommen er central, fordi den kobler dispensationsvurderingen efter [sygedagpengelovens § 38, stk. 7](#) sammen med fritagelseskriterierne i [§ 69 a, stk. 2](#): opfylder borgeren reelt betingelserne for fritagelse, kan det få betydning, selv om fritagelsen først meddeles bagefter. Tænketaenken Justitia indtrådte som biintervenient og fremhævede den gruppe borgere, der klarer sig via netværkshjælp og derfor aldrig har søgt fritagelse.

3. Klagen er indgivet rettidigt, men i forkert form. I [FOB 2020-24](#) henstillede ombudsmanden til Miljø- og Fødevareklagenævnet at genoptage en sag, hvor klageren havde klaget rettidigt til rette myndighed, men uden om den obligatoriske klageportal. Ombudsmanden fandt, at klagen måtte anses for rettidig, hvis klageren efter vejledning retter op på manglen – også selv om klagefristen imens er sprunget.

Modsat viser [BS-7833/2022-KBH](#), hvor sagsøgeren var frtaget sit danske statsborgerskab og først anlagde sag ni måneder efter fristen, fordi hans NemID-nøglekort var udløbet, mens han opholdt sig i Tyrkiet. Retten citerede forarbejderne til [indfødsretslovens § 8 F](#):

at det ikke vil være et undskyldeligt forhold, at parten har bragt sig selv i en situation, hvor det ikke er muligt for vedkommende at tilgå sin e-boks eller læse Statstidende.

Retten lagde vægt på, at sagsøgeren – registreret som udrejst – kunne have anmodet om fritagelse efter § 3, stk. 4, jf. § 5, stk. 1, og at han kunne have bestilt NemID online og afhentet en midlertidig adgangskode på en af de mange danske repræsentationer i Tyrkiet. Hverken EMRK artikel 6 eller grundlovens § 63 kunne føre til et andet resultat.

Grænsen mellem type 2 og den afviste sag er reel: den udslagsgivende faktor er, om borgeren **selv** har bragt sig i den digitale afskærelse, og om fristoverskridelsen er beskeden og efterfulgt af prompte reaktion.

LOV

Forvaltningsloven § 7, stk. 1

Lov om Digital Post fra offentlige afsendere § 3, stk. 4

Sygedagpengeloven § 38, stk. 7

Sygedagpengeloven § 69a, stk. 2

PRAKSIS	Byretten · Afgørelse om dispensation for fristoverskridelse ved ansøgning om sygedagpenge grundet manglende digitale kompetencer	11.10.2023
	Byretten · Afvisning af søgsmål om fratagelse af dansk indfødsret på grund af overskredet søgsmålsfrist	27.03.2023
	Ankestyrelsen · Særlig vejledningspligt ved skift fra fysisk post til Digital Post om børnetilskud	01.01.2013

§ 8 Fritagelse efter § 5: kommunalbestyrelsens afgørelse, hjælpealternativet og den afskårne rekurs

Fritagelsesordningen er den ventil, hele systemet hviler på – og den er detaljeret reguleret.

Hjemlen er § 5, stk. 1, hvorefter finansministeren fastsætter regler om fritagelse, "hvor der foreligger særlige omstændigheder, som kan bevirke, at en person er hindret i at modtage sin post digitalt". Kompetencen ligger efter § 5, stk. 2 hos kommunalbestyrelsen i bopælskommunen – eller senest folkeregistrerede kommune. For erhvervsforhold og juridiske enheder ligger kompetencen hos erhvervsministeren, jf. § 5, stk. 3-5, og ministeren kan efter § 5, stk. 6 fastsætte, at sådanne afgørelser ikke kan indbringes for anden administrativ myndighed.

De materielle kriterier findes i § 7 i bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere, der opregner ni fritagelsesgrunde:

Nr.	Fritagelsesgrund
1	Kognitiv funktionsnedsættelse, der hindrer brug af Digital Post
2	Fysisk funktionsnedsættelse, der hindrer brug af Digital Post
3	Manglende adgang til computer, smartphone eller tablet i eget hjem/opholdssted
4	Registreret i CPR som udrejst af Danmark
5	Registreret uden fast bopæl i CPR, jf. CPR-lovens § 6, stk. 4
6	Sproglige barrierer (manglende beherskelse af dansk)
7	Praktiske vanskeligheder ved at skaffe et elektronisk id
8	Bopæl i område uden internetforbindelse med mindst 512 kbit/s download
9	Konkret vurdering, hvis der foreligger ganske særlige forhold

Proceduren er formbunden: anmodningen indgives ved **personligt fremmøde** i kommunen på den anviste blanket mod forevisning af gyldigt sundhedskort eller anden behørig legitimation, jf. § 8. Der kan gives fuldmagt,

jf. § 9, stk. 1-3, og for personer med varig svækkelse, der hverken kan møde op eller give fuldmagt, kan kommunalbestyrelsen efter § 9, stk. 4 træffe afgørelse på grundlag af kommunens eget kendskab til forholdene.

Afgørende er § 10, der indeholder tre elementer af forvaltningsretlig betydning:

- **Hjælpeforpligtelsen:** "Forinden afgørelse træffes, yder kommunalbestyrelsen efter konkret vurdering hjælp og vejledning med henblik på, at personen bliver i stand til at tilgå sin post i Digital Post i stedet for at blive fritaget." Fritagelse er altså subsidier i forhold til kompetenceopbygning.
- **Skriftlighed:** Afslag meddeles skriftligt.
- **Afskåret rekurs:** "[A]fgørelsen kan ikke indbringes for anden administrativ myndighed." Prøvelse må derfor ske ved domstolene eller – i praksis oftere – hos Folketingets Ombudsmand.

Fritagelse har virkning fra registreringsdatoen og gælder **tidsubegrænset**, jf. § 11. Efter § 12 skal kommunen oplyse om uåbnet post og på anmodning sørge for, at de seneste seks måneders uåbnede post sendes til folkeregisteradressen – men kommunen har ikke selv adgang til postkassen og kan derfor hverken oplyse omfang, indhold eller afsendere. Og efter § 13 modtager offentlige afsendere automatisk oplysning om, hvem der er tilsluttet; er en person ikke tilsluttet, **skal** afsenderen sørge for papirpost.

Et centralt alternativ til fritagelse er adgangstildeling efter § 16: ved personligt fremmøde kan borgeren tildele en anden fysisk person eller juridisk enhed enten **læseadgang** eller **fuld adgang** (læse, besvare og skrive) – op til ti adgange. Retsvirkningen berøres dog ikke: "Uanset at en fysisk person har tildelt adgang til en anden, anses meddelelser i Digital Post for at være kommet frem til den, der har tildelt adgang."

Ombudsmanden har i [FOB 2015-22](#) understreget, at postløsningen som sådan skal indrettes efter almindelige forvaltningsretlige krav. Han konstaterede, at det ikke i alle tilfælde var muligt at se, hvilken myndighed der var afsender, og fandt det ønskeligt, at myndighederne havde sikret sig dette **inden** den obligatoriske tilslutning trådte i kraft – bl.a. i lyset af [forvaltningslovens § 32 b](#) om entydig identifikation af afsenderen. Samme sag afklarede, at kommuner lovligt kan drive lokale postløsninger ved siden af Digital Post, men da skal vejlede tydeligt om, at samtykke hertil **ikke** fritager for at tjekke Digital Post.

LOV

[Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 7](#)[Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 10](#)[Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 16](#)[Forvaltningsloven § 32b, stk. 1](#)[Lov om Digital Post fra offentlige afsendere § 5, stk. 1-6](#)

Obligatorisk digital selvbetjening og loven om fravigelse (2023):

§ 9 fritagelse som objektivt kriterium

Digital Post og obligatorisk digital selvbetjening er to forskellige ordninger med forskellige fritagelsesmodeller – en asymmetri, som Digitaliseringsstyrelsen udførligt forsvarede over for ombudsmanden i [FOB 2017-19](#):

En borger kan således fritages generelt for Digital Post, fordi borgeren uopfordret og også uventet kan modtage breve fra det offentlige i sin digitale postkasse. [...] I forhold til obligatorisk digital selvbetjening er det derimod borgeren, der primært har behov for at kontakte offentlige myndigheder.

Styrelsen oplyste samtidig, at Folketinget den 12. maj 2015 forkastede et beslutningsforslag om at indføre en ensartet fritagelsesmodel.

Det blev delvist ændret ved [lov om fravigelse fra obligatorisk digital selvbetjening](#), der trådte i kraft 1. juni 2023. Loven gælder efter [§ 1](#) alle offentlige myndigheders obligatoriske digitale selvbetjeningsløsninger, hvor lovgivningen giver mulighed for at fravige udgangspunktet – dog ikke domstolenes digitale portaler. Kernebestemmelsen er [§ 2](#):

Fysiske personer, der er fritaget fra obligatorisk tilslutning til Digital Post efter regler udstedt i medfør af § 5, stk. 1, i lov om Digital Post fra offentlige afsendere, har efter anmodning ret til at benytte den pågældende lovgivnings hjemlede alternativ til den obligatoriske digitale selvbetjeningsløsning.

Fritagelse fra Digital Post er dermed blevet et **objektivt kriterium** på tværs af sektorlovenes selvbetjeningskrav: borgeren skal ikke længere godtgøre "særlige forhold" i hver enkelt sag. Beskæftigelsesministeriets [vejledning om obligatorisk digital selvbetjening i sygedagpengesager](#), pkt. 3.5 udtrykker det klart: borgeren "skal alene oplyse kommunen, at vedkommende vil fritages [...] Det er således ikke nødvendigt, at en borger yderligere begrundes, hvorfor vedkommende ikke vil anvende »Mit Sygefravær«."

To begrænsninger er dog væsentlige. For det første gælder fravigelsen kun **efter anmodning** og kun for det konkrete forløb – i modsætning til Digital Post-fritagelsen, der er generel og tidsubegrænset. For det andet skal anmodningen indgives inden for de gældende frister; har borgeren ikke anmodet rettidigt, kan fritagelsen fra Digital Post ikke efterfølgende bruges til at dispensere for en overskreden frist. Samme princip fremgår af [bekendtgørelse om obligatorisk digital selvbetjening vedrørende ansøgninger og meddelelser m.v. om sociale ydelser m.v. § 2](#).

Sektorlovene følger et fast mønster, som fx [vejlovens § 83](#), [børnelovens § 33 a](#) og [forældreansvarslovens § 31](#) illustrerer: obligatorisk digital selvbetjening → afvisning ved manglende brug → **skal** tilbyde alternativ ved "særlige forhold" → **kan** helt ekstraordinært undlade afvisning ved klare økonomiske fordele → digital henvendelse anses kommet frem, når den er tilgængelig for myndigheden.

Ombudsmanden har ad flere omgange sat forvaltningsretlige rammer om disse løsninger. I [FOB 2015-36](#) fastslog han, at der ikke er hjemmel til at kræve digital selvbetjening ved klage over parkeringsafgift, og at vejledning ikke må fremstå, som om en frivillig løsning er obligatorisk. I [FOB 2019-11](#) konstaterede han flere mangler i en kommunes selvbetjeningsløsning: uklarhed om hvad der var obligatorisk (kun [servicelovens § 112](#), ikke §§ 113 og 116), manglende vejledning om den ikke-digitale ansøgningsprocedure, og at løsningen utilsigtet afskar partsrepræsentation. Om vejledningsstedet udtalte han:

I tilfælde som det foreliggende, hvor der anvendes en digital selvbetjeningsløsning i forbindelse med ansøgninger om hjælp – og hvor der som følge heraf som udgangspunkt ikke er kontakt mellem borgeren og kommunen – bør vejledning om indholdet af den ikke-digitale ansøgningsprocedure efter min opfattelse ske på kommunens hjemmeside samt på borger.dk.

Partsrepræsentationsproblemet var allerede rejst i [FOB 2016-1](#), hvor Digitaliseringsstyrelsen bl.a. måtte implementere en systemændring, så meddelelser også kunne sendes til fuldmagtshavers digitale postkasse. Og i [FOB 2019-22](#) behandlede ombudsmanden det strukturelle problem, at ansvaret for vejledningen på borger.dk er delt mellem statslige, fælleskommunale og kommunale parter – med behov for klarhed over ansvaret og overordnet koordinering.

Finansministeriets vejledning om digitaliseringsklar lovgivning sammenfatter kravet til lovgiver: skal digital kommunikation være obligatorisk, kræver det lovhjemmel, og hjemlen bør være teknologineutral – og der skal fortsat tilbydes alternative løsninger til dem, der ikke kan kommunikere digitalt.

LOV

Lov om fravigelse fra obligatorisk digital selvbetjening § 1

Lov om fravigelse fra obligatorisk digital selvbetjening § 2, stk. 1, 2

Serviceloven § 112

Vejloven § 83, stk. 1-4

Fra NemID til MitID: FOB 2017-19 og hjemmelskritikken der udløste lovgivningen

§ 10

MitID-lovens tilblivelse er et af de tydeligste eksempler på, at en ombudsmandsudtalelse driver lovgivning frem.

I [FOB 2017-19](#) undersøgte ombudsmanden – efter henvendelse fra en kommunal borgerrådgiver – forvaltningen af NemID. Digitaliseringsstyrelsen måtte oplyse, at der "ikke [er] nogen lovregler, der regulerer NemID eller udstedelse heraf". Ordningen hvilede i stedet på en kontrakt med Nets DanID efter EU-udbud, på den styrelsejede OCES-standard og på individuelle RA-aftaler mellem hver enkelt kommune og Nets DanID. Kommunernes borgerservicecentre fungerede som registreringsenheder **på vegne af en privat virksomhed**, og styrelsens og kommunernes opfattelse var derfor, at afslag på NemID ikke var afgørelsesvirksomhed i forvaltningslovens forstand – bl.a. fordi borgere uden NemID "skal betjenes på anden vis af kommunerne".

Afslag blev meddelt **mundtligt** og blev ikke registreret. Klageadgangen var lige så uformel: klager skulle først rettes til Nets DanID, kunne videresendes til Digitaliseringsstyrelsen, hvis afgørelser efter almindelige forvaltningsretlige principper om ulovbestemt rekurs kunne indbringes for Finansministeriet.

Ombudsmanden tilsluttede sig styrelsens egen erkendelse af behovet for lovregulering og tilføjede den bærende betragtning:

NemID er således gået fra at være et tilbud om, at borgere, som ønskede det, i visse tilfælde kunne betjene sig af digitale løsninger, til at være praktisk talt afgørende for, at borgerne kan opnå en tidssvarende betjening i forhold til store dele af det offentlige, både for så vidt angår offentlig servicevirksomhed (faktisk forvaltningsvirksomhed) og for så vidt angår offentlig afgørelsesvirksomhed.

Han bemærkede desuden, at ordningen med at lade kommunerne fungere som registreringsenheder for en privat virksomhed "også rejser hjemmelsspørgsmål", og gik ud fra, at det kommende lovforslag udtrykkeligt ville forholde sig til, om opgavevaretagelsen er afgørelsesvirksomhed.

Ombudsmanden rejste samtidig spørgsmålet om den manglende **automatiske kobling**: hvorfor medfører et afslag på NemID – meddelt på det offentlige foranledning – ikke i sig selv fritagelse for Digital Post og obligatorisk digital selvbetjening? Digitaliseringsstyrelsen fastholdt, at en sådan kobling ikke var hensigtsmæssig, men henviste til, at problemstillingen ville blive inddraget i lovarbejdet, og pegede på det eksisterende alternativ: at borgerservice kan tildele læseadgang til en pårørende efter fritagelsesbekendtgørelsens regler om adgangstildeling.

Resultatet blev [lov om MitID og NemLog-in](#), der efter [§ 1](#) omfatter både MitID-løsningen (den danske nationale elektroniske identifikationsordning) og NemLog-in (den fællesoffentlige digitale infrastrukturløsning). [§ 2](#)

definerer bl.a. sikringsniveauerne – lav, betydelig og høj – og "sikker autentifikation" som niveau betydelig eller høj.

Disse niveauer er ikke danske opfindelser, men følger [eIDAS-forordningen](#) (forordning (EU) nr. 910/2014). Efter [artikel 8](#) skal en anmeldt elektronisk identifikationsordning angive sikringsniveauerne »lav«, »betydelig« og/eller »høj«, som defineres ved graden af tillid til en persons påståede identitet. Efter [artikel 6](#) skal et elektronisk identifikationsmiddel udstedt i én medlemsstat anerkendes i en anden ved adgang til offentlige onlinetjenester, når niveauet svarer til eller overstiger det krævede, og dette er »betydelig« eller »høj«. Den danske NSIS-standard implementerer denne ramme, og [MitID-bekendtgørelsen § 3, stk. 2](#) fastslår, at kravene til legitimationsdokumenter "skærpes i takt med, at graden af sikringsniveau øges, jf. NSIS".

LOV

[Bekendtgørelse om MitID til privatpersoner § 3, stk. 2](#)[Lov om MitID og NemLog-in § 1](#)[Lov om MitID og NemLog-in § 2](#)

MitID-forvaltningen: udstedelse, afslag, spærring og suspension som § 11 forvaltningsafgørelser

Efter [§ 3, stk. 1](#) stiller Digitaliseringsstyrelsen MitID-løsningen til rådighed og sikrer udvikling, drift og vedligeholdelse; efter [§ 3, stk. 2](#) stilles MitID til rådighed for privatpersoner og erhvervsbrugere, hvis betingelserne er opfyldt.

Selve forvaltningsopgaverne er samlet i [§ 4, stk. 1](#): identitetssikring, registrering samt udstedelse, suspension, spærring og genåbning – både for privatpersoner (nr. 1) og for erhvervsbrugeres identifikationsmidler (nr. 2). Ministeren for digitalisering fastsætter efter [§ 4, stk. 2](#) de nærmere regler, herunder om klageadgang til Digitaliseringsstyrelsen. Efter [§ 5](#) kan styrelsen udpege andre til at varetage opgaverne – og kommunalbestyrelsen **skal** varetage opgaver efter [§ 4, stk. 1](#). Hermed er den hjemmelsmangel, ombudsmanden pegede på i 2017, lukket.

Forarbejderne til [§ 4](#) er utvetydige om afgørelseskarakteren:

Et afslag på udstedelse af MitID indebærer en væsentlig begrænsning i indehaverens digitale færden og udgør en forvaltningsretlig afgørelse.

Herudover vil en spærring foretaget af andre end indehaveren selv, udgøre en forvaltningsretlig afgørelse.

Og om klagevejen:

Det forventes, at en afgørelse om afslag på udstedelse af MitID, spærring og suspension af MitID, efter genvurdering hos registreringsenheden, skal kunne indbringes for Digitaliseringsstyrelsen.

Dette er udmøntet i [bekendtgørelse om MitID til privatpersoner](#), hvis [§ 10](#) fastslår, at afgørelser efter bekendtgørelsen kan påklages til Digitaliseringsstyrelsen, og at styrelsen kan kræve enhver oplysning udleveret af registreringsenheder og supportorganisationer. Parallelt gælder [§ 7 i bekendtgørelsen om MitID Erhverv og MitID Privat til Erhverv](#). Endelig fastslår [lovens § 20](#) udtrykkeligt, at forvaltningsloven finder anvendelse på afgørelser om udstedelse, spærring og genåbning truffet af udpegede juridiske enheder – dvs. også af pengeinstitutter i deres rolle som registreringsenhed.

Afslagsgrundene er nu objektiverede i [MitID-bekendtgørelsens § 4, stk. 3 og 4](#): registreringsenheden skal give afslag, når privatpersonen ikke kan identificeres tilstrækkeligt, ved tvivl om legitimationsdokumentationens ægthed eller gyldighed, ved nægtelse af nødvendig registrering – og når enheden vurderer, at personen ikke er i stand til at forstå og overholde besiddelsesbetingelserne i [§ 8](#). Betingelserne er, at borgeren skal håndtere MitID sikkert og forsvarligt, beskytte identifikationsmidler og koder mod kompromittering, ikke videregive adgangskoder eller pinkoder, og selv spærre ved manglende efterlevelse.

Spærring og suspension reguleres i [§ 9](#). Suspension er midlertidig med automatisk genåbning ved periodens udløb; spærring er endelig og kræver ny udstedelse. Digitaliseringsstyrelsen, registreringsenheden eller supportorganisationen **skal** omgående suspendere ved mistanke om, at betingelserne ikke overholdes, eller ved mistanke om svindel – og **skal** omgående spærre ved mistanke om urigtige oplysninger eller falske legitimationsdokumenter ved udstedelsen, samt når indehaveren er erklæret forsvundet eller død. En værgе kan mod behørig dokumentation kræve spærring. Afgørende retssikkerhedsmæssigt er [§ 9, stk. 8](#): den enhed, der suspenderer eller spærre uden anmodning fra indehaveren, **skal orientere privatpersonen om årsagen**, når det er muligt.

Vejledningspligten er selvstændigt hjemlet i [§ 1, stk. 4](#): registreringsenheder skal på anmodning tilbyde vejledning om betingelser og vilkår, og "[o]mfanget af vejledningen skal forstås i overensstemmelse med forvaltningslovens § 7".

Erhvervssiden hviler på [§ 9](#): Digitaliseringsstyrelsen forvalter NemLog-in og kan spærre brugerorganisationers adgang til serviceområdet Erhvervsadministration. Efter [§ 9, stk. 3](#) kan en erhvervsbruger tilknytte det identifikationsmiddel, der hører til den private MitID-identitet, til sin erhvervsidentitet – men "[t]ilknytningen er frivillig for erhvervsbrugeren og frivillig for brugerorganisationen". Forarbejderne kalder dette det **dobbelte frivillighedsprincip**.

Endelig regulerer [§ 11](#) tjenesteudbydersiden: offentlige myndigheder og offentligretlige organer, der anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, **skal** anvende serviceområderne login/autentifikation (hvis sikker autentifikation kræves) og digital repræsentation – og skal anskaffe dem fra Digitaliseringsstyrelsen, jf. [§ 11, stk. 5](#), jf. [§ 6, stk. 1](#). Pligten til at tilbyde **digital repræsentation** er den lovgivningsmæssige besvarelse af det partsrepræsentationsproblem, ombudsmanden rejste i FOB 2016-1 og FOB 2019-11.

LOV

Bekendtgørelse om MitID til privatpersoner § 9

Bekendtgørelse om MitID til privatpersoner § 10

Lov om MitID og NemLog-in § 4, stk. 1, 2

Lov om MitID og NemLog-in § 9, stk. 1, 3, 4

Lov om MitID og NemLog-in § 11, stk. 1, 5

Lov om MitID og NemLog-in § 20, stk. 1, 2

§ 12 Myndighedens hjælpeforpligtelse over for borgere uden MitID

Et af de vigtigste punkter i MitID-lovens forarbejder besvarer netop den kobling, ombudsmanden efterlyste i FOB 2017-19. Lovgiver anerkender udtrykkeligt konsekvenserne af et afslag:

Det er således væsentligt, at en privatperson kan klage over et afslag på udstedelse, da et afslag kan have indgribende betydning for den persons digitale færden. Ligeledes er MitID en forudsætning for, at en privatperson kan tilgå

Digital Post og anvende offentlige digitale selvbetjeningsløsninger. Privatpersoner, som ikke kan få udstedt MitID, vil ikke kunne betjene sig hos en offentlig myndighed eller et offentligretligt organ via den fællesoffentlige adgang.

Og herefter den positive forpligtelse:

De enkelte myndigheder vil i den sammenhæng være forpligtet til at vejlede privatpersoner efter de forvaltningsretlige regler, hvilket blandt andet indebærer, at en myndighed har pligt til at vejlede og hjælpe privatpersoner inden for de ressortområder, som de er ansvarlige for. Således har en myndighed pligt til at hjælpe en privatperson, der fx ikke kan få udstedt MitID til at agere inden for myndighedens område og give privatpersonen adgang til de oplysninger og den offentlige service, som andre privatpersoner kan tilgå ved brug af MitID.

Denne forpligtelse har flere selvstændige forankringspunkter. Hjemlen er [forvaltningslovens § 7, stk. 1](#), men ombudsmanden har gentagne gange fremhævet, at vejledningspligten rækker videre. I [FOB 2019-22](#) formulerede han det således:

Det følger dog af almindelige retsgrundsætninger og god forvaltningsskik, at der også skal ydes vejledning uden for forvaltningslovens anvendelsesområde, herunder i forbindelse med faktisk forvaltningsvirksomhed. [...] Vejledningspligten gælder desuden i tilfælde, hvor en borger ikke selv har fremsat en anmodning om vejledning, men hvor det fremstår som naturligt og relevant at give borgeren information og vejledning i anledning af den sag, kontakten angår.

I [FOB 2025-19 om krav til myndigheders telefonbetjening](#) har ombudsmanden videreført denne linje ind i den digitale forvaltning: formålet med vejledningspligten er "at imødekomme borgernes informationsbehov og undgå, at borgerne på grund af fejl, uvidenhed eller misforståelser udsættes for retstab", og vejledningen skal ydes i den form, der giver den bedste virkning over for den konkrete borger.

Bemærk desuden, at fritagelsesbekendtgørelsens [§ 10](#) pålægger kommunen en **forudgående** hjælpe- og vejledningsforpligtelse – fritagelse skal først komme på tale, når hjælp ikke kan sætte borgeren i stand til selv at tilgå posten. Sammenholdt med bekendtgørelsens fritagelsesgrund nr. 7 om "praktiske vanskeligheder ved at skaffe et elektronisk id" udgør dette den praktiske bro mellem MitID-afslag og Digital Post-fritagelse, som lovgiver ikke ville automatisere: koblingen sker ikke af sig selv, men borgerservice skal vejlede om den.

LOV

[Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 7](#)

[Forvaltningsloven § 7, stk. 1](#)

[Lov om MitID og NemLog-in § 4, stk. 2](#)

Digital post i retsplejen: forkyndelse, ankefrister og grænserne for samtykke

Digital Post-lovens fremkomstregel er ikke uden videre overførbart til retsplejens formkrav, hvor der gælder selvstændige regler om forkyndelse og digital kommunikation.

Vestre Landsret behandlede i [SS-2244/2015-VLR](#) spørgsmålet, om en tiltalts oprettelse af en e-Boks – og dermed den blotte tekniske mulighed for at modtage digital post – kunne sidestilles med udtrykkeligt eller stiltiende samtykke til, at retten kunne fremsende meddelelser digitalt efter [retsplejelovens § 154 a, stk. 1](#). Anklagemyndigheden mente, at den tekniske modtagemulighed var tilstrækkelig til at fremme sagen som udeblivelsessag efter [§ 897, stk. 1](#); byretten og landsretten lagde vægt på det modsatte. Afgørelsen markerer

en klar grænse: Digital Post-lovens fremkomstregel indebærer ikke i sig selv, at retsplejelovens krav til samtykke og forkyndelse er opfyldt.

Omvendt har digital fremsendelse fuld effekt, hvor loven tillader det. I **S-2080-23** fastslog landsretten, at fremkomst i e-Boks er tilstrækkelig til at afbryde forældelsen efter **straffelovens § 94, stk. 5**, jf. **retsplejelovens § 153, stk. 3**. Og i **S-1656-22** blev en genpart af en ankemeddelelse sendt via Digital Post anset for gyldig efter **retsplejelovens § 907, stk. 1**, selv om tiltalte var varetægtsfængslet på fremsendelsestidspunktet. Østre Landsret nåede i **SS-1778/2019-OLR** frem til, at en anke var modtaget rettidigt trods forenklet digital forkyndelse, jf. **retsplejelovens § 155** og **§ 219 a, stk. 5**.

I civile sager har digital fremsendelse tilsvarende fuld retsvirkning. I **BS-5704/2017-KBH** afviste Københavns Byret genoptagelse efter **retsplejelovens § 367, stk. 2**, fordi sagsøgtens advokat for tredje gang udeblev fra et retsmøde. Advokaten anførte, at han hverken havde modtaget indkaldelsen eller retsbogen – men Domstolsstyrelsen bekræftede over for retten: "Ved digital post og FDF (eBoks) er vi helt sikre på, at posten er leveret." Retten lagde herefter leveringen til grund og lod udeblivelsesdommen stå ved magt.

Uden for retsplejen viser Højesterets kendelse i **BS-12/2024-HJR**, hvor langt fremkomstprincippet rækker over for erhvervsdrivende. En enkeltmandsvirksomhed havde fået sendt både forsikringssselskabets rykker- og varslingsbrev og DFIM's opkrævninger af dagsgebyrer efter **færdselslovens § 106, stk. 4 og 5** til **virksomhedens** e-Boks. Ejeren forklarede under strafansvar, at han ikke havde modtaget brevene, at virksomheden havde været uden aktivitet i over et år, og at han troede, en enkeltmandsvirksomhed ikke behøvede separat MitID/e-Boks. Fogedretten og landsretten nægtede at fremme udpanntningen; Højesteret ophævede landsrettens kendelse:

Under disse omstændigheder finder Højesteret, at det var berettiget, at Thisted Forsikrings rykker- og varslingsbrev af 25. maj 2022 og DFIM's efterfølgende breve om betaling af dagsgebyrer blev sendt til Indkærede (virksomhed)s e-Boks med "Indkærede (virksomhed)" som adressat.

Afgørende var, at køretøjet i Motorregisteret var indregistreret med virksomheden som primær bruger, og at forsikringen var tegnet i virksomhedens navn. Færdselslovens forarbejder understøtter samme linje: meddelelsen kan fremsendes "via digitale postløsninger", og kravet er opfyldt, "selvom ejeren m.v. måtte anføre, at meddelelsen ikke er modtaget eller kommet til vedkommendes kendskab".

LOV	Færdselsloven § 106, stk. 4, 5	Retsplejeloven § 154a, stk. 1
	Retsplejeloven § 367, stk. 2	Straffeloven § 94, stk. 5
PRAKSIS	Højesteret · Højesterets afgørelse om gyldigheden af varsling via virksomhedens e-Boks for dagsgebyrer ved manglende bilforsikring 17.09.2024 Landsretten · Kendelse om gyldigheden af anke via Digital Post til varetægtsfængslet person 09.02.2024 Landsretten · Forældelsesafbrydelse ved digital sigtelse: Fremkomst i e-boks er tilstrækkelig for afbrydelse efter Straffeloven § 94, stk. 5 27.09.2023 Landsretten · Østre Landsret: Anke modtaget rettidigt trods forenklet digital forkyndelse 03.10.2019 Landsretten · Digital Indkaldelse og Retsproces: Vurdering af Udeblivelsesbetingelser 07.01.2016 Byretten · Afvisning af genoptagelse af civil sag efter gentagne udeblivelser trods digital forkyndelse 18.09.2018	

§ 14 Sammenfatning: hvad praksis samlet set fortæller

Praksis på området er usædvanligt konsistent og lader sig sammenfatte i seks led.

Fremkomstreglen er hård og bevidst hård. Lovgiver har med åbne øjne valgt et fremkomstprincip svarende til papirbrevet i den fysiske postkasse – ikke et kundskabsprincip. Ombudsmanden bekræftede i [FOB 2016-34](#), at heller ikke god forvaltningsskik forpligter myndigheden til at kontrollere, om posten er læst:

Da reglerne om anvendelsen af Offentlig Digital Post og retsvirkningerne heraf er klart beskrevet i lov om Offentlig Digital Post og forarbejderne hertil, mener jeg ikke, at en offentlig myndighed er forpligtet til at kontrollere, om en borger har læst den eller de meddelelser, som myndigheden har sendt til borgerens e-Boks [...] før myndigheden sender den pågældende en rykker eventuelt med et rykkergebyr eller som her et administrativt bødeforelæg.

Ombudsmanden holdt dog udtrykkeligt døren på klem for, at der kan tænkes "helt særlige situationer", hvor god forvaltningsskik tilsiger fysisk post eller vejledning om fritagelsesmuligheden – han tog blot ikke stilling til dem i den konkrete sag om en 90-årig bilejer.

Risikoen er skarpt delt efter årsagsdomæne. Postløsning og visningsklient → myndighedens risiko. Eget udstyr, egen forbindelse, mistede koder, manglende opsætning af den kommercielle klient → borgerens risiko. Ankestyrelsens principmeddelelse [33-23](#) er den autoritative udmøntning.

Men fremkomsten skal bevises. Efter [26-16](#) skal myndigheden ved bestridt modtagelse fremlægge forsendelseslog, der dokumenterer **levering**, ikke blot afsendelse – og efter [33-23](#) tillige undersøge driftsforstyrrelser i visningsklienten.

Dispensationspraksis er restriktiv, men ikke lukket. Tværgående i [Planklagenævnet](#), [Vejdirektoratet](#), [Erhvervsankenævnet](#), [Landsskatteretten](#) og [Udlændingenævnet](#) er argumentet det samme: kunne du ikke tjekke din e-Boks, burde du have søgt fritagelse. Undtagelserne er (i) myndighedens skift af kommunikationsform uden forudgående vejledning ([125-13](#)), (ii) reel digital afskærelse kombineret med minimal fristoverskridelse og prompte reaktion ([BS-27387/2022-KOL](#)), og (iii) dokumenterede tekniske barrierer i myndighedens egne systemer ([BS-42968/2019-HJR](#)).

Fritagelsesordningen er systemets ventil – og dens tilgængelighed er det egentlige retssikkerhedsspørgsmål. Ni objektive fritagelsesgrunde, personligt fremmøde, en forudgående hjælpeforpligtelse, tidsubegrænset virkning – og afskåret administrativ rekurs. Siden 1. juni 2023 giver fritagelsen tillige et objektivi krav på alternativet til obligatoriske selvbetjeningsløsninger, jf. [lov om fravigelse fra obligatorisk digital selvbetjening § 2](#). Prisen for den skarpe fremkomstregel er, at fritagelsesadgangen reelt skal være kendt og tilgængelig for dem, der har brug for den – hvilket er præcis det, ombudsmandens vejledningskritik i [FOB 2019-11](#) og [FOB 2019-22](#) handler om.

MitID er nu lovreguleret forvaltning. Efter [FOB 2017-19](#) er den kontraktbaserede NemID-ordning afløst af [lov om MitID og NemLog-in](#) med udtrykkelig hjemmel til kommunernes rolle ([§ 5](#)), forvaltningslovens anvendelse på udpegede private aktørers afgørelser ([§ 20](#)) og lovfæstet klageadgang til Digitaliseringsstyrelsen ([§ 4, stk. 2](#), udmøntet i [MitID-bekendtgørelsens § 10](#)). Afslag og myndighedsbestemt spærring er nu utvetydigt forvaltningsafgørelser med begrundelses- og orienteringspligt.

Afgrænsningsmæssigt behandler denne oversigt alene den it-retlige retsvirkning af digital meddelelse og MitID-infrastrukturen. Strafbart misbrug af MitID/NemID hører under [mitid-nemid-misbrug](#) og [sms-phishing-smishing](#); persondataretligt tilsyn med digitale løsninger under [datatilsynet-afgoerelser](#) og [ai-systemer-gdpr](#); udbudstviser om selve postløsningen under [klagenævnet-for-udbud-procedure](#); og den generelle begrundelses- og genoptagelsespraksis under [begrundelse-forvaltning](#) og [genoptagelse-forvaltning](#).

Lov om Digital Post fra offentlige afsendere § 10

Lov om fravigelse fra obligatorisk digital selvbetjening § 2, stk. 1

Lov om MitID og NemLog-in § 20

PRAKSIS	Højesteret · Kæreskrift indgivet pr. mail pga. tekniske fejl på sagsportalen anset for gyldigt	11.02.2020
	Byretten · Afgørelse om dispensation for fristoverskridelse ved ansøgning om sygedagpenge grundet manglende digitale kompetencer	11.10.2023
	Landsskatteretten · Afslag på genoptagelse af momstilsvær grundet overskredne frister og manglende tjek af e-Boks	22.11.2023
	Ankestyrelsen · Sygedagpenge – Bortfald ved manglende medvirken i digital post; risikofordeling ved brug af visningsklienter og kommunens undersøgelsespligt	01.01.2023
	Ankestyrelsen · Dokumentationskrav for digital post: Myndighedens bevisbyrde for levering i borgernes digitale postkasse	01.01.2016
	Ankestyrelsen · Særlig vejledningspligt ved skift fra fysisk post til Digital Post om børnetilskud	01.01.2013
	Erhvervsankenævnet · Stadfæstelse af ledelsesaftifter for for sent indsendt årsrapport trods sygdom og manglende kendskab til Digital Post	14.09.2016
	Planklagenævnet · Afvisning af klage over påbud om lovliggørelse på grund af overskredet klagefrist	16.12.2020
	Udlændingenævnet · Afvisning af klage over opholdstilladelse grundet overskredet klagefrist og udvisning med indrejseforbud	11.11.2017
	Vejdirektoratet · Afvisning af klage over nedlæggelse af privat fællesvej på grund af overskredet klagefrist	17.03.2025

REFERENCE Lovgrundlag

8 paragraffer

Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere § 7		Lov om Digital Post fra offentlige afsendere § 3	stk. 1
Lov om Digital Post fra offentlige afsendere § 4	stk. 1	Lov om Digital Post fra offentlige afsendere § 5	stk. 1
Lov om Digital Post fra offentlige afsendere § 10		Lov om fravigelse fra obligatorisk digital selvbetjening § 2	stk. 1
Lov om MitID og NemLog-in § 4	stk. 1	Lov om MitID og NemLog-in § 20	stk. 1

MATERIALE Citerede afgørelser

36 afgørelser

HØJESTERET · ØVERSTE INSTANS

2

17.09.2024	Højesterets afgørelse om gyldigheden af varsling via virksomhedens e-Boks for dagsgebyrer ved manglende bilforsikring	6190-7422
11.02.2020	Kæreskrift indgivet pr. mail pga. tekniske fejl på sagsportalen anset for gyldigt	bs-42968-2019-hjr

LANDSRETTE · ANKEINSTANS

4

09.02.2024	Kendelse om gyldigheden af anke via Digital Post til varetægtsfængslet person	S-1656-22
27.09.2023	Forældelsesafbrydelse ved digital sigtelse: Fremkomst i e-boks er tilstrækkelig for afbrydelse efter Straffeloven § 94, stk. 5	S-2080-23

03.10.2019	Østre Landsret: Anke modtaget rettidigt trods forenklet digital forkyndelse	514-591
07.01.2016	Digital Indkaldelse og Retsproces: Vurdering af Udeblevelsesbetingelser	1008-1215
BYRET TEN · FØRSTE INSTANS		3
11.10.2023	Afgørelse om dispensation for fristoverskridelse ved ansøgning om sygedagpenge grundet manglende digitale kompetencer	3929-4743
27.03.2023	Afvisning af søgsmål om fratagelse af dansk indfødsret på grund af overskredet søgsmålsfrist	5872-7013
18.09.2018	Afvisning af genoptagelse af civil sag efter gentagne udeblivelser trods digital forkyndelse	801-904
LANDSSKATTERETTEN · ADMINISTRATIV KLAGEINSTANS		2
22.11.2023	Afslag på genoptagelse af momstilsvær grundet overskredne frister og manglende tjek af e-Boks	22-0074112
03.05.2023	Afslag på ekstraordinær genoptagelse af momstilsvær vedrørende foreløbig fastsættelse modtaget i e-Boks	19-0045533
VEJDIREKTORATET · NÆVN / KLAGEINSTANS		7
21.04.2026	Afvisning af klage over kommunalt beskæringspåbud – klagefrist overskredet (EMN-2026-11265)	emn_2026_11265
17.03.2025	Afvisning af klage over nedlæggelse af privat fællesvej på grund af overskredet klagefrist	emn_2025_11047
20.11.2024	Afvisning af klage over vejvedligeholdelse grundet overskredet klagefrist	emn_2024_621376
24.11.2023	Afvisning af klage over parasolopstilling: Forvirring om e-boks var ikke en 'særlig grund' til at se bort fra klagefrist	23_15241
25.11.2021	Påbud om lukning af formodet udvidet adgang ophævet på grund af manglende bevis og usaglig begrundelse	21_13508
15.06.2021	Afvisning af Genoptagelse: Manglende Tjek af e-Boks Grundet Sygdom Ikke Gyldig Grund for Overskredet Klagefrist	21_02975
29.01.2020	Klage over påbud om beskæring afvist på grund af overskredet klagefrist	20_00687
PLANKLAGENÆVNET · NÆVN / KLAGEINSTANS		6
07.08.2024	Planklagenævnets afvisning af klage over afslag på lovliggørende landzonetilladelse i Roskilde Kommune grundet fristoverskridelse	24/06060
10.12.2021	Planklagenævnets afslag på genoptagelse af klagesag vedrørende dispensation i Herning	21/13508
20.05.2021	Afvisning af klage over byggetilladelse grundet overskredet klagefrist	21/04751
16.12.2020	Afvisning af klage over påbud om lovliggørelse på grund af overskredet klagefrist	20/11016

09.05.2019	Afvisning af klage over påbud om lovliggørelse af kvist på grund af overskredet klagefrist	19/03357
10.11.2015	Natur- og Miljøklagenævnets afvisning af realitetsbehandling i sag om gyldighed af byplanvedtægt grundet overskredet klagefrist	NMK-33-03220
ANKESTYRELSEN · NÆVN / KLAGEINSTANS		4
01.01.2023	Sygedagpenge – Bortfald ved manglende medvirken i digital post; risikofordeling ved brug af visningsklienter og kommunens undersøgelsespligt	33-23
01.01.2021	Anmeldelsesfrist for arbejdsskadesager: Udløbstidspunkt for fysisk og digital post	7-21
01.01.2016	Dokumentationskrav for digital post: Myndighedens bevisbyrde for levering i borgernes digitale postkasse	26-16
01.01.2013	Særlig vejledningspligt ved skift fra fysisk post til Digital Post om børnetilskud	125-13
ERHVERVSANKENÆVNET · NÆVN / KLAGEINSTANS		3
28.09.2021	Stadfæstelse af lukning for straksregistrering på virk.dk efter manglende dokumentation for ejerændringer	21/00029
14.09.2016	Stadfæstelse af ledelsesafgifter for for sent indsendt årsrapport trods sygdom og manglende kendskab til Digital Post	2016-657
08.02.2016	Stadfæstelse af afgifter for for sent indsendt årsrapport trods påstand om manglende modtagelse af digitalt påkrav	2015-8794
UDLÆNDINGENÆVNET · NÆVN / KLAGEINSTANS		3
20.06.2025	Afvisning af klage over udvisning grundet overskridelse af klagefrist ved digital forkyndelse	W20250952925
13.11.2019	Afvisning af for sent indgivet klage trods betegnelse som ankesag i korrespondance	
11.11.2017	Afvisning af klage over opholdstilladelse grundet overskredet klagefrist og udvisning med indrejseforbud	
PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS		1
16.12.2024	Uenighed om observationstid ved uvirksom elektronisk p-skive i Helsingør	park-7422
RIGSADVOKATEN · NÆVN / KLAGEINSTANS		1
11.03.2025	Ikke erstatning for mistet jakke under polititransport – Klage afvist grundet overskridelse af klagefrist	AM2025.03.11RA

FORARBEJDE Betænkninger

3 referencer

e-signatur og formkrav i lovgivningen – delbetænkning afgivet af Justitsministeriets udvalg om retsvirkningerne af digital signatur m.v. (Betænkning nr. 1400)

nr. 1400 · 2000 · Justitsministeriet

Betænkning nr. 1456/2004 om e-signaturs retsvirkninger

nr. 1456 · 2004 · Justitsministeriet

Beretning om elektronisk aftaleindgåelse og handel

nr. 1517 · 2010 · Justitsministeriet

14

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over persondatabehandling i ansættelsesforhold

Kontrolforanstaltninger, overvågning og medarbejderes rettigheder under GDPR og databeskyttelsesloven

Version 2 · Opdateret 27. jun. 2026 · 21 afgørelser · 2019-2026

[Læs online](#)

INTRODUKTION

Arbejdsgivers behandling af medarbejderes personoplysninger reguleres af et komplekst samspil mellem databeskyttelsesforordningen (GDPR), databeskyttelsesloven (DBL) § 12, tv-overvågningsloven, helbredsloven og kollektive aftaler om kontrolforanstaltninger. Praksis fra navnlig Datatilsynet, Arbejdsretten, Højesteret og EU-Domstolen tegner et billede af et retsområde, hvor gennemsigtighedsprincippet og proportionalitetsvurderingen er altafgørende – og hvor virksomheder hyppigt fejler på oplysningspligten, sletningsreglerne og kravene til behandlingssikkerhed. Samtykke er som hovedregel uegnet som behandlingsgrundlag i ansættelsesforhold pga. det ulige magtforhold, og EU-Domstolen har fastslået, at nationale særregler vedtaget efter GDPR art. 88 ikke kan fravige forordningens grundlæggende principper.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Samtykke er som hovedregel uegnet som behandlingsgrundlag i ansættelsesforhold pga. det ulige magtforhold mellem arbejdsgiver og ansat – interesseafvejning efter GDPR art. 6, stk. 1, litra f eller DBL § 12, stk. 1, er det primære grundlag.
- 02** Arbejdsgivere skal give medarbejdere forudgående, skriftlig og specifik information om enhver kontrolforanstaltning – mundtlig orientering alene opfylder ikke oplysningspligten efter GDPR art. 13-14.
- 03** Tv-overvågning af medarbejdere kan være lovlig af sikkerhedshensyn, men gennemsyn af optagelser med henblik på retskrav mod ansatte forudsætter begrundet mistanke om grovere overtrædelser.
- 04** GPS-sporing af firmabiler er kun lovlig til saglige driftsformål og kræver forudgående varsling – iværksættelse uden begrundet mistanke og uden overholdelse af varslingsfristen udløser bod i Arbejdsretten.
- 05** Biometrisk identifikation til almindelig tidsregistrering er uforholdsmæssig, da mindre indgribende metoder kan opfylde formålet – fingeraftryk til adgangskontrol kan derimod være lovlig, når der er et konkret sikkerhedsbehov.

- 06 Adgang til en fratrådt medarbejders e-mail og filer kræver klar hjemmel og forudgående information – uberettiget adgang udgør en alvorlig overtrædelse.
- 07 Billeder og videoer af tidligere medarbejdere skal slettes uden unødigt forsinkelse efter samtykkets tilbagetrækning – fortsat brug til markedsføring efter fratrædelse er ulovlig.
- 08 Nationale særregler efter GDPR art. 88 skal indeholde specifikke garantier ud over det generelle nødvendighedskrav – bestemmelser der blot gentager art. 6 har ikke det krævede normative indhold.
- 09 Kollektive overenskomster om behandling af ansattes data kan ikke fravige GDPR's grundlæggende principper i art. 5, 6 og 9, og den nationale domstol skal foretage fuld prøvelse af nødvendigheden.
- 10 Frygt for misbrug efter et databrud kan udgøre immateriel skade efter GDPR art. 82, men kræver at den registrerede løfter bevisbyrden for, at frykten er velbegrundet og konkret.

Retsgrundlag og hjemmelsstruktur for behandling af ansattes

§ 1 personoplysninger

Behandlingen af medarbejderes personoplysninger hviler på et flerlagssystem bestående af GDPR, nationale supplementer og kollektive aftaler.

Databeskyttelsesforordningens generelle regler finder direkte anvendelse. De grundlæggende principper i [GDPR art. 5](#) – lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning og integritet – gælder fuldt ud for ansættelsesdata. Behandlingsgrundlaget fastlægges efter [art. 6, stk. 1](#), og for følsomme oplysninger (helbred, fagforening, race m.v.) gælder det skærpede forbud i [art. 9, stk. 1](#) med de snævre undtagelser i stk. 2.

Databeskyttelsesloven § 12 udgør den centrale nationale supplement. Bestemmelsen er vedtaget med hjemmel i [GDPR art. 88](#), der giver medlemsstaterne mulighed for at fastsætte "mere specifikke bestemmelser" for ansættelsesforhold. [DBL § 12, stk. 1](#) hjemler behandling af både almindelige og følsomme oplysninger, når behandlingen er nødvendig for at overholde arbejdsretlige forpligtelser eller rettigheder fastlagt i lovgivning eller kollektive overenskomster. [Stk. 2](#) indeholder en interesseafvejningsregel svarende til [GDPR art. 6, stk. 1, litra f](#), der også gælder for offentlige arbejdsgivere. [Stk. 3](#) fastslår, at samtykke kan anvendes som behandlingsgrundlag i ansættelsesforhold, dog under iagttagelse af [GDPR art. 7's](#) frivillighedskrav.

Som det fremgår af forarbejderne til § 12:

Med lovforslagets § 12 er det hensigten at bringe fuldstændig sikkerhed for, at der på det offentlige og private arbejdsmarked lovligt kan behandles personoplysninger før, under og efter ansættelsesforholdet i samme omfang som hidtil.

Der er ingen vedtagne, ikke-konsoliderede ændringer til bestemmelsen (seneste konsolidering: 22. marts 2024).

Sideordnede regelsæt supplerer GDPR-regimet. Tv-overvågningsloven regulerer kameraovervågning, herunder skiltningsspligt og opbevaringsfrister. Helbredsloven regulerer arbejdsgivers indhentning af helbredsoplysninger. Og DA/FH-aftalen om kontrolforanstaltninger kræver saglig begrundelse, driftsmæssig

nødvendighed, proportionalitet og 6 ugers forudgående varsling af nye kontrolforanstaltninger i overenskomstdækkede virksomheder.

Det dogmatiske fundament for området blev lagt i [Betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning](#), der analyserede overgangsområdet mellem den dagældende persondatalov og den kommende databeskyttelseslov, herunder de særlige spørgsmål om ansattes data.

LOV

Databeskyttelsesforordningen (GDPR) § 5, stk. 1

Databeskyttelsesforordningen (GDPR) § 6, stk. 1

Databeskyttelsesforordningen (GDPR) § 9, stk. 1

Databeskyttelsesforordningen (GDPR) § 88, stk. 1-2

Databeskyttelsesloven § 12, stk. 1-3

§ 2 Behandlingsgrundlag – samtykkets begrænsning og interesseafvejningens dominans

Et centralt tema i Datatilsynets praksis er, at **samtykke** som hovedregel er uegnet som behandlingsgrundlag i ansættelsesforhold. Det skyldes det ulige magtforhold mellem arbejdsgiver og ansat, som gør det tvivlsomt, om samtykket er afgivet frivilligt.

Datatilsynet har i sin principielle udtalelse om fingeraftryk til tidsregistrering ([2018-211-0135](#)) fastslået:

Som følge af det afhængighedsforhold, der er mellem en arbejdsgiver og en ansat, er det efter Datatilsynets opfattelse tvivlsomt, om en ansat kan afvise at give en arbejdsgiver sit samtykke ... uden frygt eller reel risiko for, at afvisningen vil være til skade for den pågældende.

Denne restriktive linje er i overensstemmelse med EDPB Guidelines 05/2020 om samtykke, der specifikt nævner ansættelsesforhold som et område, hvor samtykkets frivillighed er undergravet af magtforholdet.

Interesseafvejning efter [GDPR art. 6, stk. 1, litra f](#) og [DBL § 12, stk. 1-2](#) er i praksis det foretrukne behandlingsgrundlag for de fleste kontrolforanstaltninger. Datatilsynet foretager en konkret afvejning af arbejdsgiverens legitime interesse over for medarbejderens rettigheder, hvor proportionalitetsprincippet er styrende.

For følsomme oplysninger (art. 9) kræves en hjemmel i art. 9, stk. 2. [DBL § 12, stk. 1](#) hjemler behandling, når den er nødvendig for at overholde arbejdsretlige forpligtelser – som anerkendt i sagen om [fingeraftryk til adgangskontrol \(2019-31-1650\)](#), hvor et slagteris biometriske system blev fundet lovligt med henvisning til fødevarerikkerhedsforpligtelser.

Datatilsynet har desuden præciseret, at **videregivelse af fagforeningstilhørsforhold** til en ekstern rådgiver kan være lovlig, når det er nødvendigt for at overholde arbejdsretlige forpligtelser, jf. [2025-31-1972](#). Omvendt har tilsynet udtalt alvorlig kritik af uberettiget videregivelse uden saglig nødvendighed, som i [TV 2/Norrbom Vinding-sagen \(2021-31-4751\)](#).

LOV

Databeskyttelsesforordningen (GDPR) § 6, stk. 1

Databeskyttelsesforordningen (GDPR) § 9, stk. 2

Databeskyttelsesloven § 12, stk. 1-3

PRAKSIS **Datatilsynet** · Lovlig videregivelse af personoplysninger og fagforeningstilhørsforhold til rådgiver under arbejdsretlig tvist

09.04.2026

Datatilsynet · Alvorlig kritik af TV 2 og Norrbom Vinding for behandling af personoplysninger i advokatundersøgelse	03.02.2022
Datatilsynet · Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	08.07.2020
Datatilsynet · Vejledende udtalelse om anvendelse af fingeraftryk til tidsregistrering i ansættelsesforhold	29.05.2019

§ 3 Kameraovervågning af medarbejdere – sikkerhedsformål vs. præstationskontrol

Tv-overvågning af arbejdspladser er et af de mest berørte områder i Datatilsynets praksis.

Overvågningen reguleres af et samspil mellem GDPR (behandlingsgrundlag, proportionalitet, oplysningspligt), tv-overvågningsloven (skiltning, opbevaringsfrister) og – for overenskomstdækkede virksomheder – DA/FH-aftalen om kontrolforanstaltninger.

Datatilsynets principielle afgørelse i [DSB Service & Retail-sagen \(2025-832-0031\)](#) fastslår de centrale rammer. Datatilsynet fandt, at tv-overvågning af medarbejdere i 7-Eleven-butikker på jernbanestationer var lovlig som sikkerhedsforanstaltning, hjemlet i [GDPR art. 6, stk. 1, litra f](#). Tilsynet understregede dog et afgørende forbehold:

Gennemsyn af optagelser med henblik på at kunne gøre retskrav gældende over for medarbejdere alene kan ske ved begrundet mistanke om grovere overtrædelser af interne retningslinjer og regler, som ikke kan prøves ved mindre indgribende midler.

Dermed er der en klar sontring mellem:

- **Lovlig overvågning:** Kriminalitetsforebyggelse, dokumentation af hændelser, sikkerhed for medarbejdere og kunder.
- **Ulovlig brug:** Løbende kontrol af arbejdsindsats, mødetider eller effektivitet via kameraoptagelser.

I samme sag præciserede Datatilsynet, at [DBL § 12](#) ikke er det rette behandlingsgrundlag for tv-overvågning, medmindre virksomheden er omfattet af en kollektiv aftale om kontrolforanstaltninger.

Oplysningspligten er en hyppig fejkilde. I [SIF Gruppen-sagen \(2019-41-0043\)](#) og [Kolding Kommune-sagen \(2019-423-0226\)](#) fandt Datatilsynet alvorlige mangler i den information, medarbejdere modtog om tv-overvågning. Fysisk skiltning med blot et kameraikon og teksten "tv-overvågning" opfylder ikke kravene i [GDPR art. 14](#), der kræver oplysning om kontrolformålet, retsgrundlaget, datakategorier og opbevaringstider.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 6, stk. 1](#)

[Databeskyttelsesforordningen \(GDPR\) § 14](#)

[Databeskyttelsesloven § 12, stk. 1](#)

PRAKSIS	Datatilsynet · Tv-overvågning af medarbejdere hos DSB Service & Retail A/S var berettiget af hensyn til sikkerhed	30.09.2025
	Datatilsynet · Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	07.08.2020
	Datatilsynet · Alvorlig kritik af Kolding Kommunes systematiske tilsidesættelse af oplysningspligten over for borgere	07.08.2020

§ 4 GPS-sporing af firmabiler – krav om saglig begrundelse og varsling

GPS-overvågning af firmakøretøjer rejser særlige proportionalitetsspørgsmål, fordi lokationsdata kan afsløre medarbejderes bevægelsesmønstre og – potentielt – privatliv.

I [SIF Gruppen-sagen \(2019-41-0043\)](#) behandlede Datatilsynet GPS-overvågning i servicebiler. Virksomheden informerede via lokale aftaler med angivelse af formål som effektivisering, kørselsadfærd og "big data-analyser", men oplysningerne manglede angivelse af det specifikke retsgrundlag, opbevaringstider og medarbejdernes rettigheder. Datatilsynet fandt overtrædelse af [GDPR art. 13](#) og det grundlæggende gennemsigtighedsprincip i [art. 5, stk. 1, litra a](#).

Det arbejdsretlige aspekt af GPS-kontrol er belyst i Arbejdsrettens dom i [FV2025-332 \(arb2-254258\)](#), der vedrørte en kommunes GPS-kontrol af hjemmeplejens køretøjer. Kommunen havde iværksat kontrollen uden begrundet mistanke om overtrædelser og uden at overholde DA/KL-aftalens varslingsfrister. Arbejdsretten idømte kommunen en bod på 50.000 kr., idet retten fastslog, at kontrolforanstaltninger efter den kollektive aftale kræver:

- Saglig begrundelse i driftsmæssige behov.
- Forudgående varslingsfrist (typisk 6 uger).
- Proportionalitet – kontrollen må ikke være mere indgribende end nødvendigt.

Disse krav afspejler de samme principper, som Datatilsynet håndhæver under GDPR, men med et selvstændigt arbejdsretligt sanktionssystem.

LOV	Databeskyttelsesforordningen (GDPR) § 5, stk. 1	Databeskyttelsesforordningen (GDPR) § 13
PRAKSIS	Arbejdsretten · Opmandskendelse FV2025-332: GPS-kontrol i kommunal hjemmepleje uden begrundet mistanke mod alle 13 medarbejdere krænker kontrolaftalen	15.06.2026
	Datatilsynet · Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	07.08.2020

§ 5 E-mail- og internetkontrol – særligt restriktive rammer

Adgang til medarbejderes e-mail og internetbrug er et af de mest følsomme kontrolområder, da det potentielt berører privat korrespondance og fortrolige oplysninger.

Datatilsynets afgørelse i sag [2024-31-0529](#) vedrørte uberettiget adgang til en fratrådt medarbejders e-mails og filer. Tilsynet udtalte alvorlig kritik, idet virksomheden havde tilgået det private materiale uden klar hjemmel og uden forudgående information til medarbejderen.

I [ATP-sagen \(2019-421-0035\)](#) gennemgik Datatilsynet ATP's praksis med adgang til medarbejderes e-mails ved fratrædelse eller sikkerhedsbrist. Tilsynet fandt, at det ikke fremgik tilstrækkeligt tydeligt, at oplysninger fra e-mails også kunne anvendes til kontrolformål. Der manglede oplysning om formålet, retsgrundlaget og opbevaringstiden.

Praksis viser følgende krav til lovlig e-mailkontrol:

- **Forudgående information:** Medarbejderen skal på forhånd vide, at e-mail kan gennemlæses under visse omstændigheder.
- **Konkret mistanke:** Stikprøvekontrol kræver konkret anledning – løbende gennemlæsning af al e-mail er uforholdsmæssig.

- **Dokumenteret politik:** Virksomheden skal have en skriftlig politik om e-mailbrug og kontrol.
- **Sondring mellem privat og professionel:** Private e-mails og filer nyder en stærkere beskyttelse.

Lignende principper gælder for logning af internetbrug. I både [ATP-sagen \(2019-421-0035\)](#) og [Nævnenes Hus-sagen \(2019-421-0034\)](#) fandt Datatilsynet, at logning af internetbrug og fagsystemer kræver specifik oplysning om formål, retsgrundlag og opbevaringstid – generelle privatlivspolitikker er utilstrækkelige.

LOV	Databeskyttelsesforordningen (GDPR) § 5, stk. 1	Databeskyttelsesforordningen (GDPR) § 13
PRAKSIS	Datatilsynet · Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer 25.10.2024	
	Datatilsynet · Alvorlig kritik af ATP for mangelfuld opfyldelse af oplysningspligt og håndtering af de registreredes rettigheder 07.08.2020	
	Datatilsynet · Kritik af Nævnenes Hus for mangelfuld oplysningspligt ved tv-overvågning og logning 07.08.2020	

§ 6 Biometrisk identifikation – nødvendighedskravets strenge grænser

Biometriske data (fingeraftryk, ansigtsgenkendelse) udgør særlige kategorier af personoplysninger under [GDPR art. 9, stk. 1](#), når de bruges til entydig identifikation. Behandlingen er derfor som udgangspunkt forbudt, medmindre en undtagelse i art. 9, stk. 2, finder anvendelse.

Datatilsynets praksis trækker en skarp grænse mellem **nødvendig** og **bekvem** biometri:

Ulovlig – fingeraftryk til tidsregistrering: I den principielle udtalelse [2018-211-0135](#) fandt Datatilsynet, at fingeraftryk til at sikre korrekt lønberegning ikke opfyldte nødvendighedskravet, da mindre indgribende metoder (adgangskort, PIN-koder, stikprøvekontroller) kunne opnå samme formål:

Kravet om nødvendighed indebærer, at behandling skal være mere end blot en praktisk måde at opfylde formålet på, ligesom kravet om nødvendighed indebærer, at formålet objektivt set ikke med rimelighed må kunne opnås ved mindre indgribende midler.

Lovlig – fingeraftryk til adgangskontrol ved slagteri: I sag [2019-31-1650](#) fandt Datatilsynet derimod, at et kreaturslagteris brug af fingeraftryk til adgangskontrol i produktionsområder var lovlig. Det afgørende var, at IFS-certificeringens krav om entydig identifikation af personale i produktionen udgjorde et konkret sikkerhedsbehov, som ikke kunne opfyldes med nøglebrikker (risiko for ombytning).

Ansigtsgenkendelse – krav om reelle alternativer: I sag [2023-31-0028](#) om ansigtsgenkendelse i fitnesscentre fastslog Datatilsynet, at samtykke til biometrisk behandling kræver reelle alternativer uden væsentlige ulemper. Et fitnessmedlem, der blev oplyst om, at fravalg begrænser adgangen til bemandede timer, havde ikke afgivet et gyldigt samtykke.

Biometrisk system	Formål	Resultat	Begrundelse
Fingeraftryk, tidsregistrering	Lønkontrol	Ulovlig	Adgangskort/PIN kan opnå formålet
Fingeraftryk, adgangskontrol (slagteri)	Fødevarer sikkerhed	Lovlig	Entydig identifikation nødvendig for certificering
Ansigtsgenkendelse, adgang (fitness)	Komfort	Betinget lovlig	Kræver reelle alternativer og informeret samtykke

LOV	Databeskyttelsesforordningen (GDPR) § 9, stk. 1-2	Databeskyttelsesloven § 12, stk. 1
PRAKSIS	Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	03.07.2024
	Datatilsynet · Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	08.07.2020
	Datatilsynet · Vejledende udtalelse om anvendelse af fingeraftryk til tidsregistrering i ansættelsesforhold	29.05.2019

§ 7 Oplysningspligt og gennemsigtighedskrav ved kontrolforanstaltninger

Datatilsynets tematiske tilsyn med kontrolforanstaltninger i 2019-2020 har etableret en klar praksis for, hvad oplysningspligten kræver ved medarbejderovervågning. Tilsynene hos ATP, Kolding Kommune, SIF Gruppen og Nævnenes Hus tegner et ensartet billede.

De centrale krav kan sammenfattes således:

- **Skriftlig form:** Oplysninger skal gives skriftligt eller elektronisk – mundtlig orientering er kun tilladt, når medarbejderen specifikt anmoder om det ([GDPR art. 12, stk. 1](#)).
- **Konkret information:** Generelle privatlivspolitikker er utilstrækkelige. For hver kontrolforanstaltning skal der oplyses om det specifikke formål, retsgrundlag, datakategorier og opbevaringstid.
- **Forudgående information:** Medarbejdere skal informeres *før* kontrollen iværksættes.
- **Lettilgængelig:** Informationen skal være let at finde – ansættelseskontrakter der tier om kontrolforanstaltninger, og intranetartikler der kræver særlig opmærksomhed, opfylder ikke kravet.

I [ATP-sagen \(2019-421-0035\)](#) fastslog Datatilsynet:

Det er Datatilsynets vurdering, at princippet om gennemsigtighed bl.a. indebærer, at den dataansvarlige skal give medarbejderne let tilgængelig – forudgående – information om de anvendte kontrolforanstaltninger, herunder særligt om kontrolformålet.

I [Kolding Kommune-sagen \(2019-423-0226\)](#) underkendte tilsynet kommunens praksis med udelukkende mundtlig orientering ved lokal introduktion. Kommunens argument om, at mundtlig orientering gav "den bedste forståelse", blev afvist:

Retten til at blive informeret er en hjørnesten i databeskyttelsesretten, da den er forudsætningen for, at borgeren kan udøve sine øvrige rettigheder, såsom retten til indsigt eller berigtigelse.

Tv-overvågningslovens skiltningsskrav supplerer, men erstatter *ikke*, GDPR's oplysningspligt. Datatilsynet har fastslået i [SIF Gruppen-sagen \(2019-41-0043\)](#) og [Nævnenes Hus-sagen \(2019-421-0034\)](#), at tv-overvågningslovens § 3 b kræver, at GDPR art. 14 overholdes *ud over* skiltningen.

LOV	Databeskyttelsesforordningen (GDPR) § 5, stk. 1	
	Databeskyttelsesforordningen (GDPR) § 12, stk. 1	Databeskyttelsesforordningen (GDPR) § 13
	Databeskyttelsesforordningen (GDPR) § 14	
PRAKSIS	Datatilsynet · Alvorlig kritik af ATP for mangelfuld opfyldelse af oplysningspligt og håndtering af de registreredes rettigheder	07.08.2020

- Datatilsynet** · Alvorlig kritik af Kolding Kommunes systematiske tilsidesættelse af oplysningspligten over for borgere 07.08.2020
- Datatilsynet** · Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten 07.08.2020
- Datatilsynet** · Kritik af Nævnenes Hus for mangelfuld oplysningspligt ved tv-overvågning og logning 07.08.2020

§ 8 Sletning af medarbejderbilleder og -data efter fratrædelse

Retten til sletning efter [GDPR art. 17](#) får særlig betydning, når en medarbejder fratræder. Datatilsynets praksis viser, at virksomheder hyppigt overser sletningspligten.

I [DMR-sagen \(2019-31-2316\)](#) klagede en tidligere ansat over, at virksomheden DMR A/S ikke fjernede videooptagelser og billeder af ham fra hjemmeside, Facebook og YouTube efter hans fratrædelse. Trods gentagne bekræftelser på, at han var "klippet ud", konstaterede Datatilsynet, at han fortsat fremgik af videoerne måneder senere. Tilsynet udtalte alvorlig kritik:

Datatilsynet vurderer, at DMR A/S ikke uden unødigt forsinkelse slettede oplysningerne om klager, idet klager ved sine henvendelser om sletning til DMR A/S må anses for at have trukket sit samtykke til behandlingen tilbage.

I sagen om [Hadsund Apotek \(762808a7d6458e9e08d38e184230aa1f\)](#) brugte apoteket billeder af en tidligere medarbejder til markedsføring efter fratrædelsen, hvilket Datatilsynet underkendte med kritik og påbud.

Praksis fastslår følgende principper for sletning efter fratrædelse:

- Samtykke til brug af billeder/videoer kan trækkes tilbage, og herefter skal sletning ske "uden unødigt forsinkelse".
- Der er ingen alternativ hjemmel til fortsat brug af markedsføringsmateriale med tidligere ansatte.
- Virksomheden bærer ansvaret for, at sletningen faktisk gennemføres på alle platforme – intern bekræftelse fritager ikke.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 17, stk. 1](#)

PRAKSIS

- Datatilsynet** · Kritik af Hadsund Apoteks brug af billeder af en tidligere medarbejder 01.12.2021
- Datatilsynet** · Alvorlig kritik af privat virksomhed for manglende sletning af personoplysninger efter anmodning 18.05.2020

§ 9 Videregivelse af følsomme medarbejderoplysninger og løndata

Videregivelse af medarbejderoplysninger til tredjeparter reguleres efter de almindelige behandlingsgrundlag i [GDPR art. 6](#) og – for følsomme oplysninger – [art. 9](#). Datatilsynets praksis tegner en skarp grænse mellem nødvendig og unødvendig videregivelse.

I sag [2025-31-1972](#) fandt Datatilsynet, at videregivelse af en medarbejders fagforeningstilhørsforhold til en ekstern rådgiver var lovlig, da det var nødvendigt for at overholde arbejdsretlige forpligtelser. Omvendt har tilsynet i [TV 2/Norrbom Vinding-sagen \(2021-31-4751\)](#) udtalt alvorlig kritik af uberettiget videregivelse af følsomme medarbejderoplysninger i forbindelse med en advokatundersøgelse.

Et nyere aspekt vedrører **entreprenørers adgang til lønoplysninger** i forbindelse med kontrol af arbejdsklausuler. I sag [2025-211-3778](#) tog Datatilsynet stilling til en hovedentreprenørs adgang til

underentreprenørers lønoplysninger for medarbejdere. Sagen illustrerer spændingsfeltet mellem offentlige bygherrers krav om kontrol med arbejdsvilkår og medarbejdernes ret til databeskyttelse.

Fagforeningsoplysninger er særligt beskyttede under [GDPR art. 9, stk. 1](#). Videregivelse kræver enten en hjemmel i art. 9, stk. 2 (typisk litra b om arbejdsretlige forpligtelser) eller en specifik lovbestemmelse. Den blotte administrative bekvemmelighed kan aldrig retfærdiggøre videregivelse af følsomme medarbejderdata.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 6, stk. 1](#)[Databeskyttelsesforordningen \(GDPR\) § 9, stk. 1-2](#)

PRAKSIS	Datatilsynet · Lovlig videregivelse af personoplysninger og fagforeningstilhørsforhold til rådgiver under arbejdsretlig tvist	09.04.2026
	Datatilsynet · Hovedentreprenørs adgang til lønoplysninger hos underentreprenører til kontrol af arbejdsklausuler	20.11.2025
	Datatilsynet · Alvorlig kritik af TV 2 og Norrbom Vinding for behandling af personoplysninger i advokatundersøgelse	03.02.2022

Kontrolforanstaltninger i Arbejdsrettens praksis – DA/FH-aftalens krav

Arbejdsretten håndhæver parallelt med Datatilsynet reglerne om kontrolforanstaltninger i ansættelsesforhold – men med hjemmel i de kollektive aftaler, navnlig DA/FH-aftalen om kontrolforanstaltninger fra 2006.

Aftalen kræver:

1. **Saglig begrundelse** i driftsmæssige behov.
2. **Proportionalitet** – kontrollen må ikke være mere indgribende end nødvendigt.
3. **6 ugers forudgående varsling** af nye kontrolforanstaltninger.

I [FV2025-332 \(arb2-254258\)](#) idømte Arbejdsretten en kommune bod på 50.000 kr. for GPS-kontrol af hjemmeplejekøretøjer iværksat uden begrundet mistanke og uden overholdelse af varslingsfristen. Dommen understreger, at kontrolforanstaltninger ikke kan iværksættes på ad hoc-basis, men kræver forudgående planlægning og information.

Omvendt frifandt Arbejdsretten i sag [arb2-219626](#) en virksomhed for videoovervågning, idet overvågningen var sagligt begrundet i kriminalitetsforebyggende formål. Afgørelsen viser, at kontrolforanstaltninger med et reelt og dokumenteret sikkerhedsformål kan opretholdes.

I sag [arb2-219772](#) om en tillidsrepræsentants krav om adgang til medarbejderoplysninger frifandt Arbejdsretten arbejdsgiveren. Sagen belyser grænsefladen mellem tillidsrepræsentantens informationsret og arbejdsgiverens databeskyttelsesforpligtelser.

Det er vigtigt at bemærke, at Arbejdsrettens og Datatilsynets kompetencer er sideordnede. Arbejdsretten bedømmer lovligheden af kontrolforanstaltninger efter den kollektive aftale, mens Datatilsynet bedømmer den databeskyttelsesretlige lovlighed. En kontrolforanstaltning kan i princippet være lovlig efter den kollektive aftale, men ulovlig efter GDPR – og omvendt.

PRAKSIS	Arbejdsretten · Opmandskendelse FV2025-332: GPS-kontrol i kommunal hjemmepleje uden begrundet mistanke mod alle 13 medarbejdere krænker kontrolaftalen	15.06.2026
---------	---	------------

Arbejdsretten · Tillidsrepræsentants krav om udlevering af navne- og kontaktoplysninger på valggrundlaget (Bygningsoverenskomsten)	14.03.2024
Arbejdsretten · Frifindelse af X ApS for påstand om misbrug af ledelsesret, ulovlig overvågning og organisationsfjendtlig adfærd over for FOA-medlemmer	24.02.2023

EU-Domstolens fortolkning af GDPR art. 88 – kravene til nationale ansættelsesregler

§ 11

EU-Domstolen har i to centrale domme fastlagt rammerne for, hvad nationale "mere specifikke bestemmelser" efter [GDPR art. 88](#) skal indeholde. Disse domme har direkte betydning for fortolkningen af [DBL § 12](#).

C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer): I denne dom af 30. marts 2023 fastslog Domstolen, at nationale bestemmelser, der blot gentager GDPR's generelle nødvendighedskrav i [art. 6, stk. 1, litra b](#), ikke udgør "mere specifikke bestemmelser" efter art. 88. For at kvalificere sig skal nationale regler have et *specifikt normativt indhold* og indeholde *passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder* ([art. 88, stk. 2](#)).

Sådanne bestemmelser synes nemlig ikke at have et specifikt normativt indhold på det område, der er reguleret, og som adskiller sig fra databeskyttelsesforordningens generelle bestemmelser. (præmis 81)

Domstolen fastslog desuden, at nationale regler, der ikke opfylder art. 88's krav, skal undlades anvendt i medfør af EU-retten forrang – medmindre de kan opretholdes som et selvstændigt retsgrundlag efter [art. 6, stk. 3](#). Sagen vedrørte læreres personoplysninger ved videoundervisning under covid-19. [C-34/21](#).

C-65/23 (MK mod K GmbH): I denne dom af 19. december 2024 uddybede Domstolen, at nationale regler og kollektive overenskomster vedtaget efter art. 88 ikke kan fravige GDPR's grundlæggende principper i [art. 5, art. 6, stk. 1](#) og [art. 9](#). Domstolen afviste endvidere, at parterne i en kollektiv overenskomst har en særlig skønsmargen, der begrænser domstolskontrollen med nødvendighedsvurderingen:

En fortolkning af databeskyttelsesforordningens artikel 88, hvorefter de nationale retsinstanser ikke kan foretage en fuldstændig domstolsprøvelse af en kollektiv overenskomst, navnlig med henblik på at efterprøve, om den i den berørte overenskomst omhandlede behandling af personoplysninger er nødvendig, er derfor ikke forenelig med denne forordning. (præmis 58)

[C-65/23](#).

For dansk ret betyder dette, at [DBL § 12](#) – der netop indeholder konkrete krav om nødvendighed knyttet til arbejdsretlige forpligtelser/rettigheder – formentlig opfylder art. 88's krav, i modsætning til mere generelle nationale bestemmelser, der blot gentager nødvendighedskravet.

LOV	Databeskyttelsesforordningen (GDPR) § 5	Databeskyttelsesforordningen (GDPR) § 6, stk. 1, 3
	Databeskyttelsesforordningen (GDPR) § 88, stk. 1-2	Databeskyttelsesloven § 12
PRAKSIS	EU-Domstolen · Beskyttelse af personoplysninger i ansættelsesforhold: Kollektive overenskomster og kravet om nødvendighed under GDPR	19.12.2024
	EU-Domstolen · Beskyttelse af læreres personoplysninger ved videoundervisning: Fortolkning af GDPR artikel 88 om 'mere specifikke bestemmelser' i ansættelsesforhold	30.03.2023

§ 12

Erstatning efter GDPR art. 82 – Højesterets dom om databrud

GDPR art. 82 giver registrerede ret til erstatning for både økonomisk og ikke-økonomisk skade forårsaget af overtrædelser af forordningen. Højesteret har i december 2025 taget principielt stilling til kravene for immateriel skadeerstatning i en sag med tilknytning til medarbejderes og borgeres data.

I [BS-14485/2025-HJR m.fl.](#) behandlede Højesteret fire sager, hvor borgere søgte godtgørelse efter et databrud i Gladsaxe Kommune. En bærbar computer med oplysninger om ca. 20.000 borgere – navne, cpr-numre, adresser og ydelsesoplysninger – blev stjålet fra rådhuset. Computeren var ikke krypteret, og regnearket var gemt lokalt i strid med interne retningslinjer.

Højesteret stadfæstede Østre Landsrets frifindelse af kommunen. Retten inddrog EU-Domstolens praksis og fastslog, at den registrerede skal godtgøre:

1. At der foreligger en overtrædelse af forordningen.
2. At der er lidt en materiel eller immateriel skade.
3. At der er årsagssammenhæng mellem overtrædelser og skaden.

Højesteret fandt, at appellanterne ikke havde løftet bevisbyrden for immateriel skade. Der var ingen lægelig dokumentation, og frygten for misbrug var ikke velbegrundet, da der 7 år efter tyveriet ikke var tegn på misbrug.

Dommen fastsætter en betydelig bevisbyrde for registrerede, der påberåber sig frygt for fremtidigt misbrug. For arbejdsgivere indebærer den dog ikke, at behandlingssikkerhedskravene i [GDPR art. 32](#) kan negligeres – overtrædelser bestod, men skaden var ikke tilstrækkeligt dokumenteret.

For en bredere gennemgang af GDPR art. 82-praksis, herunder EU-Domstolens fortolkning, se [gdpr-erstatning-artikel-82](#).

LOV

Databeskyttelsesforordningen (GDPR) § 32, stk. 1

Databeskyttelsesforordningen (GDPR) § 82, stk. 1

PRAKSIS **Højesteret** · Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer 19.12.2025

§ 13 Ulovligt indsamlede personoplysninger som bevismiddel

Et særligt spørgsmål opstår, når personoplysninger indsamlet i strid med GDPR ønskes brugt som bevis i en retssag – typisk en ansættelsesretlig tvist. EU-Domstolen har i sag [C-484/24](#) taget stilling til dette spørgsmål.

Domstolen fastslog, at GDPR ikke i sig selv regulerer spørgsmålet om bevisers antagelighed i retssager – det henhører under national procesret. Dog skal de nationale regler sikre, at retten til effektivt forsvar og kravet om en retfærdig rettergang respekteres. En national ret kan derfor tillade, at ulovligt indsamlede personoplysninger bruges som bevis, men skal inddrage den registreredes rettigheder i afvejningen.

For danske arbejdsgivere understreger dommen, at selv om en ulovlig overvågning potentielt kan give brugbart bevismateriale, fjerner det ikke den databeskyttelsesretlige overtrædelse. Arbejdsgiveren risikerer sanktioner fra Datatilsynet (kritik, påbud, bøde) uafhængigt af, om beviset tillades i den ansættelsesretlige sag.

Databeskyttelsesforordningen (GDPR) § 6, stk. 1

LOV

PRAKSIS EU-Domstolen · C-484/24: GDPR og bevisfremlæggelse – domstoles behandling af ulovligt indsamlede personoplysninger

18.06.2026

§ 14 Sammenfatning og vejledning for arbejdsgivere

Den samlede praksis fra Datatilsynet, Arbejdsretten, Højesteret og EU-Domstolen tegner følgende hovedmønstre for lovlig behandling af medarbejderes personoplysninger:

Behandlingsgrundlag: Brug interesseafvejning ([GDPR art. 6, stk. 1, litra f](#)) eller [DBL § 12, stk. 1](#) – ikke samtykke, medmindre der er tale om en reel valgfrihed uden konsekvens for ansættelsen.

Proportionalitet: Enhver kontrolforanstaltning kræver en konkret interesseafvejning. Formålet skal være sagligt og udtrykkeligt angivet, og midlet må ikke være mere indgribende end nødvendigt. Datatilsynets sammenlignende tabel i fingeraftryksudtalelsen ([2018-211-0135](#)) er vejledende: kan formålet opnås med mindre indgribende midler, er biometri/GPS/total overvågning uforholdsmæssig.

Oplysningspligt: Den mest udbredte overtrædelsestype. Arbejdsgivere skal udarbejde konkrete, skriftlige oplysninger om *hver* kontrolforanstaltning med angivelse af formål, retsgrundlag, datakategorier, opbevaringstid og rettigheder – og give dem *forudgående* og i en lettilgængelig form.

Sletning: Medarbejderbilleder og -data skal slettes uden unødigt forsinkelse ved fratrædelse, når samtykke trækkes tilbage, og der ikke foreligger et alternativt behandlingsgrundlag.

Kollektive aftaler: DA/FH-aftalens varslings- og proportionalitetskrav supplerer GDPR, men kan ikke fravige forordningens grundlæggende principper. EU-Domstolen har fastslået, at nationale domstole skal foretage fuld prøvelse af nødvendigheden, uanset kollektive aftalers indhold.

Erstatning: Registrerede bærer bevisbyrden for konkret immateriel skade efter [GDPR art. 82](#). Frygt for misbrug kan udgøre skade, men kræver dokumentation.

For Datatilsynets generelle afgørelsespraksis se [datatilsynet-afgoerelser](#). For whistleblowerdata se [whistleblower-beskyttelse](#).

LOV

Databeskyttelsesforordningen (GDPR) § 6, stk. 1

Databeskyttelsesforordningen (GDPR) § 82, stk. 1

Databeskyttelsesloven § 12, stk. 1

PRAKSIS Datatilsynet · Vejledende udtalelse om anvendelse af fingeraftryk til tidsregistrering i ansættelsesforhold

29.05.2019

REFERENCE Lovgrundlag

6 paragraffer

Databeskyttelsesforordningen (GDPR) § 6 stk. 1

Databeskyttelsesforordningen (GDPR) § 9 stk. 1

Databeskyttelsesforordningen (GDPR) § 13

Databeskyttelsesforordningen (GDPR) § 82 stk. 1

Databeskyttelsesforordningen (GDPR) § 88 stk. 1-2

Databeskyttelsesloven § 12

stk. 1-3

MATERIALE Citerede afgørelser 21 afgørelser

HØJESTERET · ØVERSTE INSTANS 1

19.12.2025	Højesterets dom om godtgørelse for immateriel skade efter databeskyttelsesforordningens artikel 82 ved tyveri af computer	14485-2025-2025-14653-2025-1 og-16195-2025
------------	---	--

EU-DOMSTOLEN · EUROPÆISK DOMSTOL 3

18.06.2026	C-484/24: GDPR og bevisfremlæggelse – domstoles behandling af ulovligt indsamlede personoplysninger	C-484/24
19.12.2024	Beskyttelse af personoplysninger i ansættelsesforhold: Kollektive overenskomster og kravet om nødvendighed under GDPR	C-65/23
30.03.2023	Beskyttelse af læreres personoplysninger ved videoundervisning: Fortolkning af GDPR artikel 88 om 'mere specifikke bestemmelser' i ansættelsesforhold	C-34/21

ARBEJDSRETEN · SPECIALRET 3

15.06.2026	Opmandskendelse FV2025-332: GPS-kontrol i kommunal hjemmepleje uden begrundet mistanke mod alle 13 medarbejdere krænker kontrolaftalen	254258
14.03.2024	Tillidsrepræsentants krav om udlevering af navne- og kontaktoplysninger på valggrundlaget (Bygningsoverenskomsten)	2023-1042
24.02.2023	Frifindelse af X ApS for påstand om misbrug af ledelsesret, ulovlig overvågning og organisationsfjendtlig adfærd over for FOA-medlemmer	2022-9

DATATILSYNET · NÆVN / KLAGEINSTANS 14

09.04.2026	Lovlig videregivelse af personoplysninger og fagforeningstilhørsforhold til rådgiver under arbejdsretlig tvist	2025-31-1972
20.11.2025	Hovedentreprenørs adgang til lønoplysninger hos underentreprenører til kontrol af arbejdsklausuler	2025-211-3778
30.09.2025	Tv-overvågning af medarbejdere hos DSB Service & Retail A/S var berettiget af hensyn til sikkerhed	2025-832-0031
25.10.2024	Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer	2024-31-0529
03.07.2024	Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	2023-31-0028
03.02.2022	Alvorlig kritik af TV 2 og Norrbom Vinding for behandling af personoplysninger i advokatundersøgelse	2021-31-4751
01.12.2021	Kritik af Hadsund Apoteks brug af billeder af en tidligere medarbejder	2021-31-4820
07.08.2020	Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	2019-41-0043
07.08.2020	Kritik af Nævnenes Hus for mangelfuld oplysningspligt ved tv-overvågning og logning	2019-421-0034

07.08.2020	Alvorlig kritik af ATP for mangelfuld opfyldelse af oplysningspligt og håndtering af de registreredes rettigheder	2019-421-0035
07.08.2020	Alvorlig kritik af Kolding Kommunes systematiske tilsidesættelse af oplysningspligten over for borgere	2019-423-0226
08.07.2020	Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	2019-31-1650
18.05.2020	Alvorlig kritik af privat virksomhed for manglende sletning af personoplysninger efter anmodning	2019-31-2316
29.05.2019	Vejledende udtalelse om anvendelse af fingeraftryk til tidsregistrering i ansættelsesforhold	2018-211-0135

FORARBEJDE Betænkninger

1 reference

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 1)
nr. 1565 · 2017 · Justitsministeriet

15

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over platformsansvar for ulovligt indhold (DSA, DMA og AVMS)

DSA-forordningen, DMA-forordningen og AVMS-direktivet i dansk og EU-retlig kontekst

Version 2 · Opdateret 27. jun. 2026 · 14 afgørelser · 2019-2025

[Læs online](#)

INTRODUKTION

Online-platformes ansvar for formidling af ulovligt indhold reguleres nu primært af DSA-forordningen (forordning (EU) 2022/2065), der trådte fuldt i kraft den 17. februar 2024 og afløste e-handelsdirektivets (2000/31/EF) ansvarsfritagelsesregler – i Danmark implementeret ved e-handelsloven. DSA-forordningen kodificerer og videreudvikler den betingede ansvarsfritagelse for hosting-udbydere, indfører en obligatorisk notice-and-action-mekanisme, forbyder generelle overvågningspligter og pålægger særlige due diligence-forpligtelser for onlineplatforme og meget store onlineplatforme (VLOP/VLOSE). EU-Domstolens praksis – navnlig Glawischnig-Piesczek (C-18/18), YouTube og Cyando (C-682/18 og C-683/18), L'Oréal mod eBay (C-324/09) og Polen mod Parlamentet og Rådet (C-401/19) – danner fortolkningsfundamentet for sondringen mellem passiv hosting og aktiv deltagelse, og denne praksis forbliver relevant under DSA. I dansk ret suppleres platformansvaret af straffelovens regler om privatlivskrænkelser (§§ 264 d-e), markedsføringslovens regler om skjult reklame (§ 6, stk. 4) – i praksis håndhævet af Forbrugerombudsmanden over for influencer-marketing – samt DMA-forordningens gatekeeper-regler og AVMS-direktivets regulering af videodelingsplatforme.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** En hosting-udbyder er ansvarsfritaget efter DSA art. 6 (tidligere e-handelsdirektivets art. 14), så længe udbyderen ikke har konkret kendskab til det ulovlige indhold – generelt kendskab til, at platformen bruges til ulovlige formål, er ikke tilstrækkeligt (YouTube og Cyando, C-682/18 og C-683/18).
- 02** En platform der spiller en 'aktiv rolle' – fx ved at fremme, optimere eller organisere brugerindhold ud over ren teknisk formidling – mister ansvarsfritagelsen (L'Oréal mod eBay, C-324/09; Louboutin mod Amazon, C-148/21).
- 03** En behørig anmeldelse (notice) under DSA art. 16 udløser konkret kundskab, og platformen skal derefter fjerne indholdet 'uden ophold' for at bevare ansvarsfritagelsen.
- 04** Nationale domstole kan pålægge en hosting-udbyder at fjerne identisk og indholdsmæssigt ækvivalent ulovligt materiale globalt, uden at dette udgør en generel overvågningsforpligtelse (Glawischnig-Piesczek, C-18/18).

- 05** Automatiserede uploadfiltre som påkrævet af ophavsretsdirektivets art. 17 udgør en begrænsning af ytringsfriheden, men er proportionale, når de ledsages af tilstrækkelige garantier – herunder forbud mod blokering af lovligt indhold, klageadgang og menneskelig kontrol (Polen mod Parlamentet og Rådet, C-401/19).
- 06** Forbuddet mod generelle overvågningspligter i DSA art. 8 (videreført fra e-handelsdirektivets art. 15) udelukker ikke specifikke overvågningspåbud rettet mod identificeret ulovligt indhold.
- 07** En onlinemarkedsplads-operatør er dataansvarlig efter GDPR for personoplysninger i brugerannoncer, selv om den samtidig er hosting-udbyder – hosting-fritagelsen i e-handelsdirektivet/DSA undtager ikke databeskyttelsespligter (C-492/23).
- 08** VLOP og VLOSE (platforme med 45+ mio. gennemsnitlige månedlige EU-brugere) er underlagt direkte Kommissions-tilsyn med bøder op til 6 % af global omsætning efter DSA art. 74.
- 09** DMA-forordningens gatekeeper-regler forbyder self-preferencing (art. 6, stk. 5) og kræver interoperabilitet (art. 7) af udpegede gatekeepere – håndhævet af Kommissionen med bøder op til 10 % af global omsætning.
- 10** Influencere og virksomheder der samarbejder om reklame på sociale medier er underlagt markedsføringslovens § 6, stk. 4, om skjult reklame – tagging af virksomheder er ikke tilstrækkelig reklamemarkering.
- 11** Erhvervsstyrelsen er udpeget som Digital Services Coordinator i Danmark efter lov nr. 481 af 14. maj 2024 og er dermed primær håndhævelsesmyndighed for DSA-forpligtelser over for platforme etableret i Danmark.

Det EU-retlige regelkompleks: fra e-handelsdirektivet til DSA-forordningen

§ 1

Ansvar for online-platforme og hostingtjenester har undergået en fundamental transformation med vedtagelsen af [DSA-forordningen \(forordning \(EU\) 2022/2065\)](#), der trådte fuldt i kraft den 17. februar 2024. Forordningen afløser den hidtidige ansvarsfritagelsesordning i e-handelsdirektivet (2000/31/EF), som i Danmark var implementeret ved e-handelsloven.

DSA-forordningen opretholder den lagdelte model med betinget ansvarsfritagelse for tre typer formidlertjenester:

- **Ren videreformidling ("mere conduit")** – [DSA art. 4](#): Tjenesteyderen overdrager blot information i et kommunikationsnet og er ansvarsfri, når den ikke udvælger eller ændrer indholdet.
- **Caching** – [DSA art. 5](#): Automatisk, mellemmand-lagring af information er ansvarsfri, når tjenesteyderen ikke ændrer indholdet og fjerner det straks ved kendskab til ulovlighed.
- **Hosting** – [DSA art. 6](#): Oplagring af information er ansvarsfri, så længe udbyderen ikke har *konkret kendskab* til det ulovlige indhold, eller – ved skadeserstatningskrav – ikke kender til omstændigheder, der gør ulovligheden åbenbar. Ved kendskab skal indholdet fjernes "uden ophold".

En væsentlig nyskabelse er [art. 7](#), den såkaldte "Good Samaritan"-klausul: en udbyder, der frivilligt iværksætter egne undersøgelser for at identificere ulovligt indhold, mister ikke derved sin ansvarsfritagelse. Bestemmelsen adresserer det hidtidige paradoks, hvor proaktiv indsats mod ulovligt indhold risikerede at give "konkret kendskab" og dermed afskar ansvarsfritagelsen.

[Art. 8](#) viderefører forbuddet mod generelle overvågningspligter fra e-handelsdirektivets art. 15:

Medlemsstaterne må ikke pålægge tjenesteydere en generel forpligtelse til at overvåge den information, de formidler eller oplagrer. Dette forbud udelukker dog ikke specifikke overvågningspåbud rettet mod identificeret ulovligt indhold i konkrete sager.

Forordningens umiddelbare og direkte virkning i alle medlemsstater indebærer, at EU-Domstolen har fortolkningsmonopol, og den betydelige retspraksis der er opbygget under e-handelsdirektivet, forbliver relevant som fortolkningsbidrag.

LOV

DSA-forordningen § 4

DSA-forordningen § 5

DSA-forordningen § 6

DSA-forordningen § 7

DSA-forordningen § 8

§ 2 EU-Domstolens centrale praksis om platformansvar

EU-Domstolens fortolkning af e-handelsdirektivets ansvarsfritagelse danner fortsat det dogmatiske fundament for forståelsen af DSA-forordningens tilsvarende bestemmelser. Tre hovedafgørelser er centrale:

Sondringen mellem passiv hosting og aktiv deltagelse

I [C-682/18](#) og [C-683/18](#) (YouTube og Cyando) fastslog EU-Domstolen (Store Afdeling), at en platformoperatør som udgangspunkt ikke selv foretager "overføring til almenheden" af ophavsretskrænkende materiale, medmindre operatøren går ud over den blotte tilrådighedsstillelse. Operatøren mister ansvarsfritagelsen i tre situationer:

- Operatøren har **konkret kendskab** til ulovligt indhold og undlader straks at slette eller blokere det.
- Operatøren ved eller burde vide, at platformen generelt anvendes til ulovlig deling, og undlader at gennemføre **passende tekniske foranstaltninger** (fx Content ID-systemer).
- Operatøren **deltager i udvælgelsen** af ulovligt indhold, stiller værktøjer specifikt til ulovlig deling til rådighed eller bevidst **fremmer** sådan deling – eksempelvis gennem en økonomisk model, der tilskynder til upload af krænkende materiale.

Domstolen præciserede, at *generelt* kendskab til, at en platform også bruges til ulovlige formål, ikke er tilstrækkeligt til at udløse ansvar. Underretning fra rettighedshavere skal være "tilstrækkelig præcis" til, at operatøren uden en dybtgående juridisk undersøgelse kan konstatere ulovligheden.

Globale fjernelsespåbud

I [C-18/18 \(Glawischnig-Piesczek mod Facebook\)](#) fastslog Domstolen, at nationale domstole kan pålægge en hosting-udbyder at fjerne ikke blot ordret identisk indhold, men også indhold med *samme betydning* som det ulovlige materiale – og at påbuddet kan have global rækkevidde inden for rammerne af folkeretten:

Eftersom et socialt netværk letter en hurtig overførsel mellem forskellige brugere af informationer, der er oplagret af hosting-udbyderen, er der en reel risiko for, at information, som er blevet erklæret ulovlig, senere gengives og deles af en anden bruger af dette netværk. (præmis 36)

Denne afgørelse er nu kodificeret i DSA art. 9 om myndighedsordrer mod ulovligt indhold.

Hybride markedspladsmodeller

I [C-148/21 \(Louboutin mod Amazon\)](#) udvidede Domstolen analysen til hybride platforme: en operatør, der både sælger egne varer og formidler tredjeparters varer i et ensartet layout, kan anses for selv at "gøre brug af" et tegn (varemærke), hvis en "almindeligt oplyst og rimeligt opmærksom bruger" får det indtryk, at operatøren i eget navn markedsfører varerne. Faktorer som ensartet præsentation, eget distributørlogo og supplerende logistikydelser (oplagring, forsendelse) er relevante.

Platform som dataansvarlig under GDPR

I [C-492/23](#) fastslog Domstolen, at en onlinemarkedsplads-operatør er dataansvarlig for personoplysninger i brugerannoncer, når den offentliggør dem til egne kommercielle formål og bestemmer parametre for formidling. Hosting-fritagelsen i e-handelsdirektivet kan ikke benyttes til at fravige GDPR-forpligtelser, da databaseskyttelse specifikt er undtaget fra direktivets anvendelsesområde.

LOV	DSA-forordningen § 6	DSA-forordningen § 9	
PRAKSIS	EU-Domstolen · Operatøren af en onlinemarkedsplads som dataansvarlig for følsomme oplysninger i annoncer EU-Domstolen · Louboutin mod Amazon: Ansvar for varemærkekrænkelser på online markedspladser ved blandet forretningsmodel EU-Domstolen · YouTube og Cyando: Ansvar for videodelings- og hostingplatforme ved brugernes ophavsretskrænkelser EU-Domstolen · Hosting-udbyderes ansvar for ærekrænkende indhold og muligheden for globale påbud		02.12.2025 22.12.2022 22.06.2021 03.10.2019

§ 3 Notice-and-action og platformens due diligence-forpligtelser under DSA

DSA-forordningen indfører et trinvist system af forpligtelser, der stiger med platformens størrelse og rolle:

Alle hostingtjenester skal implementere en notice-and-action-mekanisme efter [DSA art. 16](#). En *behørig anmeldelse* (notice) skal indeholde en forklaring af, hvorfor indholdet er ulovligt, en identifikation af det

pågældende indhold samt anmelderens kontaktoplysninger. Modtagelsen af en behørig anmeldelse udløser konkret kundskab, og platformen skal derefter fjerne indholdet "uden ophold" for at bevare ansvarsfritagelsen.

Når indhold fjernes, kræver [art. 17](#) en klar og specifik begrundelse til den berørte bruger, herunder information om klagemuligheder.

Onlineplatforme (der stiller brugergenereret indhold til rådighed for almenheden) har yderligere forpligtelser:

- **Intern klageordning** ([art. 20](#)): Brugere, hvis indhold er fjernet, skal have adgang til en effektiv intern klagemekanisme.
- **Udenretlig tvistbilæggelse** ([art. 21](#)): Brugere skal kunne henvende sig til certificerede tvistbilæggesorganer.
- **Trusted flaggers** ([art. 22](#)): Anmeldelser fra udpegede betroede indberettere behandles prioriteret.
- **Transparensrapporter** ([art. 24](#)): Platformene skal offentliggøre årlige rapporter om indholdsmoderation.
- **Reklametransparens** ([art. 26-28](#)): Onlinereklamer skal ledsages af oplysning om, at der er tale om reklame, hvem der betaler, og de vigtigste parametre for målretning.

Onlinemarkedspladser er derudover underlagt KYBC-pligter (Know Your Business Customer) efter [art. 30-32](#): platforme, der giver forbrugere mulighed for at indgå aftaler med erhvervsdrivende, skal indhente, verificere og opbevare sælgeroplysninger.

VLOP og VLOSE (Very Large Online Platforms/Search Engines med 45+ mio. gennemsnitlige månedlige EU-brugere) har de mest vidtgående forpligtelser:

- Årlig systemisk risikovurdering ([art. 34](#)) vedrørende spredning af ulovligt indhold, risici for grundlæggende rettigheder og offentlig debat.
- Afbødende foranstaltninger ([art. 35](#)) tilpasset de identificerede risici.
- Kriseresponsmekanisme ([art. 36](#)) i alvorlige situationer.
- Uafhængig revision ([art. 37](#)) mindst én gang årligt.
- Dataadgang for forskere ([art. 40](#)).

Kommissionens gennemførelsesforordning (EU) 2023/1201 fastsætter de nærmere procedureregler for kontrolbesøg, overvågning og aktindsigt i forbindelse med Kommissionens tilsyn med VLOP og VLOSE.

LOV

DSA-forordningen § 16

DSA-forordningen § 17

DSA-forordningen § 20-22

DSA-forordningen § 34-37

§ 4 Uploadfiltre og ophavsret: ophavsretsdirektivets artikel 17

Forholdet mellem platformansvar og ophavsret blev skærpet med ophavsretsdirektivets (direktiv (EU) 2019/790) art. 17, der indfører en selvstændig ansvarsordning for udbydere af onlineindholdsdelingstjenester. Ordningen fastsætter, at platforme foretager "overføring til almenheden" af ophavsretskrænkende materiale og kun kan opnå ansvarsfritagelse, hvis de har gjort deres "bedste indsats" for at indhente tilladelser og forhindre tilgængeliggørelsen af specifikt identificerede værker.

I praksis forudsætter dette brug af automatiserede genkendelses- og filtreringsværktøjer (uploadfiltre).

I [C-401/19 \(Polen mod Parlamentet og Rådet\)](#) forkastede EU-Domstolen (Store Afdeling) Polens annulationssøgsmål og fastslog:

- Filtreringsforpligtelsen udgør en **begrænsning af ytringsfriheden** efter Chartrets art. 11, da den *de facto* tvinger platforme til forudgående kontrol af brugeruploadet indhold.
- Begrænsningen er imidlertid **proportional**, da direktivet indeholder tilstrækkelige garantier:
 - Et **absolut forbud** mod blokering af lovligt indhold ([art. 17, stk. 7](#)).
 - Obligatoriske **undtagelser** for citater, kritik, parodier og pastiches i hele EU.
 - Forbuddet mod **generelle overvågningspligter** gælder fortsat ([art. 17, stk. 8](#)).
 - Effektiv **klageadgang** med menneskelig kontrol ([art. 17, stk. 9](#)).

En sådan forudgående kontrol og filtrering kan imidlertid medføre en begrænsning af et vigtigt middel til udbredelse af indhold online og således udgøre en begrænsning af den ret, der er sikret ved chartrets artikel 11. (præmis)

Denne afgørelse har direkte relevans for DSA-forordningens fortolkning: selv om DSA ikke pålægger filterpligter, skal enhver national foranstaltning, der kræver specifikke indholdskontrolforanstaltninger, overholde de samme proportionalitetskrav.

LOV

DSA-forordningen § 8

PRAKSIS

EU-Domstolen · Polen mod Parlamentet og Rådet: Lovligheden af platformes filtreringsforpligtelser i ophavsretsdirektivet (Sag C-401/19) 26.04.2022

§ 5 DMA-forordningens gatekeeper-regulering

Parallelt med DSA regulerer [DMA-forordningen \(forordning \(EU\) 2022/1925\)](#) de største digitale aktørers markedsadfærd. DMA retter sig mod udpegede *gatekeepere* – virksomheder der kontrollerer centrale platformstjenester (søgemaskiner, sociale netværk, app-butikker, annoncetjenester m.v.) med en betydelig indvirkning på det indre marked.

Pr. 2024 er syv virksomheder udpeget som gatekeepere: Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta (Facebook/Instagram), Microsoft og Booking.

DMA's kernepligter omfatter:

- **Forbud mod self-preferencing** ([art. 6, stk. 5](#)): En gatekeeper må ikke give egne tjenester en mere fordelagtig rangordning end tredjeparters tilsvarende tjenester.
- **Interoperabilitet** ([art. 7](#)): Gatekeepere der udbyder nummeruafhængige kommunikationstjenester skal gøre grundlæggende funktionaliteter interoperable med tredjeparter.
- **Dataportabilitet** ([art. 6, stk. 9](#)): Slutbrugere skal effektivt kunne overføre deres data.
- **Forbud mod kombinerende af persondata** ([art. 5, stk. 2](#)): Gatekeepere må ikke kombinere persondata fra deres platformstjeneste med data fra andre tjenester eller tredjeparter uden brugerens samtykke.

Håndhævelsen er centraliseret hos Kommissionen med bøder op til 10 % af global årlig omsætning – ved gentagelse op til 20 %. I Danmark varetager Konkurrence- og Forbrugerstyrelsen den nationale kontakt.

DMA og DSA supplerer hinanden: DSA regulerer platformens ansvar for *indhold*, mens DMA regulerer platformens *markedsadfærd*. En overtrædelse af DMA's interoperabilitets- eller dataportabilitetskrav kan i sig selv understøtte et ulovlighedspåbud under DSA, da manglende interoperabilitet kan begrænse brugeres mulighed for at skifte platform og dermed forværre lock-in-effekter.

LOV

[DMA-forordningen § 5, stk. 2](#)[DMA-forordningen § 6, stk. 5](#)[DMA-forordningen § 7](#)

Dansk håndhævelse: Erhvervsstyrelsen, Forbrugerombudsmanden og domstolene

Håndhævelseslandskabet i Danmark fordeler sig på flere myndigheder:

Erhvervsstyrelsen som Digital Services Coordinator

Ved lov nr. 481 af 14. maj 2024 om håndhævelse af forordningen om digitale tjenester er Erhvervsstyrelsen udpeget som Danmarks Digital Services Coordinator (DSC). Erhvervsstyrelsen har dermed kompetence til at håndhæve DSA-forpligtelserne over for platforme, der har deres hovedetablering i Danmark, herunder tilsynet med at de trinvis due diligence-forpligtelser overholdes. VLOP/VLOSE er dog under direkte Kommissions-tilsyn.

Forbrugerombudsmanden og markedsføringsret

For reklame formidlet via platforme er Forbrugerombudsmanden den primære håndhævelsesmyndighed. Praksis illustrerer dette navnlig i influencer-sagerne:

I [sagen om influencers skjulte reklame over for børn og unge](#) vurderede Forbrugerombudsmanden, at influencerne overtrådte [markedsføringslovens § 6, stk. 4](#) ved at omtale virksomheder, de havde ejerandele i, uden at markere opslagene som reklame. Tagging af virksomheder var ikke tilstrækkelig markering.

I [sagen om manglende oplysning om rabatkoder](#) fandt Forbrugerombudsmanden, at brug af personlige rabatkoder, som influenter tjente provision på, udløste oplysningspligt om kommerciel hensigt.

Praksis kulminerede i en straffedom: I [sagen om influencer dømt for skjult reklame](#) blev en influent idømt bøde – Østre Landsret nedsatte byrettens bøde fra 50.000 kr. til 30.000 kr. på grund af lang sagsbehandlingstid for 23 opslag uden reklamemarkering.

Forbrugerombudsmandens [Retningslinjer om offentliggørelse af brugeranmeldelser](#) fra 2015 opstiller krav til platforme, der formidler brugeranmeldelser – herunder e-handelslovens regler om formidleransvar og forpligtelsen til at offentliggøre alle anmeldelser uselektivt.

Domstolene og platformansvar

I [BS-24663/2023-SHR \(Flex Gulvservice mod Trustpilot\)](#) behandlede Sø- og Handelsretten spørgsmålet om Trustpilots ansvar for en uretmæssig brugeranmeldelse fra en tidligere ansat. Sagen illustrerer den praktiske afvejning mellem platformens ansvarsfritagelse som hosting-udbyder og dens forpligtelse til at reagere på konkret kendskab til ulovligt indhold.

LOV

[Markedsføringsloven § 6, stk. 4](#)

PRAKSIS

Sø- og Handelsretten · Ansvar for uretmæssige anmeldelser på onlineplatform: Flex Gulvservice ApS mod Trustpilot A/S	19.03.2024
Forbrugerombudsmanden · Influencer dømt for skjult reklame på sociale medier: Mangelfuld reklamemarkering og overtrædelse af markedsføringsloven	21.02.2025
Forbrugerombudsmanden · Influencers markedsføring på sociale medier: Skjult reklame over for børn og unge	08.10.2024
Forbrugerombudsmanden · Influencers skjulte reklame: Manglende oplysning om kommerciel hensigt ved omtale af rabatkoder	08.10.2024
Forbrugerombudsmanden · Influencer dømt for skjult reklame på Instagram og blog	17.05.2023

§ 7 Influencer-marketing på platforme: praksis om skjult reklame

Forbrugerombudsmandens praksis om influencer-marketing på sociale medier danner en selvstændig kategori af platformansvar – her er det ikke platformen som formidler, men platformen som *arena* for reklame, der er i fokus. Praksis bygger på [markedsføringslovens § 6, stk. 4](#) om forbud mod skjult reklame.

Hovedmønstrene i praksis er:

- **Kommerciel hensigt** foreligger, når influenten modtager *enhver form for fordel*: betaling, rabatter, gratis produkter, lån af tøj, invitationer til arrangementer eller personlige rabatkoder med provision.
- **Tagging** af virksomheder i opslag er **ikke tilstrækkelig** reklamemarkering – den kommercielle hensigt skal fremgå klart og tydeligt.
- **Skærpede krav** gælder ved reklame rettet mod **børn og unge**, som har sværere ved at gennemskue reklamer.
- **YouTube og videoindhold**: Reklamemarkering skal fremgå af titlen og være synlig i søgeresultater og kanalforsider *før* afspilning.
- **Influentens selvstændige ansvar**: En influent bærer eget ansvar for lovligheden, uanset om et managementbureau har rådgivet om, at markering ikke var nødvendig.

Sag	Udfald	Bøde/sanktion
Influencer-reklame overfor børn	Skjult reklame	Indskærpelse
Influencer-reklame markering	Skjult reklame	Indskærpelse
Rabatkode-provision	Skjult reklame	Indskærpelse
Influencer dømt – 23 opslag	Straffedom	30.000 kr. (ØL)
Influencer dømt – blog + Instagram	Straffedom	15.000 kr. (ØL)
Direkte købsopfordring til børn	Overtrådt § 9	Indskærpelse

DSA-forordningen supplerer denne praksis med sit krav om reklametransparens i [art. 26](#): onlinereklamer på platforme skal ledsages af oplysning om, at der er tale om reklame, hvem der betaler, og de vigtigste parametre for målretning. Forbrugerombudsmandens praksis om influencer-marketing og DSA's transparenskrav virker således kumulativt.

LOV	DSA-forordningen § 26	Markedsføringsloven § 6, stk. 4	Markedsføringsloven § 9
PRAKSIS	Forbrugerombudsmanden · Influencer dømt for skjult reklame på sociale medier: Mangelfuld reklamemarkering og overtrædelse af markedsføringsloven		
			21.02.2025

Forbrugerombudsmanden · Influencers markedsføring på sociale medier: Skjult reklame over for børn og unge	08.10.2024
Forbrugerombudsmanden · Influencer og skjult reklame: Krav om tydelig markering af kommerciel hensigt på sociale medier	08.10.2024
Forbrugerombudsmanden · Forbrugerombudsmandens vurdering af influencers markedsføring på sociale medier: Skjult reklame	08.10.2024
Forbrugerombudsmanden · Influencers skjulte reklame: Manglende oplysning om kommerciel hensigt ved omtale af rabatkoder	08.10.2024
Forbrugerombudsmanden · Influencers aktiviteter på sociale medier er omfattet af markedsføringsloven	08.10.2024
Forbrugerombudsmanden · Forbrugerombudsmanden indskærper regler om direkte købsopfordringer til børn i influencer-marketing	08.10.2024
Forbrugerombudsmanden · Influencer dømt for skjult reklame på Instagram og blog	17.05.2023

§ 8 AVMS-direktivet og videodelingsplatforme

AVMS-direktivet (direktiv 2010/13/EU) som ændret ved direktiv (EU) 2018/1808 regulerer *videodelingsplatformstjenester* – platforme hvis væsentlige funktionalitet er at tilbyde programmer, brugergenerede videoer eller begge dele til almenheden.

Direktivets [art. 28a-28b](#) pålægger udbydere af videodelingsplatformstjenester at træffe passende foranstaltninger til:

- Beskyttelse af mindreårige mod indhold, der kan skade deres fysiske, psykiske eller moralske udvikling.
- Beskyttelse af den brede offentlighed mod indhold, der tilskynder til vold, had eller terrorisme.
- Overholdelse af audiovisuelle kommercielle kommunikationsregler – herunder forbud mod skjult reklame og produktplacering uden tydelig markering.

Tilsynsmyndighed i Danmark er Radio- og tv-nævnet. AVMS-regulering supplerer DSA for det specifikke segment af videodelingstjenester og fastsætter indholdsmæssige standarder, som DSA's generelle notice-and-action-mekanisme alene ikke afdækker.

Afgrænsningen mellem AVMS og DSA er vigtig: en videodelingsplatform, der også er en "onlineplatform" under DSA, er underlagt begge regelsæt. DSA regulerer *processen* for indholdsmoderation (notice-and-action, transparens, klageordning), mens AVMS fastsætter de *materielle* standarder for audiovisuelt indhold (beskyttelse af mindreårige, reklamemarkering, hadefuldt indhold).

§ 9 National strafferet: platformformidlet ulovligt indhold

Ulovligt indhold, der formidles via platforme, kan aktualisere en række strafferetlige bestemmelser i dansk ret:

- **Uberettiget videregivelse af billeder** ([straffelovens § 264 d](#)): Deling af private billeder eller meddelelser vedrørende en andens privatliv på platforme uden samtykke.
- **Udbredelse af materiale med seksuelt misbrug af børn** ([straffelovens § 235](#)): Platformens forpligtelse til at fjerne sådant materiale straks ved kendskab understreges af DSA art. 18, der kræver, at hosting-udbydere underretter retshåndhævende myndigheder ved mistanke om strafbare handlinger der indebærer en trussel mod menneskers liv eller sikkerhed.

- **Hadetale og offentlig forhånelse** (straffelovens § 266 b): Offentlig forhånelse eller nedværdigelse af grupper på grund af race, etnisk oprindelse, tro eller seksuel orientering.
- **Freds- og æreskrænkelser** (straffelovens kap. 27): Injurier og æreskrænkende udtalelser formidlet via platforme – se praksisoversigten [injurier og æreskrænkelser på sociale medier](#) for den detaljerede behandling.

Den strafferetlige dogmatik om hosting-udbyderes ansvar blev drøftet allerede i Straffelovrådets betænkning nr. 1462/2005 om kriminalisering af generelle opfordringer til selvmord m.v., der analyserede, hvornår en "host" kan ifalde strafansvar for retsstridig udbredelse af information:

Om en internetudbyder som 'host' kan ifalde strafansvar for retsstridig udbredelse af information fra udlejede pladser på serveren, antages at bero på en vurdering af, i hvilket omfang internetudbyderen har pligt til at føre kontrol og faktisk har gjort det.

Under DSA-forordningen er dette spørgsmål nu yderligere reguleret: en hosting-udbyder, der overholder art. 6's betingelser (ingen konkret kundskab eller hurtig fjernelse), er ansvarsfritaget – men denne ansvarsfritagelse udelukker ikke national strafferetlig forfølgning af den bruger, der uploadede det ulovlige indhold.

LOV

Straffeloven § 235

Straffeloven § 264d

Straffeloven § 266b

§ 10 Sammenfatning og afgrænsning mod tilgrænsende emner

Platformansvaret for ulovligt indhold hviler efter 2024 på tre søjler:

1. **DSA-forordningen** som det centrale regelsæt: betinget ansvarsfritagelse, notice-and-action, trinvis due diligence-forpligtelser og direkte Kommissions-tilsyn med VLOP/VLOSE.
2. **DMA-forordningen** for de største aktørers markedsadfærd: interoperabilitet, dataporterbarhed og forbud mod self-preferencing og tvangssammenkædning af persondata.
3. **National ret** – straffelov, markedsføringslov og AVMS-implementering – som supplerer EU-reglerne med materielle standarder for ulovligt indhold, reklamemarkering og audiovisuelt indhold.

EU-Domstolens praksis under e-handelsdirektivet forbliver det fortolkningsmæssige fundament for DSA's ansvarsfritagelsesregler. Den centrale sondring mellem passiv hosting og aktiv deltagelse, som udviklet i YouTube og Cyando (C-682/18), L'Oréal mod eBay (C-324/09) og Louboutin mod Amazon (C-148/21), gælder fortsat fuldt ud.

Denne praksisoversigt afgrænser sig mod:

- Æreskrænkende ytringer på sociale medier mellem privatpersoner: se [injurier og æreskrænkelser på sociale medier](#).
- Klager til Pressenævnet over redigerede medier: se [god presseskik](#).
- Erstatning for ulovlig persondatabehandling: se [GDPR-erstatning efter artikel 82](#).
- Ytringsfrihedens grænser efter EMRK art. 10: se [EMRK artikel 10 – ytringsfrihed](#).
- Datatilsynets afgørelsespraksis generelt: se [Datatilsynets afgørelser](#).

LOV

DMA-forordningen § 6, stk. 5

DSA-forordningen § 6

PRAKSIS	EU-Domstolen · Louboutin mod Amazon: Ansvar for varemærkekrænkelser på online markedspladser ved blandet forretningsmodel	22.12.2022
	EU-Domstolen · YouTube og Cyando: Ansvar for videodelings- og hostingplatforme ved brugernes ophavsretskrænkelser	22.06.2021

REFERENCE Lovgrundlag

6 paragraffer

DMA-forordningen § 5-7	DSA-forordningen § 8
DSA-forordningen § 16	DSA-forordningen § 4-6
Markedsføringsloven § 6	stk. 4
	Straffeloven § 264d

MATERIALE Citerede afgørelser

14 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		5
02.12.2025	Operatøren af en onlinemarkedsplads som dataansvarlig for følsomme oplysninger i annoncer	C-492/23
22.12.2022	Louboutin mod Amazon: Ansvar for varemærkekrænkelser på online markedspladser ved blandet forretningsmodel	C-148/21
26.04.2022	Polen mod Parlamentet og Rådet: Lovligheden af platformes filtreringsforpligtelser i ophavsretsdirektivet (Sag C-401/19)	C-401/19
22.06.2021	YouTube og Cyando: Ansvar for videodelings- og hostingplatforme ved brugernes ophavsretskrænkelser	C-682/18
03.10.2019	Hosting-udbyderes ansvar for ærekrænkende indhold og muligheden for globale påbud	C-18/18
SØ- OG HANDELSRET TEN · SPECIALRET		1
19.03.2024	Ansvar for uretmæssige anmeldelser på onlineplatform: Flex Gulvservice ApS mod Trustpilot A/S	6821-8195
FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS		8
21.02.2025	Influencer dømt for skjult reklame på sociale medier: Mangelfuld reklamemarkering og overtrædelse af markedsføringsloven	
08.10.2024	Influencers markedsføring på sociale medier: Skjult reklame over for børn og unge	
08.10.2024	Influencer og skjult reklame: Krav om tydelig markering af kommerciel hensigt på sociale medier	
08.10.2024	Forbrugerombudsmandens vurdering af influencers markedsføring på sociale medier: Skjult reklame	
08.10.2024	Influencers skjulte reklame: Manglende oplysning om kommerciel hensigt ved omtale af rabatkoder	

08.10.2024 Influencers aktiviteter på sociale medier er omfattet af markedsføringsloven

08.10.2024 Forbrugerombudsmanden indskærper regler om direkte købsopfordringer til børn i influencer-marketing

17.05.2023 Influencer dømt for skjult reklame på Instagram og blog

FORARBEJDE Betænkninger

1 reference

Straffelovrådets betænkning om kriminalisering af generelle opfordringer til selvmord m.v.

nr. 1462 · 2005 · Justitsministeriet

16

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over ret til at blive glemt

Sletning, deindeksering og den journalistiske undtagelse efter GDPR art. 17

Version 2 · Opdateret 26. jun. 2026 · 19 afgørelser · 2017-2025

[Læs online](#)

INTRODUKTION

Retten til at blive glemt – sletteretten – er en central registreret ret i GDPR art. 17, der giver den registrerede ret til at få personoplysninger slettet, når de ikke længere er nødvendige, samtykket er trukket tilbage, eller behandlingen er ulovlig. EU-Domstolen har i en række principielle afgørelser fastlagt rammerne for søgemaskinedeindeksering, behandling af følsomme data i søgeresultater og sletterettens geografiske rækkevidde. I dansk ret suppleres sletteretten af databeskyttelseslovens § 3, der undtager journalistiske medier, informationsdatabaser og kunstnerisk/litterær virksomhed fra GDPR's kapitel II-VII og IX. Praksisoversigten dækker EU-Domstolens, Datatilsynets og Pressenævnets afgørelser om konkrete sletteanmodninger.

PRINCIPPER UDLEDT AF PRAKSIS

- 01 Den registrerede har som udgangspunkt ret til at få søgeresultater på sit eget navn deindekseret, medmindre offentlighedens adgang til informationen vejer tungere (Google Spain-doktrinen).
- 02 En søgemaskineoperatør er selvstændig dataansvarlig for sin behandling af personoplysninger i søgeresultater og skal foretage en konkret interesseafvejning ved sletteanmodninger.
- 03 Offentlige personers – herunder politikere, embedsfolk og offentligt kendte – ret til sletning er begrænset, idet offentlighedens interesse i information om deres virke normalt vejer tungere.
- 04 Urigtige personoplysninger skal som udgangspunkt slettes eller berigtiges, og den registrerede behøver ikke bevise urigtigheden ved en domstolsafgørelse – det er tilstrækkeligt at fremlægge relevante beviser.
- 05 GDPR forpligter ikke søgemaskineoperatøren til verdensomspændende deindeksering, men minimum til effektiv deindeksering inden for EU's grænser.
- 06 Journalistiske mediers informationsdatabaser er undtaget GDPR's kapitel II-VII og IX efter databeskyttelsesloven § 3, stk. 5-8, når indlæggelsen er sket uændret i forhold til den oprindelige offentliggørelse.
- 07 Pressenævnet vurderer sletteanmodninger over for medier efter de presseetiske regler punkt B.8 og D.1, ikke efter GDPR – spørgsmål om databeskyttelseslovgivningen hører under Datatilsynet.

- 08** Sletning af gammel medieomtale af straffedomme kræver en afvejning af domens alder, dens alvor, den registreredes rolle og den samfundsmæssige interesse i fortsat tilgængelighed.
- 09** Den dataansvarlige bærer bevisbyrden for, at en undtagelse i GDPR art. 17, stk. 3, finder anvendelse.
- 10** Anonymisering kan være et tilstrækkeligt alternativ til fuld sletning, når det fjerner identifikationsmuligheden uden at krænke det journalistiske arkivs integritet.
- 11** Oplysninger om enkeltpersoners erhvervsmæssige virke vurderes lempeligere end private oplysninger – professionelle bidrag i mediearkiver er som udgangspunkt ikke 'særligt belastende'.

GDPR art. 17 og databeskyttelsesloven § 3 – retsgrundlaget for sletteretten

Sletteretten – retten til at blive glemt – er hjemlet i [GDPR art. 17](#), der pålægger den dataansvarlige at slette personoplysninger uden unødigt forsinkelse, når en af de seks slettegrunde i stk. 1 er opfyldt:

- Oplysningerne er ikke længere nødvendige til formålet ([art. 17, stk. 1, litra a](#))
- Samtykket er trukket tilbage ([art. 17, stk. 1, litra b](#))
- Den registrerede gør indsigelse mod behandlingen ([art. 17, stk. 1, litra c](#))
- Behandlingen er ulovlig ([art. 17, stk. 1, litra d](#))
- Sletning er nødvendig for at overholde en retlig forpligtelse ([art. 17, stk. 1, litra e](#))
- Oplysningerne er indsamlet i forbindelse med informationssamfundstjenester ([art. 17, stk. 1, litra f](#))

Sletteretten er dog ikke absolut. [Art. 17, stk. 3](#) fastsætter undtagelser, hvor behandling fortsat er nødvendig, herunder for at udøve retten til ytrings- og informationsfrihed (litra a), for at overholde en retlig forpligtelse (litra b), af hensyn til folkesundheden (litra c), til arkiv-/forskningsformål (litra d) og for at retskrav kan fastlægges, gøres gældende eller forsvares (litra e).

Når den dataansvarlige har offentliggjort personoplysningerne, skal denne desuden underrette andre dataansvarlige om sletteanmodningen, jf. [art. 17, stk. 2](#) – den såkaldte "videreformidlingspligt" ved sletning.

[GDPR art. 85](#) pålægger medlemsstaterne at forene databeskyttelsesretten med retten til ytrings- og informationsfrihed, herunder ved at fastsætte undtagelser for journalistisk virksomhed. I dansk ret er dette gennemført ved [databeskyttelsesloven § 3](#). Bestemmelsens stk. 4-8 undtager forskellige typer mediebehandling fra størstedelen af loven og forordningen:

- **Stk. 4:** Behandlinger omfattet af lov om massemediers informationsdatabaser er helt undtaget.
- **Stk. 5-6:** Uredigerede fuldttekstdatabaser med allerede offentliggjorte periodiske skrifter eller lyd-/billedprogrammer er undtaget fra GDPR kap. II-VII og IX, når indlæggelsen er sket uændret.
- **Stk. 7:** Manuelle arkiver over udklip fra offentliggjorte trykte artikler, udelukkende behandlet i journalistisk øjemed, er undtaget.
- **Stk. 8:** Behandling i øvrigt udelukkende i journalistisk øjemed – samt kunstnerisk eller litterær virksomhed – er undtaget.

Som forarbejderne til [databeskyttelsesloven](#) udtrykker det, er undtagelserne en videreførelse af de gældende regler fra persondatalovens § 2, stk. 5-9:

De nævnte regler gælder alene for behandling af oplysninger, som udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed. Hvis behandlingen ikke kan anses for udelukkende at ske til de nævnte formål, finder loven og forordningens regler fuldt ud anvendelse.

Forarbejderne fremhæver desuden, at det ikke er tilstrækkeligt, at den dataansvarlige selv anser behandlingen for journalistisk – der påhviler den dataansvarlige en forpligtelse til at sandsynliggøre, at aktiviteterne falder ind under undtagelsesreglen.

LOV

[Databeskyttelsesforordningen \(GDPR\) § 17, stk. 1-3](#)[Databeskyttelsesforordningen \(GDPR\) § 85](#)[Databeskyttelsesloven § 3, stk. 4-8](#)

§ 2 Google Spain-doktrinen – søgemaskineoperatøren som dataansvarlig

Den fundamentale retlige ramme for søgemaskinedeindeksering blev fastlagt i EU-Domstolens dom i **sag C-131/12, Google Spain** (13. maj 2014). Domstolen fastslog, at en søgemaskineoperatør er selvstændig dataansvarlig for sin behandling af personoplysninger, der fremkommer i søgeresultatlister. Den registrerede har som udgangspunkt ret til at få fjernet links fra søgeresultater på sit eget navn, medmindre offentlighedens interesse i at have adgang til oplysningen vejer tungere – typisk når den registrerede udøver en offentlig rolle, eller oplysningen er aktuel og samfundsrelevant.

Denne doktrin er siden blevet videreudviklet i en række efterfølgende afgørelser.

I **C-136/17 (GC and Others mod CNIL)** præciserede EU-Domstolen, at søgemaskineoperatøren har et selvstændigt ansvar for at vurdere, om søgeresultater indeholder følsomme personoplysninger (herunder oplysninger om straffedomme). Domstolen fastslog, at operatøren ved en anmodning om fjernelse af links skal foretage en afvejning mellem den registreredes grundlæggende rettigheder (EMRK art. 7 og 8) og den brede offentligheds informationsinteresse. Sagen omhandlede fire forskellige situationer:

- En person, der tidligere havde været politisk aktiv, men ikke længere var kandidat
- En person nævnt i forbindelse med Scientology, men som ikke længere beklædte den omtalte stilling
- En person, der havde været genstand for en korruptionsundersøgelse, som endte med frafald
- En person idømt fængselsstraf for seksuelle overgreb på mindreårige

Domstolen understregede, at retten til deindeksering ikke er automatisk – der skal foretages en konkret interesseafvejning i hvert enkelt tilfælde, hvor bl.a. oplysningens art, dens følsomhed, offentlighedens interesse og den registreredes rolle vurderes.

I **C-398/15 (Manni)** tog Domstolen stilling til sletteretten i forhold til selskabsregistre. Domstolen fandt, at medlemsstaterne ikke generelt kan give tredjemand ret til at kræve sletning af personoplysninger (navn, fødselsdato) i offentlige selskabsregistre, men anerkendte, at der efter en tilstrækkelig lang periode kan være grundlag for at begrænse adgangen til oplysningerne.

LOV [Databeskyttelsesforordningen \(GDPR\) § 17, stk. 1](#)

PRAKSIS **EU-Domstolen** · Søgemaskineudbyderes forpligtelser ved behandling af følsomme personoplysninger og retten til at blive glemmt 24.09.2019

EU-Domstolen · Begrænsning af offentlig adgang til personoplysninger i selskabsregistret efter virksomhedsopløsning – Foreneligheden mellem databeskyttelsesdirektiv 95/46 og selskabsdirektiv 68/151 08.03.2017

§ 3 Geografisk rækkevidde – deindeksering inden for EU eller globalt

Spørgsmålet om den geografiske rækkevidde af deindeksering blev afgjort i [C-507/17 \(Google mod CNIL\)](#). Den franske databeskyttelsesmyndighed CNIL havde pålagt Google at foretage verdensomspændende deindeksering – altså fjernelse af links fra alle versioner af søgemaskinen (google.com, google.ca osv.), ikke kun europæiske domæner.

EU-Domstolen fastslog, at:

EU-retten på nuværende tidspunkt ikke forpligter en søgemaskineoperatør, der imødekommer en anmodning om fjernelse af links, til at foretage en sådan fjernelse for alle versioner af søgemaskinen.

Domstolen præciserede dog, at deindekseringen som minimum skal være effektiv inden for EU's grænser. Søgemaskineoperatøren skal anvende foranstaltninger, der effektivt forhindrer EU-brugere i at få adgang til de pågældende links – herunder geoblokeringsteknikker. Derudover fastslog Domstolen, at den nationale tilsynsmyndighed under hensyntagen til de nationale grundlæggende rettigheder kan pålægge global deindeksering i konkrete sager.

Dommen balancerer mellem beskyttelsen af privatlivet og hensynet til, at tredjelandssstater har selvstændige retsordener og ikke nødvendigvis anerkender en EU-baseret ret til sletning. Resultatet er et **minimum-harmoniseringsprincip**: EU-retten kræver effektiv deindeksering inden for EU, men udelukker ikke, at nationale myndigheder kan gå videre.

LOV [Databeskyttelsesforordningen \(GDPR\) § 17, stk. 1](#)

PRAKSIS **EU-Domstolen** · Den geografiske rækkevidde af retten til at blive glemmt: Global eller EU-dækkende fjernelse af links? 24.09.2019

§ 4 Urigtige versus faktisk korrekte oplysninger – sletning og berigtigelse

I [C-460/20 \(TU og RE mod Google\)](#) præciserede EU-Domstolen reglerne for deindeksering af søgeresultater, der refererer til indhold, som den registrerede hævder er faktisk urigtigt.

Domstolen fastslog, at:

- Den registrerede har ret til at kræve deindeksering, når søgeresultaterne linker til indhold med påstået urigtige personoplysninger.
- Den registrerede behøver **ikke** at have opnået en retskendelse mod den oprindelige udgiver, men skal fremlægge relevante beviser for urigtigheden.

- Søgemaskineoperatøren skal foretage en selvstændig vurdering af, om den registreredes dokumentation er tilstrækkelig til at begrunde deindeksering.

Domstolen understregede dog, at søgemaskineoperatøren ikke har pligt til selv at efterforske oplysningens rigtighed – men skal reagere, når den registrerede fremlægger tilstrækkeligt bevis. Den dataansvarlige (søgemaskinen) bærer bevisbyrden for, at en undtagelse i art. 17, stk. 3, finder anvendelse.

For faktisk korrekte men *forældede* oplysninger – særligt gamle straffedomme – er praksis mere nuanceret. I [C-136/17 \(GC and Others\)](#) fastslog Domstolen, at oplysninger om straffedomme kræver en særlig streng interesseafvejning, og at der navnlig skal tages hensyn til:

- Hvor lang tid der er gået siden dommen
- Om den registrerede har afsonet sin straf
- Oplysningens aktualitet og samfundsmæssige relevans
- Om den registrerede er en offentlig person

I [C-37/20](#) tog Domstolen stilling til offentlige registre (her hvidvaskregistre med reelle ejere). Domstolen fastslog, at offentlig adgang til disse registre udgør et indgreb i den registreredes ret til privatliv, men at indgrebet kan være berettiget af hensyn til bekæmpelse af hvidvask og terrorfinansiering – forudsat at der er tilstrækkelige garantier mod misbrug.

LOV	Databeskyttelsesforordningen (GDPR) § 5	Databeskyttelsesforordningen (GDPR) § 17, stk. 1, 3
PRAKSIS	EU-Domstolen · Afvejning af retten til at blive glemt og informationsfriheden: Søgemaskiners ansvar ved urigtige oplysninger og miniaturebilleder 08.12.2022 EU-Domstolen · Ugyldighed af offentlig adgang til oplysninger om reelt ejerskab i hvidvaskdirektivet (Sag C-37/20 og C-601/20) 22.11.2022 EU-Domstolen · Søgemaskineudbyderes forpligtelser ved behandling af følsomme personoplysninger og retten til at blive glemt 24.09.2019	

§ 5 Datatilsynets praksis om sletning af personoplysninger

Datatilsynet behandler klager over manglende efterlevelse af sletteansmodninger i henhold til [GDPR art. 17](#) og [art. 77](#) (klage til tilsynsmyndigheden). Praksis viser, at Datatilsynet foretager en konkret vurdering af, om den dataansvarlige har haft tilstrækkelig hjemmel til at afvise en sletteansmodning.

I [sag 2019-31-1950](#) udtalte Datatilsynet **alvorlig kritik** af en privat virksomhed, der havde offentliggjort billeder af to klagere på sin hjemmeside og YouTube-kanal uden gyldigt samtykke og efterfølgende afvist deres sletteansmodninger. Datatilsynet fastslog, at virksomheden ikke havde dokumenteret gyldigt samtykke i overensstemmelse med [GDPR art. 6, stk. 1, litra a](#) og [art. 7](#), og at billederne derfor var behandlet ulovligt. Virksomheden blev pålagt at efterkomme sletteansmodningen.

Datatilsynet har endvidere i en række sager (herunder [sag 2019-32-0704](#), [sag 2019-31-1252](#) og [sag 2019-31-2538](#)) vurderet, om dataansvarlige har opfyldt deres forpligtelser i forbindelse med sletteansmodninger. De centrale principper i Datatilsynets praksis er:

- Den dataansvarlige skal have et klart og dokumenteret retsgrundlag for fortsat behandling, hvis en sletteansmodning afvises

- Afvisning af en sletteanmodning kræver, at den dataansvarlige konkret kan dokumentere, at en undtagelse i art. 17, stk. 3, finder anvendelse
- Der skal foretages en interesseafvejning, hvor oplysningens art, formålet med behandlingen og den registreredes interesse i sletning indgår
- Manglende reaktion på en sletteanmodning udgør i sig selv en overtrædelse af forordningen

For sager om søgemaskinedeindeksering specifikt henviser Datatilsynet til EU-Domstolens praksis, jf. Google Spain-doktrinen, og vurderer, om søgemaskineoperatøren har foretaget en tilstrækkelig interesseafvejning. Sager om sletning af [kreditoplysninger \(RKI/Experian\)](#) [behandles under en selvstændig praksisoversigt](#).

LOV	Databeskyttelsesforordningen (GDPR) § 6, stk. 1	Databeskyttelsesforordningen (GDPR) § 7
	Databeskyttelsesforordningen (GDPR) § 17, stk. 1, 3	
PRAKSIS	Datatilsynet · Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	12.12.2025
	Datatilsynet · Offentliggørelse af personoplysninger på hjemmeside under den journalistiske undtagelse	09.09.2020
	Datatilsynet · Alvorlig kritik af Københavns Kommune for ekstremt langsom sletningsproces	08.07.2020
	Datatilsynet · Alvorlig kritik af privat virksomhed for behandling uden gyldigt samtykke og manglende efterlevelse af sletteanmodning	18.05.2020
	Datatilsynet · Kritik af manglende overholdelse af frister for indsigt og sletning hos privat virksomhed	25.09.2019

§ 6 Den journalistiske undtagelse og forholdet til mediearkiver

I dansk ret er mediers behandling af personoplysninger i vidt omfang undtaget fra GDPR's materielle regler. [Databeskyttelsesloven § 3, stk. 5-8](#) implementerer [GDPR art. 85](#) ved at undtage informationsdatabaser, manuelle arkiver og behandling udelukkende i journalistisk øjemed fra forordningens kapitel II-VII og IX.

Undtagelsen medfører, at den registreredes ret til sletning efter GDPR art. 17 som udgangspunkt **ikke** gælder over for journalistiske medier, når behandlingen udelukkende sker i journalistisk øjemed. Den registrerede kan i stedet rette henvendelse til Pressenævnet efter de presseetiske regler, eller til Datatilsynet, der vil vurdere, om mediet opfylder betingelserne for undtagelsen.

Forarbejderne til databeskyttelsesloven § 3 understreger to centrale betingelser for undtagelsen:

Det er ikke tilstrækkeligt, at den dataansvarlige selv er af den opfattelse, at der er tale om behandling, som finder sted i journalistisk øjemed. Der påhviler således den pågældende en vis forpligtelse til at sandsynliggøre, at vedkommendes aktiviteter falder ind under undtagelsesreglen.

Og:

De nævnte regler gælder alene for behandling af oplysninger, som udelukkende finder sted i journalistisk øjemed [...]. Hvis behandlingen ikke kan anses for udelukkende at ske til de nævnte formål, finder loven og forordningens regler fuldt ud anvendelse.

Det er værd at bemærke, at selv under den journalistiske undtagelse finder GDPR's regler om behandlingssikkerhed (art. 32) og databehandlafter (art. 28) fortsat anvendelse, ligesom kapitel VIII om erstatning (art. 82) gælder fuldt ud.

[Straffelovrådets betænkning nr. 1563/2017 om freds- og ærekrænkelser](#) indeholder en grundig analyse af forholdet mellem GDPR art. 17 og straffelovens regler om sletning efter dom for freds- og ærekrænkelser (straffelovens § 271). Betænkningen konstaterer, at straffelovens slettehjemmel for tilfælde inden for GDPR's område blot får karakter af et retsmiddel til håndhævelse af den allerede eksisterende sletteforpligtelse efter art. 17, mens den for tilfælde uden for GDPR's område indebærer en selvstændig ret til sletning.

For den bredere praksis om [Datatilsynets generelle tilsynsvirksomhed](#) henvises til den særskilte praksisoversigt.

LOV

Databeskyttelsesforordningen (GDPR) § 85

Databeskyttelsesloven § 3, stk. 5-8

Medieansvarsloven § 1

§ 7 Pressenævnets praksis om sletning, anonymisering og afindeksering

Pressenævnet vurderer anmodninger om sletning, anonymisering og afindeksering efter de vejledende regler for god presseskik, navnlig punkt B.8 (privatlivets fred og genoptagelse af gamle straffesager) og punkt D.1 (tilgængelighed af historiske artikler). Nævnet understreger konsekvent, at GDPR-spørgsmål hører under Datatilsynet og domstolene – nævnets kompetence er begrænset til [medieansvarsloven § 34](#).

Pressenævnets praksis kan inddeles i tre typesituationer:

1. Gamle straffedomme og retssager

I [sag 17-70-01093](#) behandlede Pressenævnet en advokats anmodning om sletning af artikler fra 2010-2011 om en dom for kokainbesiddelse. Nævnet afviste sletning med henvisning til, at klageren selv havde udtalt sig offentligt om dommen og måtte anses for en offentlig kendt person. Oplysningerne blev ikke skønnet så belastende, at det var rimeligt at hindre tilgængeligheden. Nævnet udtalte derimod **kritik** af Ekstra Bladets fornyede omtale i 2017, hvor avisen fremdrog den gamle straffesag, efter at klageren havde anmodet om sletning – dette blev anset for at underminere selve hensynet bag punkt B.8.

I [sag 2022-80-0778](#) afviste Pressenævnet anonymisering af den såkaldte "tys-tys-kilde" i Se og Hør-sagen (dom: halvandet års ubetinget fængsel). Nævnet lagde vægt på sagens ekstraordinære samfundsmæssige interesse som en af Danmarkshistoriens største medieskandaler og klagerens misbrug af sin betroede stilling.

Sag	Dom/oplysning	Tid siden	Afgørelse	Begrundelse
17-70-01093	Bøde 20.000 kr. for kokain	7 år	Afvist sletning	Offentlig kendt, selv udtalt sig
2022-80-0778	1½ års fængsel (Se og Hør)	5½ år	Afvist anonymisering	Ekstraordinær samfundsmæssig interesse

2. Sletning ved lang tids forløb og ung alder

I [sag 2025-02-21 \(nazisme-artikel\)](#) udtalte Pressenævnet derimod **kritik** af Århus Stiftstidende for ikke at anonymisere en 15 år gammel lederartikel om en persons deltagelse i en nazistisk sammenhæng. Nævnet lagde afgørende vægt på klagerens **unge alder** på tidspunktet (18 år), at der var gået næsten 16 år, at aktiviteterne var enkeltstående, og at klageren ikke var en offentlig person. Artiklen blev ikke påbudt slettet – anonymisering var tilstrækkelig.

I [sag 2022-80-0825](#) fandt nævnet, at Berlingskes anonymisering af en artikel om en efterlysning (selvmordsfrygt) var tilstrækkelig til at opfylde kravene. Da alle identificerbare oplysninger var fjernet, kunne artiklen lovligt forblive i databasen.

3. Professionelt virke – brevkassesager

I tre parallelle sager fra september 2024 ([Viborg Stifts Folkeblad](#), [Folkebladet Lemvig](#) og [Dagbladet Ringkøbing-Skjern](#)) afviste Pressenævnet sletning af 13 år gamle brevkasseartikler om sex og samliv. Klageren, der tidligere var sexolog men nu arbejdede på en danseskole, påberåbte sig GDPR-sletteretten. Nævnet afviste med henvisning til, at:

- Oplysningerne stammede fra klagerens eget professionelle virke som brevkasseredaktør
- Artiklerne ikke indeholdt følsomme eller private oplysninger *om* klageren
- Artiklerne fortsat havde almen interesse
- Karriereskifte og ulønnet arbejde ikke ændrede den presseetiske vurdering

LOV	Medieansvarsloven § 34	Medieansvarsloven § 49	
PRAKSIS	Pressenævnet · Afvisning af klage over manglende anonymisering af artikel om personligt sygdomsforløb		21.02.2025
	Pressenævnet · Pressenævnet kritiserer avis for manglende anonymisering af 15 år gammel lederartikel		21.02.2025
	Pressenævnet · Pressenævnet afviser anmodning om sletning af gamle brevkasseartikler om sex og samliv		25.09.2024
	Pressenævnet · Pressenævnet afviser anmodning om sletning af 13 år gamle brevkasseartikler om sex og samliv		25.09.2024
	Pressenævnet · Pressenævnet afviser anmodning om sletning af brevkasseartikler om sex og samliv		25.09.2024
	Pressenævnet · Anmodning om sletning af anonymiseret artikel om efterlysning afvist		18.05.2022
	Pressenævnet · Pressenævnet afviser krav om anonymisering af "tys-tys-kilden" i artikler om Se og Hør-sagen		22.03.2022
	Pressenævnet · Pressenævnets vurdering af "retten til at blive glemt" i sag om gammel narkodom og ny medieomtale		05.04.2017

§ 8 Pressenævnets vurderingskriterier – punkt B.8 og D.1

Pressenævnets afgørelser om sletning og afindeksering bygger på to centrale bestemmelser i de vejledende regler for god presseskik:

Punkt B.8 vedrører privatlivets fred og mediernes omtale af gamle straffesager. Reglen tilsiger, at en person, der har begået en forseelse og enten er idømt straf eller har underkastet sig en bøde, ikke bør udsættes for unødigt genoptagelse af sagen i pressen, medmindre genoptagelsen er begrundet i offentlig interesse.

Punkt D.1 vedrører mediernes ansvar for at tage stilling til anmodninger om at hindre tilgængelighed af tidligere offentliggjorte, følsomme eller private oplysninger i digitale medier. Reglen pålægger mediet en aktiv stillingtagen til sådanne anmodninger.

På tværs af Pressenævnets praksis kan følgende vurderingskriterier identificeres:

-

Oplysningernes art og belastningsgrad: Er oplysningerne særligt belastende for den omtalte? Oplysninger om straffedomme, helbredsmæssige forhold og seksuelle forhold vurderes strengere end erhvervsmæssige oplysninger.

- **Tidsforløbet:** Jo længere tid der er gået, desto mere taler for sletning/anonymisering. 15-16 år gav medhold i nazisme-sagen; 5-7 år var utilstrækkeligt i Se og Hør-sagen og narkodomsagen.
- **Den registreredes rolle:** Offentlige personer og offentligt kendte har en svagere ret til sletning. Privatpersoner, særligt dem der var unge på gerningstidspunktet, har en stærkere beskyttelse.
- **Sagens alvor og samfundsmæssige interesse:** Alvorlige straffedomme og sager af vidtrækkende samfundsmæssig betydning taler mod sletning.
- **Frivillig medvirken:** I [sag om sygdomsforløb](#) lagde nævnet afgørende vægt på, at klageren selv havde henvendt sig til mediet og godkendt artiklen.
- **Anonymisering som alternativ:** Nævnet foretrækker ofte anonymisering (fjernelse af navn og identifikationsoplysninger) frem for fuld sletning, da dette balancerer privatlivshensyn med informationsfrihed.

Kriterium	Taler FOR sletning	Taler MOD sletning
Tidsforløb	> 10-15 år	< 5 år
Personens rolle	Privatperson, ung alder	Offentlig person, betroet stilling
Sagens karakter	Enkelstående, mindre forseelse	Alvorlig, systematisk, samfundsrelevant
Medvirken	Ufrivillig omtale	Klager selv henvendte sig til mediet
Oplysningsart	Straffedom, helbred, seksualitet	Erhvervsmæssigt virke

LOV

[Medieansvarsloven § 34](#)

PRAKSIS

- Pressenævnet** · Pressenævnet kritiserer avis for manglende anonymisering af 15 år gammel lederartikel 21.02.2025
- Pressenævnet** · Afvisning af klage over manglende anonymisering af artikel om personligt sygdomsforløb 21.02.2025
- Pressenævnet** · Pressenævnet afviser krav om anonymisering af "tys-tys-kilden" i artikler om Se og Hør-sagen 22.03.2022
- Pressenævnet** · Pressenævnets vurdering af "retten til at blive glemt" i sag om gammel narkodom og ny medieomtale 05.04.2017

§ 9 Sammenfatning – centrale retsprincipper for sletteretten

Praksis om retten til at blive glemt viser et retligt landskab, der er præget af en vedvarende spænding mellem privatlivsbeskyttelse og informationsfrihed. De centrale retsprincipper kan sammenfattes som følger:

EU-Domstolens niveauer: Sletteretten i GDPR art. 17 er udgangspunktet, men den er aldrig absolut. Søgmaskineoperatøren skal foretage en selvstændig interesseafvejning, der tager hensyn til oplysningens art, den registreredes rolle, offentlighedens informationsinteresse og det tidsrum, der er gået. Urigtige oplysninger har et stærkere sletningskrav end korrekte men forældede. Den geografiske rækkevidde er som minimum EU-dækkende, men kan udvides af nationale myndigheder.

Dansk praksis: Datatilsynet håndhæver sletteretten direkte og stiller krav om, at den dataansvarlige konkret dokumenterer sit retsgrundlag for fortsat behandling. Pressenævnet opererer med et selvstændigt presseetisk regelsæt (punkt B.8 og D.1), der i praksis fører til lignende afvejninger – dog med en klar bias mod at bevare det journalistiske arkivs integritet.

Den journalistiske undtagelse: Databeskyttelsesloven § 3, stk. 5-8, undtager journalistiske informationsdatabaser og behandling i journalistisk øjemed fra størstedelen af GDPR. Denne undtagelse er bred, men ikke ubegrænset – den kræver, at behandlingen *udelukkende* sker i journalistisk øjemed, og Datatilsynet (samt domstolene) kan gribe ind ved misbrug.

Anonymisering som mellemvej: Både Pressenævnet og Datatilsynet anerkender anonymisering som et proportionalt alternativ til fuld sletning. Fjernelse af identifikationsoplysninger kan opfylde den registreredes behov uden at krænke mediernes arkivfunktion eller offentlighedens informationsinteresse.

Den registrerede, der ønsker at påberåbe sig sletteretten, bør i første omgang rette henvendelse direkte til den dataansvarlige med en konkret identificeret URL/oplysning og anmodning om sletning. Hvis dette afvises, kan der klages til Datatilsynet efter [GDPR art. 77](#). For medier omfattet af medieansvarsloven kan anmodningen alternativt rettes til Pressenævnet efter punkt B.8/D.1. Endelig kan sagen indbringes for domstolene efter [GDPR art. 79](#).

LOV

[Databeskyttelsesforordningen \(GDPR\) § 17, stk. 1, 3](#)[Databeskyttelsesforordningen \(GDPR\) § 77](#)[Databeskyttelsesforordningen \(GDPR\) § 79](#)[Databeskyttelsesloven § 3, stk. 5-8](#)[Medieansvarsloven § 34](#)

REFERENCE Lovgrundlag

5 paragraffer

[Databeskyttelsesforordningen \(GDPR\) § 17](#) stk. 1, 3[Databeskyttelsesforordningen \(GDPR\) § 21](#) stk. 1[Databeskyttelsesforordningen \(GDPR\) § 85](#)[Databeskyttelsesloven § 3](#) stk. 5-8[Medieansvarsloven § 34](#)

MATERIALE Citerede afgørelser

19 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL

6

08.12.2022	Afvejning af retten til at blive glemt og informationsfriheden: Søgmaskiners ansvar ved urigtige oplysninger og miniaturebilleder	C-460/20
22.11.2022	Ugyldighed af offentlig adgang til oplysninger om reelt ejerskab i hvidvaskdirektivet (Sag C-37/20 og C-601/20)	C-37/20
01.08.2022	Offentliggørelse af private interesser og beskyttelse af følsomme personoplysninger i den offentlige sektor (Sag C-184/20)	C-184/20

24.09.2019	Søgemaskineudbyderes forpligtelser ved behandling af følsomme personoplysninger og retten til at blive glemt	C-136/17
24.09.2019	Den geografiske rækkevidde af retten til at blive glemt: Global eller EU-dækkende fjernelse af links?	C-507/17
08.03.2017	Begrænsning af offentlig adgang til personoplysninger i selskabsregistret efter virksomhedsopløsning – Foreneligheden mellem databeskyttelsesdirektiv 95/46 og selskabsdirektiv 68/151	C-398/15

PRESSENÆVNET · NÆVN / KLAGEINSTANS

8

21.02.2025	Afvisning af klage over manglende anonymisering af artikel om personligt sygdomsforløb	
21.02.2025	Pressenævnet kritiserer avis for manglende anonymisering af 15 år gammel lederartikel	
25.09.2024	Pressenævnet afviser anmodning om sletning af gamle brevkasseartikler om sex og samliv	
25.09.2024	Pressenævnet afviser anmodning om sletning af 13 år gamle brevkasseartikler om sex og samliv	
25.09.2024	Pressenævnet afviser anmodning om sletning af brevkasseartikler om sex og samliv	
18.05.2022	Anmodning om sletning af anonymiseret artikel om efterlysning afvist	2022-80-0825
22.03.2022	Pressenævnet afviser krav om anonymisering af "tys-tys-kilden" i artikler om Se og Hør-sagen	2022-80-0778
05.04.2017	Pressenævnets vurdering af "retten til at blive glemt" i sag om gammel narkodom og ny medieomtale	17-70-01093

DATATILSYNET · NÆVN / KLAGEINSTANS

5

12.12.2025	Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	2025-41-0139
09.09.2020	Offentliggørelse af personoplysninger på hjemmeside under den journalistiske undtagelse	2019-31-2538
08.07.2020	Alvorlig kritik af Københavns Kommune for ekstremt langsom sletningsproces	2019-32-0704
18.05.2020	Alvorlig kritik af privat virksomhed for behandling uden gyldigt samtykke og manglende efterlevelse af sletteanmodning	2019-31-1950
25.09.2019	Kritik af manglende overholdelse af frister for indsigt og sletning hos privat virksomhed	2019-31-1252

FORARBEJDE **Betænkninger**

1 reference

Straffelovrådets betænkning om freds- og ærekrænkelser

nr. 1563 · 2017 · Justitsministeriet

17

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over sletning fra RKI / Experian – kreditoplysningsbureauer (DBL §§ 19-22)

Tilladelseskrav, femårsreglen og angrebsmuligheder mod registrering efter databeskyttelseslovens kapitel 5

Version 2 · Opdateret 16. jul. 2026 · 25 afgørelser · 2002-2025

[Læs online](#)

INTRODUKTION

Kreditoplysningsbureauer som Experians RKI-register, Debitor Registret og Bisnode Kredit er underlagt en særlig national ramme i databeskyttelseslovens kapitel 5 (§§ 19-22), der supplerer og skærper databeskyttelsesforordningen. Rammen bygger på fire søjler: et forudgående tilladelseskrav med vilkår (§ 19, jf. § 26), en snæver afgrænsning af hvilke oplysninger der overhovedet må behandles (§ 20), formkrav til videregivelsen til abonnenter (§ 21) og en mulighed for at begrænse den registreredes rettigheder (§ 22). Praksis er fordelt på Datatilsynet som primær tilsyns- og klagemyndighed, på Det Finansielle Ankenævn – som prøver indberetterens ansvar, men afviser selve sletningsspørgsmålet – og på EU-Domstolen, hvis SCHUFA-domme fra december 2023 har flyttet retsstillingen om lagringsfrister og kreditscoring markant.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Femårsfristen i databeskyttelseslovens § 20, stk. 3, er en MAKSIMUMSFRIST – mister oplysningen sin betydning for kreditvurderingen tidligere, skal den slettes tidligere, og Datatilsynet har i fast praksis fastsat vejledende slettefrister, der er kortere end fem år.
- 02** Et kreditoplysningsbureau må ikke registrere en fordring, der er bestridt af skyldneren, medmindre fordringen har været forelagt en retslig instans – begrundelsen er, at der ellers registreres betalingsVILJE i stedet for betalingsEVNE.
- 03** En oplysning, der er forældet efter § 20, stk. 3, må heller ikke bruges som grundlag for en bedømmelse, selv om selve oplysningen ikke videregives.
- 04** Summariske oplysninger om skyldforhold må kun videregives, hvis kravet overstiger 1.000 kr. til samme kreditor OG kreditor har skyldnerens skriftlige erkendelse af forfalden gæld eller har foretaget retslige skridt – abonnenten bærer dokumentationsbyrden.
- 05** Oplysninger om endeligt godkendt gældssanering må aldrig videregives, jf. § 21, stk. 3, 2. pkt.

- 06 Oplysninger til abonnenter skal som hovedregel meddeles skriftligt; mundtlig meddelelse af summariske oplysninger kræver, at spørgerens navn og adresse noteres og opbevares i mindst 6 måneder.
- 07 Offentlige myndigheder må først indberette gæld, når den samlede forfaldne gæld overstiger 7.500 kr., administreres af samme inddrivelsesmyndighed, og der foreligger enten to rykkere og udpantningsret, udlæg, endelig dom eller skriftlig erkendelse.
- 08 Myndigheden skal give skyldneren skriftlig meddelelse mindst 4 uger før indberetning, og indberetningen skal undlades, hvis gælden betales, eller der indgås og overholdes en afdragsaftale.
- 09 En registrering af den SAMME fordring, der allerede burde have været slettet efter femårsreglen, kan ikke foretages på ny – det var afgørende i Det Finansielle Ankenævns sag 292/2014, hvor Datatilsynet underkendte en registrering foretaget 23 år efter gældens opståen.
- 10 Et pengeinstitut kan handle ansvarspådragende ved en uberettiget RKI-indberetning, men den registrerede skal selv løfte bevisbyrden for et konkret økonomisk tab – og Det Finansielle Ankenævn tilkender ikke godtgørelse for tort.
- 11 Det Finansielle Ankenævn afviser klager over selve RKI-registreringen og henviser dem til Datatilsynet; fogedretten kan heller ikke behandle et afregistreringskrav under en udlægssag – det kræver selvstændigt søgsmål.
- 12 Efter EU-Domstolens dom i C-26/22 (SCHUFA) må et kreditoplysningsbureau ikke lagre oplysninger om restgældsbe frielse længere end det offentlige insolvensregister, og tilsynsmyndighedens afgørelse er undergivet fuld domstolsprøvelse.
- 13 Efter C-634/21 (SCHUFA-scoring) udgør selve beregningen af en kreditscore en automatisk afgørelse efter forordningens artikel 22, når tredjemand lægger afgørende vægt på scoren.
- 14 Efter C-203/22 giver indsichtsretten krav på en reel forklaring af logikken bag scoringen; forretningshemmeligheder kan ikke i sig selv begrunde et blankt afslag, men fordrer en afvejning.
- 15 Erstatning efter forordningens artikel 82 kræver tre kumulative betingelser – overtrædelse, faktisk skade og årsagsforbindelse – men der gælder ingen bagatel- eller alvorstærskel for immateriel skade, jf. C-300/21 og C-456/22.
- 16 Datatilsynet er ikke forpligtet til at pålægge en sanktion, når en overtrædelse konstateres, hvis indgriben ikke er passende, nødvendig og forholdsmæssig, jf. C-768/21 – den registrerede har ingen subjektiv ret til at kræve en bøde.
- 17 Overtrædelse af §§ 20, 21 eller tilsidesættelse af Datatilsynets vilkår straffes med bøde eller fængsel indtil 6 måneder, og retten til at drive kreditoplysningsvirksomhed kan frakendes ved dom efter § 43.

Tilladelseskravet i § 19 – hvem er overhovedet et kreditoplysningsbureau?

§ 1

Efter [databeskyttelseslovens § 19](#) skal den, der ønsker at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse, indhente tilladelse fra Datatilsynet, **inden** behandlingen påbegyndes. Hjemlen findes i [§ 26, stk. 1, nr. 2](#), og efter [§ 26, stk. 4](#) kan tilsynet fastsætte **vilkår** for behandlingen til beskyttelse af de registreredes privatliv. Det er denne vilkårsadgang – ikke lovteksten – der i praksis bærer de detaljerede slettefrister, som RKI og de øvrige bureauer arbejder efter.

Forarbejderne til § 19 afgrænser anvendelsesområdet bredere, end man umiddelbart skulle tro:

»Ordene »driver virksomhed med« er indsat for at præcisere, at bestemmelsen ikke omfatter virksomheder eller andre, der i enkeltstående tilfælde eller lejlighedsvis skaffer sig, registrerer og videregiver soliditetsoplysninger til konkrete formål, f.eks. advokater. Derimod er det ikke herved sigtet til at begrænse bestemmelsen til kun at omfatte registreringsaktiviteter, der drives som traditionelle erhvervsvirksomheder [...] Eksempelvis vil også foreninger, der registrerer og videregiver soliditetsoplysning til medlemmerne, efter omstændighederne være omfattet af bestemmelsen.«

Afgørende er alene, at den pågældende indsamler og registrerer soliditetsoplysninger **med henblik på videregivelse**. Forarbejderne slår desuden fast, at det ikke hjælper at pakke aktiviteten ind i anden virksomhed:

»Selvom virksomheden tillige og måske som hovedformål driver anden form for erhvervsvirksomhed, f.eks. inkassovirksomhed, bringer dette ikke virksomheden uden for kapitel 5, hvis betingelserne i § 19 er opfyldt.«

Det er en praktisk vigtig pointe: inkassobureauer, der ved siden af inddrivelsen opbygger og sælger adgang til skyldnerdata, kan uden videre være omfattet af tilladelseskravet.

Behovet for kontrol med bureauerne blev allerede begrundet i [Delbetænkning om private registre \(betænkning nr. 687/1973\)](#), s. 40:

»[D]a kreditoplysningsbureauerne indsamler oplysninger af fortrolig karakter om personer og virksomheder, ofte uden de pågældendes viden, og da disse oplysninger ofte ved videregivelsen kan få væsentlig indflydelse på de pågældende virksomheders og personers dispositionsmuligheder [...] bør der gennemføres en kontrol med bureauerne.«

Hvordan et sådant bureau faktisk ser ud, er beskrevet i Sø- og Handelsrettens dom **V-0060-01 (V-0060-01-)**, hvor RKI fik forbudt konkurrenten PKI at bruge sit navn. Dommen dokumenterer RKI's historie – etableret i 1971 af familien Riber som Ribers Kredit Information, overtaget af The Thomson Corporation i 1984 – og markedspositionen: i 2000 havde bureauet 10.283 virksomhedskunder og afgav over 3,5 mio. kreditoplysninger. Sagen illustrerer, at kreditoplysningsvirksomhed i Danmark reelt er koncentreret hos ganske få aktører, hvilket gør en enkelt fejlregistrering desto mere indgribende.

LOV

[Databeskyttelsesloven § 19](#)[Databeskyttelsesloven § 26, stk. 1, 4](#)

PRAKSIS

Sø- og Handelsretten · Varemærkekrænkelse: Forvekslelighed mellem RKI og PKI i kreditoplysningsvirksomhed

25.06.2002

§ 20, stk. 1 og 2 – relevanskravet og det absolutte forbud mod at registrere bestridte fordringer

§ 2

[Databeskyttelseslovens § 20, stk. 1](#) fastslår, at kreditoplysningsbureauer **kun** må behandle oplysninger, »som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed«. Bestemmelsen viderefører persondatalovens § 20, og forarbejderne understreger, at »[d]en gældende praksis på området vil dermed fortsat være af betydning« – en kontinuitet der rækker helt tilbage til lov om private registre.

Den praktisk vigtigste sætning i hele kapitel 5 står i forarbejderne til stk. 1, og den er kernen i den hyppigste angrebsmulighed mod en registrering:

»Det betyder endvidere bl.a., at et kreditoplysningsbureau ikke må registrere oplysninger om fordringer, der er bestridt af skyldneren, såfremt fordringen ikke har været forelagt en retslig instans. Baggrunden herfor er, at der i så fald ikke er tale om registrering af oplysninger om betalingsevne, men derimod registrering af oplysninger om betalingsvilje.«

Sondringen mellem betalingsEVNE og betalingsVILJE er afgørende. Et kreditoplysningsbureau er ikke et pressionsmiddel i en civilretlig tvist. Bestrider skyldneren fordringen – helt eller delvist – og foreligger der ikke dom, udlæg eller anden retslig afgørelse, falder oplysningen uden for det, bureauet overhovedet har lov at behandle. Samme forståelse blev formuleret allerede af Registerudvalget i [betænkning nr. 1345/1997, s. 104](#):

»Registertilsynet har på baggrund af bestemmelsen givet udtryk for, at der ikke må ske registrering af fordringer, som bestrides af debitor, medmindre fordragens størrelse eller eksistens er fastslået ved en endelig domstolsafgørelse.«

Betænkningen tilføjer det kriterium, der binder relevanskravet sammen: »Det er afgørende for, om en oplysning må registreres og videregives, at den har betydning for vurderingen af den registreredes betalingsevne i **andre fremtidige** skyldforhold.«

Relevanskravet afgrænser også bureauets virkefelt. Forarbejderne siger, at et bureau ikke må indsamle oplysninger om f.eks. faglige evner og dermed »virke som en art ”ansættelsesnævn” for private virksomheder« – en formulering der går ubrudt tilbage til [betænkning nr. 687/1973, s. 63](#). Endvidere gælder, at når et bureau registrerer oplysninger om en person eller virksomhed, »må oplysningerne kun vedrøre netop denne person eller virksomhed« – et forbud mod smitte fra ægtefælle, samlever eller koncernforbundne selskaber.

[§ 20, stk. 2](#) supplerer med et **absolut** forbud mod at behandle følsomme oplysninger efter [forordningens artikel 9, stk. 1](#) og oplysninger om strafbare forhold efter [artikel 10](#). Forarbejderne erkender, at forbuddet i vidt omfang er overflødigt ved siden af stk. 1, men begrundet det selvstændigt:

»At der desuagtet er fastsat et forbud i stk. 2 og herved fjernet enhver fortolkningstvivl omkring disse præcist angivne oplysninger, skyldes, at der er tale om oplysninger af følsom karakter, hvis registrering ikke blot vil være i strid med hensynet til det enkelte menneskets frihed, men også med et ønske om at beskytte minoritetsgrupper.«

Endelig udvider [§ 20, stk. 4](#) forordningens artikel 12-19 til også at gælde behandling af oplysninger om **virksomheder**, når behandlingen udføres for et kreditoplysningsbureau. Registrerede selskaber har dermed samme ret til indsigelse, berigtigelse og sletning som fysiske personer – en national særregel uden modstykke i forordningen.

§ 3 Femårsreglen i § 20, stk. 3 – en maksimumsfrist, ikke en ret til fem års registrering

Databeskyttelseslovens § 20, stk. 3 bestemmer, at oplysninger om forhold, der taler imod kreditværdighed, og som er mere end 5 år gamle, ikke må behandles, »medmindre det i det enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for bedømmelsen af den pågældendes økonomiske soliditet og kreditværdighed«.

Den udbredte misforståelse er, at bestemmelsen giver bureauet ret til at registrere i fem år. Det gør den ikke. Konkursrådet formulerer det utvetydigt i [betænkning nr. 1578/2022, s. 117](#):

»Femårsfristen i § 20, stk. 3, er en maksimumsfrist. Hvis en oplysning på et tidligere tidspunkt end efter fem år har mistet sin betydning for kreditvurdering, skal der ske sletning tidligere. Ifølge Datatilsynets faste praksis er der fastsat særlige vejledende slettefrister, som er kortere end fem år.«

De kortere frister udspringer af de vilkår, Datatilsynet knytter til tilladelsen efter § 26, stk. 4, og de varierer efter gældspostens type. Overtrædelse af et vilkår er selvstændigt strafbelagt, jf. § 41, stk. 2, nr. 8.

Undtagelsen – »åbenbart [...] af afgørende betydning« – er tilsigtet ganske snæver. Forarbejderne begrundes den alene med insolvensforhold:

»Adgangen til i meget begrænset omfang at registrere eller videregive oplysninger om forhold, der er mere end 5 år gamle er medtaget, fordi navnlig visse former for betalingsstandsning, som f.eks. konkurs, efter omstændighederne fortsat kan være så relevante for den økonomiske bedømmelse, at der bør være adgang til at videregive oplysningen om forholdet ud over 5-årsfristen.«

To yderligere afgrænsninger fremgår af forarbejderne. For det første rammer femårsreglen kun **negative** oplysninger: »Objektive oplysninger, som f.eks. identifikationsoplysninger, bør ifølge sagens natur ikke være genstand for forældelse [...] Der ses heller ikke at være behov for en forældelsesregel vedrørende oplysninger, der er ”positive” for den pågældende.« For det andet – og det er den bestemmelse, bureauerne oftest overser – gælder et brugsforbud, ikke blot et videregivelsesforbud:

»Kreditoplysningsbureauet må endvidere ikke benytte en oplysning, der er forældet efter denne bestemmelse, som grundlag for en bedømmelse, selv om selve oplysningen ikke herved videregives.«

En forældet gældspost må altså heller ikke indgå som skjult variabel i en scoringsmodel.

Det Finansielle Ankenævns sag **292/2014 (292/2014)** viser reglens gennemslagskraft. Klageren havde i 1987 optaget et lån på 153.000 kr. i Danske Bank; efter en tvangsauktion i 1988 stod banken med et udækket krav. Selvom betingelserne for registrering var opfyldt allerede i 1988, indberettede banken først til Experian den 6. april 2011. Datatilsynet fandt ved afgørelse af 6. september 2013 – efter at have genoptaget sagen på nye oplysninger – at registreringen var uberettiget, fordi en registrering skulle have været slettet senest fem år efter 1988, og fordi **samme fordring ikke må registreres igen**. Sagen fastslår dermed to ting: femårsfristen løber fra det forhold, der taler imod kreditværdighed – ikke fra indberetningstidspunktet – og kreditor kan ikke nulstille fristen ved at genindberette en gammel fordring.

Modsat forholdt det sig i **66/2018 (66/2018)**, hvor Danske Bank blev frifundet for en RKI-indberetning foretaget ti år efter misligholdelsen. Afgørelsen trækker på persondatalovens § 4, stk. 1, om god databehandlingsskik og [retsplejelovens § 477 e, stk. 2](#) om betalingspåkrav. Sammenholdt med 292/2014 tegner der sig det mønster, at det ikke i sig selv diskvalificerer en indberetning, at der er gået lang tid siden misligholdelsen, når fordringen fortsat er retskraftig og ikke tidligere har været registreret og slettet – mens en **genregistrering** af en fordring, der allerede burde være slettet, er udelukket.

Særligt om insolvens fremgår det af [betænkning nr. 1578/2022, s. 119](#), at Konkursrådet har overvejet »den nugældende ordning, hvor en skyldner, der har været under konkurs, fortsat kan være registreret hos et kreditoplysningsbureau i op til to år efter gældssanering«. Rådet noterer, at hensynet til potentielle långivere alternativt kan varetages gennem udelukkelsesgrundene for gældssanering frem for gennem fortsat registrering.

LOV

[Databeskyttelsesloven § 20, stk. 3](#)[Databeskyttelsesloven § 26, stk. 4](#)[Databeskyttelsesloven § 41, stk. 2](#)

PRAKSIS	Det finansielle ankenævn · Danske Bank frifundet for RKI-indberetning foretaget ti år efter misligholdelse	21.08.2018
	Det finansielle ankenævn · Krav om erstatning for uberettiget RKI-registrering foretaget 23 år efter gældens opståen	20.08.2015

§ 21 – formkrav til videregivelsen og 1.000-kroners-tærsklen for summariske skyldoplysninger

[Databeskyttelseslovens § 21, stk. 1](#) bestemmer, at oplysninger om økonomisk soliditet og kreditværdighed til abonnenter **kun må meddeles skriftligt**. Summariske oplysninger kan dog gives mundtligt, hvis spørgerens navn og adresse noteres og opbevares i mindst 6 måneder.

Skriftlighedskravet er ikke formalisme. Forarbejderne forklarer formålet:

»Herved sikres fornødent bevis for, hvad der er oplyst til tredjemand, hvilket er et nødvendigt led i den kontrol mv., der etableres efter reglerne i lovforslagets kapitel 5.«

Og noteringspligten ved mundtlige oplysninger tjener et konkret retsbeskyttelsesformål: »Notering af navn og adresse på spørgeren er nødvendig af hensyn til forordningens artikel 19, hvorefter den dataansvarlige underretter hver modtager, som personoplysningerne er videregivet til, om enhver berigtigelse eller sletning«. Uden noteringen kan bureauet ikke opfylde [forordningens artikel 19](#), når registreringen viser sig forkert – og den registrerede efterlades med en fejl, der er spredt til modtagere, ingen kan identificere. Seksmånedersfristen er begrundet i, at »forespørgere normalt kun vil benytte nyligt indhentede oplysninger som grundlag for kreditværdighedsvurderinger«.

Den materielt vigtigste regel står i [§ 21, stk. 3](#). Summariske oplysninger om skyldforhold må kun videregives, hvis oplysningerne hidrører fra Statstidende, er indberettet af en offentlig myndighed efter kapitel 4, eller hvis **begge** følgende er opfyldt:

- skyldforholdet vedrører **samme kreditor** og overstiger **1.000 kr.**, og
- kreditor har enten erhvervet den registreredes **skriftlige erkendelse** af en forfalden gæld, **eller** der er foretaget **retslige skridt** mod den pågældende.

Forarbejderne præciserer, at bevisbyrden ligger hos indberetteren: »[A]bonnenterne [er] forpligtede til at dokumentere, at fordringen er større end 1.000 kr., samt at debitor har erkendt den forfaldne gæld enten i form af en underskrevet skylderklæring eller et frivilligt forlig, eller at kreditor har foretaget retslige skridt mod debitor, f.eks. udtaget stævning.«

To yderligere begrænsninger følger af bestemmelsen. Oplysninger om **endeligt godkendt gældssanering må ikke videregives** ([§ 21, stk. 3, 2. pkt.](#)) – et absolut forbud. Og efter [§ 21, stk. 3, 3. pkt.](#) gælder betingelserne

»tillige for videregivelse af summariske oplysninger om skyldforhold i forbindelse med udarbejdelse af **bredere kreditbedømmelser**«. Man kan altså ikke omgå tærsklen ved at indbæge den utilstrækkeligt dokumenterede gældspost i en samlet vurdering.

§ 21, stk. 2 begrænser publikationer til abonnenter og forbyder personnumre heri. Forarbejderne begrundet abonnentkravet med hensynet til den private fred: oplysningerne »er dog ofte af så privat karakter, at en egentlig offentliggørelse ville kunne føles som en krænkelse af den private fred«. Offentligt salg må ikke finde sted – hverken »ved salg f.eks. via boghandlere, ved salg i butikker eller online, men også ved salg til enhver direkte fra bureauet«.

§ 21, stk. 4 forbyder videregivelse af summariske oplysninger om enkeltpersoners skyldforhold på en måde, der kan danne grundlag for vurdering af **andre** end den pågældende. Forarbejderne forudsætter dog, at bestemmelsen »ikke er til hinder for, at kreditoplysningsbureauerne videregiver oplysninger opdelt efter postnumre«, med henvisning til [betænkning nr. 1345/1997, s. 281 f.](#)

RKI-registrets praktiske indretning er beskrevet i [betænkning nr. 1578/2022, s. 119](#) og afspejler § 21 direkte:

»En indberetning fra en fordringshaver til RKI-registeret om en dårlig betaler skal indeholde fundamentet for kravet, som kan være en dom, et udlæg, en skylderkendelse mv., navn på fordringshaveren, beløbets størrelse, indberetningsdato samt slettedato. [...] Foreligger der ikke et fundament for fordringshaverens krav, fremgår en indberetning kun af et lukket register, hvor indberetningen kun er tilgængelig for indberetteren selv.«

Betænkningen tilføjer, at når konkurs eller gældssanering er indledt, kan der ikke indberettes yderligere krav, men allerede indberettede krav bliver stående.

LOV

Databeskyttelsesloven § 21, stk. 1-4

§ 5 Underretning før registrering – offentlig gæld efter §§ 16-18 og pengeinstitutternes særregler

Kravene til, hvad der skal gå forud for en indberetning, er skarpest for **offentlig gæld**. Efter [databeskyttelseslovens § 16, stk. 1, nr. 2](#) kan gæld til det offentlige kun videregives, hvis den samlede gæld er forfalden og **overstiger 7.500 kr.**, og der må ikke heri indgå gældsposter omfattet af en **overholdt** aftale om henstand eller afdragsvis betaling. Hertil kommer to kumulative betingelser:

- [§ 16, stk. 2](#): den samlede gæld skal administreres af **samme inddrivelsesmyndighed**, og
- [§ 16, stk. 3](#): gælden skal kunne inddrives ved udpanthning **og** der skal være fremsendt **to rykkere**, eller der skal være foretaget/forsøgt foretaget **udlæg**, eller kravet skal være fastslået ved **endelig dom**, eller det offentlige skal have erhvervet skyldnerens **skriftlige erkendelse** af den forfaldne gæld.

[§ 17, stk. 1](#) pålægger myndigheden at give skyldneren skriftlig meddelelse forinden, og videregivelse må **tidligst ske 4 uger efter**. Meddelelsen skal efter [§ 17, stk. 2](#) angive hvilke oplysninger der videregives, til hvilket bureau, hvornår – og:

»at videregivelse ikke vil ske, hvis betaling af gælden sker inden videregivelsen eller der indrømmes henstand eller indgås og overholdes en aftale om afdragsvis betaling.«

Dette er en **materiel** betingelse, ikke blot en oplysningspligt: betales gælden, eller indgås og overholdes en afdragsordning inden fristens udløb, må registreringen ikke gennemføres. Fire angrebepunkter følger direkte af §§ 16-17: manglende eller for sen underretning, gæld under 7.500 kr., sammenlægning af gæld fra flere inddrivelsesmyndigheder, og medregning af poster omfattet af en overholdt afdragsaftale. § 18 bemyndiger vedkommende minister til at fastsætte skærpede regler for bestemte gældstyper.

For **pengeinstitutter** gælder en særskilt ramme i [bekendtgørelse om pengeinstitutters videregivelse af kreditoplysninger](#). Efter § 1 skal instituttet inden 4 uger efter første videregivelse give kunden meddelelse herom, og efter § 2 må videregivelse ikke ske, hvis kunden skriftligt har frabedt sig det. § 3 giver kunden ret til inden 4 uger at få oplyst indholdet af kreditoplysninger videregivet inden for de sidste 6 måneder samt kategorien af modtagere og oplysningernes kilde – mod højst 200 kr. ved skriftligt svar. Den skarpeste bestemmelse er § 4:

»Har et pengeinstitut videregivet en kreditoplysning, der viser sig at være urigtig eller vildledende, skal pengeinstituttet straks berigtige oplysningen samt give skriftlig underretning om berigtigelsen til kunden og til alle, der har modtaget kreditoplysningen inden for de sidste 6 måneder, før pengeinstituttet blev bekendt med forholdet.«

Berigtigelsespligten er altså **aktiv og udadrettet** – det er ikke nok at rette i eget system. Efter § 5 skal en anmodning om berigtigelse besvares skriftligt inden 4 uger, og nægter instituttet, kan kunden inden 4 uger indbringe spørgsmålet for Datatilsynet, som træffer afgørelse; svaret skal indeholde klagevejledning. Efter § 6 gælder bekendtgørelsen også for oplysninger om virksomheder.

Den skærpede stilling for de finansielle indberettere har historiske rødder. [Betænkning nr. 1345/1997, s. 104](#) beskriver, at pengeinstitutter, forsikringsselskaber og realkreditinstitutter er underlagt særlige retningslinjer fra Finanstilsynet, netop fordi de er bundet af tavshedspligt:

»Der kan derfor først ske indberetning til et kreditoplysningsbureau, når der foreligger en retslig afgørelse i sagen, f.eks. i form af en dom eller fogedrettens opgørelse af kravet.«

Spørgsmålet om, hvornår et pengeinstitut lovligt kan overdrage til inkasso og videregive oplysninger til kreditvurdering, blev prøvet i [69/2015 \(69/2015\)](#), der behandler samspillet med tavshedspligten i [lov om finansiell virksomhed § 117](#).

LOV

[Databeskyttelsesloven § 16, stk. 1-3](#)
[Databeskyttelsesloven § 17, stk. 1, 2](#)
[Databeskyttelsesloven § 18](#)

PRAKSIS

Det finansielle ankenævn · Spørgsmål om berettigelse af inkassooverdragelse og videregivelse af oplysninger til kreditvurdering

04.03.2016

§ 6 EU-Domstolens SCHUFA-domme – lagringsfrist, scoring og fuld domstolsprøvelse

Den 7. december 2023 afsagde EU-Domstolen to domme, der har flyttet retsstillingen for kreditoplysningsbureauer i hele Unionen, og som må inddrages ved enhver fortolkning af §§ 20-22.

C-26/22 (C-26/22) angik grænserne for kreditoplysningsbureauers datalagring og prøvelsen af tilsynsmyndighedens afgørelser. Dommen bygger på [forordningens artikel 6](#), [artikel 17](#), [artikel 40](#) og [artikel 78](#) sammenholdt med insolvensforordningen (EU) 2015/848. Kernen er, at et privat bureau ikke kan påberåbe

sig en legitim interesse i at lagre oplysninger om insolvensbehandling og restgældsbefrielse **længere**, end oplysningen er offentligt tilgængelig i det offentlige register – og at tilsynsmyndighedens afgørelse er undergivet **fuld domstolsprøvelse**, ikke blot en legalitetskontrol. For dansk ret betyder det, at en branchekutyme om at fastholde en insolvensoplysning ud over den offentlige tilgængelighedsperiode ikke i sig selv kan bære registreringen; den må stå sin prøve på interesseafvejningen.

C-634/21 (C-634/21) angik SCHUFA's kreditscoring. OQ fik afslag på et lån hos en bank på grundlag af en negativ sandsynlighedsværdi (score), som SCHUFA havde beregnet ud fra en matematisk-statistisk model, der placerede ham i en gruppe med lignende karakteristika. SCHUFA oplyste scorens niveau og en generisk beskrivelse af metoden, men afviste at videregive de konkrete variabler og deres vægtning under henvisning til forretningshemmeligheder. Sagens kerne var [forordningens artikel 22](#):

»Den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.«

Dommen fastslår, at **selve beregningen af scoren** hos bureauet udgør en automatisk afgørelse i artikel 22's forstand, når tredjemand (banken) lægger afgørende vægt på scoren ved sin beslutning. Konsekvensen er betydelig: bureauet – og ikke kun kreditgiveren – bliver ansvarssubjekt for artikel 22's garantier. Det harmonerer med [§ 20, stk. 3](#)-forarbejdernes brugsforbud: en forældet oplysning må ikke indgå i bedømmelsen, selv om den ikke videregives.

C-203/22 (C-203/22) af 27. februar 2025 førte tråden videre og præciserede indsichtsretten i kreditvurderings-scoring: hvilke krav stilles til forklaringen af logikken bag automatiske afgørelser efter [artikel 15](#), og hvordan afvejes den mod forretningshemmeligheder efter direktiv (EU) 2016/943? Dommen understreger, at et blankt afslag med henvisning til forretningshemmeligheder ikke er tilstrækkeligt – der skal foretages en reel afvejning, og den registrerede har krav på en meningsfuld forklaring.

Dette har direkte betydning for rækkevidden af [§ 22, stk. 1](#), hvis forarbejder ellers rummer en forholdsvis rummelig undtagelse:

»Vedrørende den indsichtsret, der følger af forordningens artikel 15, stk. 1, litra h, om information om forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, vil den dataansvarlige eksempelvis ikke være forpligtet til at udlevere oplysninger, som må anses for at være forretningshemmeligheder, eller som er beskyttet efter den immaterielle lovgivning, herunder ophavsretsloven.«

Efter C-203/22 må denne forarbejdspassage læses EU-konformt: undtagelsen kan ikke anvendes som et generelt skjold, men kun efter en konkret afvejning oplysning for oplysning.

C-46/23 (C-46/23) supplerer med, at en tilsynsmyndighed **ex officio** kan påbyde sletning af ulovligt behandlede personoplysninger efter [artikel 58](#), jf. [artikel 17](#) – også uden anmodning fra den registrerede. Datatilsynet kan altså gribe ind af egen drift over for en systematisk fejlpraksis hos et bureau.

LOV

[Databeskyttelsesforordningen § 17](#)
[Databeskyttelsesforordningen § 22, stk. 1](#)
[Databeskyttelsesloven § 22, stk. 1](#)

PRAKSIS	EU-Domstolen · Indsichtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	27.02.2025
	EU-Domstolen · Tilsynsmyndighedens beføjelse til ex officio at påbyde sletning af ulovligt behandlede personoplysninger under GDPR	14.03.2024

EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
EU-Domstolen · Automatisk kredit scoring som en individuel afgørelse efter GDPR	07.12.2023

§ 7 § 22 – hvornår kan bureauet nægte indsigt og oplysning?

Databeskyttelseslovens § 22, stk. 1 tillader, at [forordningens artikel 13, stk. 1-3, artikel 14, stk. 1-4, artikel 15 og artikel 34](#) fraviges, »hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv«. [Stk. 2](#) rummer det tilsvarende for offentlige interesser.

Bestemmelsen er den mest oversete i kapitel 5 – og den, bureauerne oftest strækker for langt. Forarbejderne opstiller fire markante begrænsninger.

For det første er tærsklen høj: »Med anvendelsen af udtrykket »afgørende« i bestemmelsen er det tilkendegivet, at undtagelse fra oplysningspligten og indsigtsretten kun kan gøres, hvor der er **nærliggende fare** for, at privates interesser vil lide skade af **væsentlig betydning**.«

For det andet skal afvejningen foretages atomistisk:

»Afvejningen må foretages for hver enkelt oplysning for sig med den virkning, at der, såfremt sådanne hensyn kun gør sig gældende for en del af de [...] nævnte oplysninger, skal gives den registrerede meddelelse om de øvrige oplysninger.«

For det tredje – og det er den skarpeste sætning – findes der ingen kategorisk undtagelse:

»Der er ikke efter bestemmelsen adgang til generelt at undtage bestemte former for behandling af oplysninger fra indsigtsretten.«

Et bureau kan altså ikke undtage »scoringsmodellen« som kategori. Det skal begrunde konkret, oplysning for oplysning.

For det fjerde anerkender forarbejderne dog reelle forretningshensyn:

»Efter en konkret vurdering vil det være muligt at nægte indsigt i oplysninger, hvis dette vil medføre, at virksomhedens forretningsgrundlag, forretningspraksis eller know-how derved vil lide væsentlig skade. Det vil endvidere efter en konkret vurdering være muligt at nægte indsigt i interne vurderinger af, hvorvidt virksomheden på basis af foreliggende oplysninger vil indgå et kontraktforhold, ændre et bestående kontraktforhold, stille særlige vilkår for fortsættelse, eventuelt helt opsige et kontraktforhold og lignende tilfælde.«

Grænsen mellem den fjerde og den tredje begrænsning er netop det, EU-Domstolen skærpede i **C-203/22** ([C-203/22](#)): forretningshemmeligheder er et lovligt hensyn, men ikke et argument der på egen hånd afgør sagen.

Det er værd at bemærke, at [§ 22, stk. 3-stk. 8](#) angår offentlige myndigheder, domstole, videnskabelige formål, politiets efterforskning, Procesbevillingsnævnet og Folketingets Ombudsmand – de har ingen betydning for private kreditoplysningsbureauer. Stk. 7 og 8 blev indsat med virkning fra 1. januar 2024. Databeskyttelsesloven er senest konsolideret ved lovbekendtgørelsen af 22. marts 2024, og der er ingen vedtagne, men endnu ikke konsoliderede ændringer af kapitel 5.

Endelig fastslår [§ 20, stk. 4](#) sammenholdt med forarbejderne, at også **virksomheder** har krav på artikel 12-19-rettighederne, når et bureau behandler oplysninger om dem: »Bestemmelsen indebærer, at også

registrerede virksomheder mv. [...] har samme ret (som ved registrering af personoplysninger) til at gøre indsigelse og få berigtiget samt slettet oplysninger mv.«

LOV

Databeskyttelsesloven § 20, stk. 4

Databeskyttelsesloven § 22, stk. 1-8

PRAKSIS

EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder 27.02.2025

§ 8 Klageadgang og kompetencefordeling – Datatilsynet, ankenævnene og domstolene

Kompetencefordelingen er en fælde for den uforberedte. **Det Finansielle Ankenævn afviser klager over selve RKI-registreringen.**

Det fremgår tydeligt af **137/2021 (137/2021)**. Klageren havde ved forlig i fogedretten den 30. november 2018 aftalt med Sparekassen Danmark, at hun skulle slettes fra RKI, når et gælds-brev var underskrevet og afdragene betalt uden anmærkninger i tre måneder. Da tvist opstod om, hvorvidt betingelserne var opfyldt, indbragte hun sagen. Ankenævnet afviste den i sin helhed:

- Efter nævnets vedtægter § 5, stk. 1, litra e, afvises klager, der har været behandlet af en domstol – og fogedretten havde allerede den 15. marts 2021 taget stilling til kravet og indsigelserne.
- Spørgsmålet om **sletning i RKI** kan slet ikke behandles af nævnet; efter vedtægternes § 4 henvises sådanne klager til **Datatilsynet**, da det vedrører offentligretlig regulering af databehandling.

Og fogedretten kan heller ikke levere. Fogedretten bemærkede i sagen udtrykkeligt, at »kravet om afregistrering fra RKI ikke kunne behandles under en udlægssag, men krævede en selvstændig civil retssag«. Den registrerede står altså med tre – og kun tre – reelle veje: klage til Datatilsynet efter **forordningens artikel 77**, selvstændigt civilt søgsmål mod bureauet eller indberetteren efter **artikel 79**, eller – hvor det er indberetterens **ansvar** og ikke registreringen som sådan, der prøves – klage til Det Finansielle Ankenævn.

Hvad kan man forvente af Datatilsynet? Her sætter EU-Domstolen en vigtig forventningsafstemning. I **C-768/21 (C-768/21)** af 26. september 2024 fastslog Domstolen:

»Artikel 57, stk. 1, litra a) og f), artikel 58, stk. 2, og artikel 77, stk. 1, i forordning (EU) 2016/679 skal fortolkes således, at tilsynsmyndigheden i tilfælde af, at der konstateres et brud på persondatasikkerheden, ikke er forpligtet til at vedtage en korrigerende foranstaltning, særligt en administrativ bøde, i henhold til artikel 58, stk. 2, når en sådan indgriben ikke er passende, nødvendig eller forholdsmæssig med henblik på at afhjælpe den konstaterede mangel og sikre fuld overholdelse af denne forordning.«

Domstolen understregede samtidig, at klageren »ikke [har] en subjektiv ret til at anmode om, at tilsynsmyndigheden skal pålægge en administrativ bøde« (præmis 41), og at myndigheden i undtagelsestilfælde kan undlade indgriben, når »den konstaterede overtrædelse ikke har været ved« (præmis 43). Men skønnet er ikke frit: myndigheden har pligt til at behandle klagen »med den fornødne omhu«, og når en tilsidesættelse konstateres, har den »pligt til at reagere på en passende måde med henblik på at afhjælpe det konstaterede utilstrækkelige beskyttelsesniveau« (præmis 33).

Modvægten er domstolsprøvelsen. **C-26/22 (C-26/22)** fastslår, at en afgørelse fra tilsynsmyndigheden efter [artikel 78](#) er undergivet **fuld** prøvelse ved de nationale domstole. Et afslag fra Datatilsynet er derfor ikke vejs ende. Og efter **C-46/23 (C-46/23)** kan tilsynet påbyde sletning ex officio.

Endelig giver **C-655/23 (C-655/23)** af 4. september 2025 den registrerede et yderligere redskab: adgang til **forebyggende undladelerspåbud** ved siden af erstatningskravet efter [artikel 82](#) – relevant hvor risikoen er, at bureauet genindberetter.

LOV	Databeskyttelsesforordningen § 77	Databeskyttelsesforordningen § 79
PRAKSIS		
	EU-Domstolen · Erstatning for immateriel skade og forebyggende undladelerspåbud efter databeskyttelsesforordningen (GDPR)	04.09.2025
	EU-Domstolen · Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	26.09.2024
	EU-Domstolen · Tilsynsmyndigheders beføjelse til ex officio at påbyde sletning af ulovligt behandlede personoplysninger under GDPR	14.03.2024
	EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
	Det finansielle ankenævn · Afvisning af klage over gældsbrev og RKI-registrering grundet tidligere behandling i fogedretten	21.03.2022

§ 9 Erstatning for uberettiget registrering – ansvarsgrundlaget er det lette, tabet det svære

Praksis viser et konsekvent mønster: **ansvarsgrundlaget er ofte let at etablere, men den registrerede taber på kausalitet og tabsopgørelse.**

Det klareste eksempel er **292/2014 (292/2014)**. Efter at Datatilsynet den 6. september 2013 havde fastslået, at Danske Banks registrering var i strid med **persondatalovens § 25** – forgængeren til de nuværende regler – nedlagde klageren påstand om 744.090 kr. i erstatning. Hun gjorde gældende, at hun i de 25,5 måneder, registreringen bestod, fik afslag på to lederstillinger hos virksomheder, der ikke ansatte RKI-registrerede, og at hun mistede adgang til lån, kreditkort, forsikringer og telefonabonnementer. Banken erkendte fejlen og udsendte et dementi, men bestred ansvaret.

Ankenævnet delte sagen i to og gav klageren medhold i det ene led:

*Ankenævnet fastslog indledningsvis, at Danske Bank havde handlet **ansvarspådragende** ved at foretage den uberettigede registrering i RKI i strid med reglerne.*

Men hun tabte alligevel. Nævnet fandt ikke, at hun havde løftet bevisbyrden for et økonomisk tab som direkte følge af registreringen – forklaringen om jobafslag var ikke tilstrækkelig dokumentation for et tab på over 700.000 kr. Og nævnet fandt »ikke grundlag for at pålægge banken at betale godtgørelse for tort, ulempe eller ikke-økonomisk skade«.

I **129/2008 (129/2008)** faldt sagen allerede på ansvarsgrundlaget. Klageren var i væsentlig misligholdelse af et privatlån på ca. 114.000 kr. og et overtræk på ca. 37.000 kr.; banken fik udlæg i fogedretten den 6. marts 2008 og indberettede den 10. marts 2008. Nævnet fandt registreringen lovlig, fordi der forelå både retsligt udlæg og konstateret misligholdelse. Afgørende for udfaldet var, at selv om klageren led et tab ved ikke at kunne omprioritere sin ejendom, »kan dette tab ikke væltes over på banken, da banken blot har varetaget sine legitime

interesser som kreditor«. Sagen illustrerer også et forligsmønster: banken havde tilbudt at slette registreringen efter 12 måneders stabil afvikling.

EU-rettens dimension ændrer billedet – men mindre end man kunne håbe. **C-300/21 (C-300/21)** opstiller tre **kumulative** betingelser for erstatning efter [artikel 82, stk. 1](#): en overtrædelse, en faktisk lidt materiel eller immateriel skade, og en årsagsforbindelse:

»Det kan derfor ikke lægges til grund, at enhver »overtrædelse« af databeskyttelsesforordningens bestemmelser i sig selv giver den registrerede [...] ret til erstatning. En sådan fortolkning ville være i strid med ordlyden af forordningens artikel 82, stk. 1.« (præmis 33)

Men Domstolen afviste samtidig enhver national **alvorstærskel** for immateriel skade (præmis 43-51) – og gentog det i **C-456/22 (C-456/22)** og **C-590/22 (C-590/22)**. Der er altså ingen bagatelgrænse. Bevisbyrden består dog: »den registrerede [skal] fortsat [...] godtgøre, at de negative virkninger reelt udgør en immateriel skade« (C-300/21, præmis 50). Erstatningen skal yde **fuld** kompensation, men må ikke have karakter af straf (præmis 57-58).

Dette er den centrale spænding for danske RKI-sager. Det Finansielle Ankenævn afviste i 292/2014 tort med henvisning til manglende kompetence og manglende grundlag. Efter C-300/21, C-456/22 og C-590/22 kan et krav på **immateriel skade** efter artikel 82 ikke afvises under henvisning til, at skaden er for ubetydelig – men den registrerede skal stadig konkretisere den. Yderligere holdepunkter: **C-741/21 (C-741/21)** om den dataansvarliges fritagelsesmulighed, **C-182/22 (C-182/22)** om identitetstyveribegrebet, og **C-507/23 (C-507/23)**, hvorefter en **undskyldning** efter omstændighederne kan udgøre tilstrækkelig godtgørelse – hvilket sætter det dementi, Danske Bank udsendte i 292/2014, i et nyt lys.

Praktisk konsekvens: den registrerede bør dokumentere tabet **samtidigt** – skriftlige afslag med begrundelse i registreringen, korrespondance med kreditgivere, dokumentation for merfinansieringsomkostninger – frem for at rekonstruere det bagefter.

LOV	Databeskyttelsesforordningen § 82, stk. 1	
PRAKSIS	EU-Domstolen · Erstatning for immateriel skade efter GDPR: Undskyldning som godtgørelse og betydningen af den dataansvarliges skyld	04.10.2024
	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024
	EU-Domstolen · Retten til erstatning for immateriel skade ved databrud og fortolkningen af identitetstyveri under GDPR	20.06.2024
	EU-Domstolen · Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR	11.04.2024
	EU-Domstolen · Ret til erstatning for immateriel skade under GDPR: Ingen bagatelgrænse for skadens alvor	14.12.2023
	EU-Domstolen · Krav om faktisk skade og afvisning af alvorstærskler ved erstatning for immateriel skade under GDPR	04.05.2023
	Det finansielle ankenævn · Krav om erstatning for uberettiget RKI-registrering foretaget 23 år efter gældens opståen	20.08.2015
	Det finansielle ankenævn · Erstatningskrav mod bank for RKI-registrering efter misligholdelse af privatlån og kontoovertræk	25.09.2008

§ 10 Følgevirkningerne af en registrering – bank, kredit og forsikring

Registreringens indgribende karakter viser sig i de afledte sager, og de udgør samtidig kilden til det tab, der skal dokumenteres i en erstatningssag.

På bankområdet er hovedreglen kontraheringsfrihed. I **237/2019 (237/2019)** havde en kunde med ca. 37.000 kr. i gæld bedt Arbejdernes Landsbank om et samlelån og gjort gældende, at afslaget var forskelsbehandling. Nævnet gav ikke medhold:

Det beror på et pengeinstituts egen forretningsmæssige afgørelse, om det ønsker at imødekomme en låneansøgning. Ankenævnet kan derfor ikke pålægge en bank at yde et lån eller en kredit.

Banken kunne lovligt følge en kreditpolitik om ikke at yde lån til RKI-registrerede inden for rammerne af [lov om finansiel virksomhed § 43](#). Sagen rummer en pointe, der ofte overraskes over: banken anførte, at »[e]n sletning fra RKI (enten ved indfrielse eller forældelse) medfører ikke automatisk en lånebevilling, da enhver ansøgning beror på en individuel, sædvanlig kreditvurdering«. Sletning genopretter altså ikke kreditværdigheden af sig selv.

Samme linje i **152/2003 (152/2003)**, hvor Vordingborg Bank lovligt kunne nægte en RKI-registreret kunde netbankadgang, fordi adgangen indebar en risiko for »selvbestaltede overtræk« via Betalingsservice – og i **193/2020 (193/2020)** om afslag på henstand med realkredittermin og dankort. Grænsen sættes af **lov om betalingskonti § 11** om **basal betalingskonto**: banken kan afvise kredit, men ikke uden videre selve kontoen.

På forsikringsområdet er konsekvensen skarpere, fordi RKI-status indgår i risikooplysningerne ved tegning. I **99721 (99721)** havde klageren ved indtegnelse med NemID svaret »nej« til spørgsmålet om RKI-registrering. Efter et færdselsuheld ophævede Aros Forsikring kaskoforsikringen med tilbagevirkende kraft. Ankenævnet gav ikke medhold: klageren havde objektivt afgivet urigtige oplysninger, dette måtte tilregnes hende som uagtsomt, og selskabet havde bevist, at det efter sine acceptregler ikke ville have tegnet forsikringen, jf. [forsikringsaftaleloven § 6, stk. 1](#). Nævnet lagde afgørende vægt på, at klageren »har accepteret forsikringsbegæringen ved sin elektroniske underskrift« – uanset om feltet var forudfyldt af selskabet.

Samme resultat i **100185 (100185)**, hvor klageren ved digital tegning bekræftede ikke at være registreret, men reelt var indberettet af to kreditorer med 51.696 kr. og 1.109 kr. Efter en totalskade afviste Tryg dækning og opsagde kaskoaftalen med tilbagevirkende kraft. Klageren anførte, at hun var i god tro og uvidende om registreringen – et anbringende der understreger, hvor afgørende [§ 17](#)-underretningen og bekendtgørelsens [§ 1](#) er: en registrering, den registrerede aldrig fik at vide om, kan koste forsikringsdækningen. **103672 (103672)** tilføjer, at indsigelsen mod opsigelsen selv kan forældes efter [forældelsesloven § 3](#).

På kreditvurderingsområdet er registreringen næsten diskvalificerende. [Vejledning om kreditværdighedsvurdering](#) formulerer det direkte:

»Hvis forbrugeren er registreret som dårlig betaler, har restancer på gæld til det offentlige eller har fået gjort udlæg i sin bolig, vil forbrugeren som udgangspunkt ikke være kreditværdig, men efter omstændighederne vil pligten til at foretage en kreditværdighedsvurdering ikke være til hinder for at yde forbrugeren kredit, hvis bevillingen afyderligere kredit har til formål og er egnet til at forbedre forbrugeren økonomiske situation.«

Kreditgiveren skal desuden efter [vejledning til bekendtgørelse om god skik for boligkredit](#) oplyse, hvilke registre der er slået op i ved et afslag – en pligt der udspringer af forbrugerkreditdirektivets artikel 9, stk. 2, jf. [betænkning nr. 1509/2009, s. 74](#). Den oplysning er ofte den registreredes første – og bedste – dokumentation for både registreringens eksistens og dens konkrete virkning.

Endelig noteres, at kreditoplysningsbureauer med Datatilsynets tilladelse har ret til at få leveret **beskyttede navne og adresser** efter [CPR-lovens § 42, stk. 4](#), jf. [Vejledning om folkeregistrering](#) – en privilegering der understreger, at tilladelsen efter § 19 ikke blot er en formalitet, men giver adgang til data, andre private er afskåret fra.

LOV

[Databeskyttelsesloven § 17](#)
[Forsikringsaftaleloven § 6, stk. 1](#)
[Lov om finansiell virksomhed § 43, stk. 1](#)

PRAKSIS	Ankenævnet for Forsikring · Forældelse af indsigelse mod opsigelse af indboforsikring og krav om dækning grundet urigtige oplysninger om RKI-registrering	24.09.2025
	Ankenævnet for Forsikring · Afvisning af dækning efter urigtige oplysninger om RKI-registrering ved tegning af bilforsikring	29.11.2023
	Ankenævnet for Forsikring · Afgørelse om ophævelse af kaskoforsikring grundet urigtige oplysninger om RKI-registrering	13.09.2023
	Det finansielle ankenævn · Afslag på henstand med realkredittermin og udstedelse af dankort grundet RKI-registrering	11.06.2021
	Det finansielle ankenævn · Afslag på låneanmodning og indsigelse om forskelsbehandling i forbindelse med RKI-registrering	19.11.2019
	Det finansielle ankenævn · Pengeinstituts afslag på netbankaftale til RKI-registreret kunde fundet berettiget	14.10.2003

§ 11 Straf, retlighedsfrakendelse og anklagemyndighedens behandling

Kapitel 5 er strafsanktioneret. Efter [databeskyttelseslovens § 41, stk. 2, nr. 1](#) straffes med **bøde eller fængsel indtil 6 måneder** den, der overtræder bl.a. [§ 20](#), [§ 21](#) eller [§ 26, stk. 1 og 5](#). Særsomt strafbelagt er efter [§ 41, stk. 2, nr. 8](#) den, der »i øvrigt undlader at efterkomme Datatilsynets afgørelser efter loven eller **tilsidesætter Datatilsynets vilkår for en tilladelse** i medfør af loven« – det er dén bestemmelse, der gør de vilkårsfastsatte slettefrister til mere end en henstilling. Efter [§ 41, stk. 3](#) skal [forordningens artikel 83, stk. 2](#) følges ved strafudmålingen, og [§ 41, stk. 7](#) fastsætter en **forældelsesfrist på 5 år**. Juridiske personer kan straffes efter [§ 41, stk. 6](#).

Den skarpeste sanktion er [§ 43](#):

»Den, der driver eller er beskæftiget med virksomhed som nævnt i [§ 26](#) eller som privat databehandler opbevarer personoplysninger, kan ved dom for strafbart forhold frakendes retten hertil, såfremt det udviste forhold begrundes en nærliggende fare for misbrug.«

[Rigsadvokatmeddelelsen, afsnittet om Databeskyttelse – Straffesager](#) pålægger anklagemyndigheden en aktiv pligt:

»I sager vedrørende den type virksomhed, der er omfattet af databeskyttelseslovens [§ 26](#), det vil sige advarselsregistervirksomhed, kreditoplysningsbureauvirksomhed og virksomhed ved behandling af oplysninger, der udelukkende finder sted med henblik på at føre retsinformationssystemer, skal anklagemyndigheden overveje, om der skal nedlægges påstand om retlighedsfrakendelse, jf. databeskyttelseslovens [§ 43](#).«

Meddelelsen fastsætter desuden en række processuelle rammer, der har praktisk betydning for den, der anmelder et bureau. Efter [pkt. 3.3](#) skal politikredsen forelægge tiltalepørgsmålet – herunder strafpåstanden – for statsadvokaten i **alle** sager om overtrædelse af databeskyttelsesreglerne, og sagerne »må ikke afgøres

med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis«. Datatilsynet skal høres inden tiltalepørgsmålet afgøres, jf. [pkt. 3.7](#), og tilsynet sender kopi af alle sine politianmeldelser til Rigspolitiets og Rigsadvokatens databeskyttelsesenheder, jf. [pkt. 3.2.1](#).

Både den dataansvarlige og databehandleren kan ifalde strafansvar, jf. [pkt. 4.1.1.4](#). Efter **C-807/21 (C-807/21)** kan en juridisk person pålægges bøde direkte, men det forudsætter, at overtrædelsen er begået **forsætligt eller uagtsomt** – der er ikke tale om et objektivt ansvar.

I praksis er strafsporet dog sjældent den registreredes vej frem. Efter **C-768/21 (C-768/21)** har klageren ingen subjektiv ret til at kræve en bøde, og Datatilsynet kan lovligt nøjes med kritik eller påbud, når overtrædelsen er bragt til ophør. Strafsporets reelle funktion er præventiv – og bagvedliggende for de vilkår, bureauerne retter sig efter.

LOV

Databeskyttelsesloven § 26, stk. 1

Databeskyttelsesloven § 41, stk. 2, 3, 6, 7

Databeskyttelsesloven § 43

PRAKSIS	EU-Domstolen · Tilsynsmyndigheders skønsebeføjelse ved brud på persondatasikkerheden under GDPR	26.09.2024
	EU-Domstolen · Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	05.12.2023

§ 12 Angrebsmulighederne i praksis – en tjekliste for sletningssagen

Sammenholdes lovtekst, forarbejder og praksis, tegner der sig et sæt konkrete angrebspunkter mod en registrering. De er ordnet efter gennemslagskraft:

- 1. Fordringen er bestridt og ikke prøvet retsligt.** Det stærkeste kort. Forarbejderne til [§ 20, stk. 1](#) er kategoriske: bureauet »må ikke registrere oplysninger om fordringer, der er bestridt af skyldneren, såfremt fordringen ikke har været forelagt en retslig instans«. Registerudvalget skærpede i [betænkning nr. 1345/1997, s. 104](#) til, at fordringen skal være fastslået ved endelig domstolsafgørelse. Bemærk: indsigelsen skal være **reel** og fremsat – ikke konstrueret efter registreringen.
- 2. Manglende fundament.** Efter [§ 21, stk. 3](#) kræves skriftlig erkendelse af forfalden gæld eller foretagne retslige skridt, og kravet skal overstige 1.000 kr. til **samme** kreditor. Uden fundament må indberetningen efter [betænkning nr. 1578/2022, s. 119](#) kun stå i et lukket register, tilgængeligt for indberetteren selv. Kontrollér om beløbet er splittet på flere kreditorer for at nå over tærsklen.
- 3. Femårsfristen er overskredet – eller fordringen er genregistreret.** [§ 20, stk. 3](#) regnes fra det forhold, der taler imod kreditværdighed. **292/2014 (292/2014)** fastslår, at samme fordring ikke må registreres igen efter at have været slettet. Husk desuden, at fristen er en **maksimumsfrist**, og at Datatilsynets vejledende frister er kortere.
- 4. Manglende underretning.** For offentlig gæld: er den skriftlige meddelelse efter [§ 17, stk. 1](#) givet, og er 4-ugersfristen overholdt? Indeholder den alle fire punkter i [§ 17, stk. 2](#)? For pengeinstitutter: er meddelelsen efter [bekendtgørelsens § 1](#) givet inden 4 uger? **100185 (100185)** viser, hvad det koster, når den registrerede ikke ved, at hun står i registret.

5. Betaling eller overholdt afdragsaftale før registreringen. Efter § 17, stk. 2, nr. 4 må videregivelse ikke ske, hvis gælden betales, eller der indgås og overholdes en afdragsordning inden videregivelsen. Og efter § 16, stk. 1, nr. 2 må poster omfattet af en **overholdt** henstands- eller afdragsaftale ikke indgå i de 7.500 kr.

6. Beløbs- og administrationsgrænser for offentlig gæld. Samlet forfalden gæld skal overstige 7.500 kr. og administreres af **samme** inddrivelsesmyndighed, jf. § 16, stk. 2, og ét af de fire alternativer i § 16, stk. 3 skal være opfyldt.

7. Forældet fordring. En forældet fordring er ikke retskraftig og kan derfor vanskeligt være »af betydning for bedømmelse af økonomisk soliditet og kreditværdighed« i § 20, stk. 1's forstand. Bemærk dog samspillet med fundamentets art: et betalingspåkrav med fogedrettens påtegning efter [retsplejelovens § 477 e](#) har lang forældelse, hvilket var relevant i **66/2018** (66/2018). Selve forældelsesspørgsmålet behandles i praksisoversigten om [forældelse af pengekrav](#).

8. Gældssanering. Endeligt godkendt gældssanering må **aldrig** videregives, jf. § 21, stk. 3, 2. pkt. Og efter C-26/22 (C-26/22) kan bureauet ikke lagre restgældsbe frielsesoplysninger længere end det offentlige register.

9. Dobbeltregistrering og smitte. Forarbejderne til § 20, stk. 1: »Når et bureau registrerer oplysninger til brug for bedømmelse af en persons eller virksomheds økonomiske soliditet og kreditværdighed, må oplysningerne kun vedrøre netop denne person eller virksomhed.«

10. Fejl i beløb eller stamdata. Her er berigtigelsespligten i [forordningens artikel 16](#) og underretningen af modtagere efter [artikel 19](#) det centrale – for pengeinstitutter skærpet i [bekendtgørelsens § 4](#), hvorefter instituttet **straks** skal berigtige og skriftligt underrette alle, der har modtaget oplysningen inden for de sidste 6 måneder.

11. Scoringen selv. Efter C-634/21 (C-634/21) er scoreberegningen en artikel 22-afgørelse, og efter C-203/22 (C-203/22) har den registrerede krav på en reel forklaring af logikken. Sammenholdt med brugsforbuddet i § 20, stk. 3-forarbejderne åbner det for at angribe en score, der bygger på forældede oplysninger.

Bemærk afgrænsningen: sletning af søgeresultater hos søgemaskiner behandles i praksisoversigten om [ret til at blive glemt](#) og hviler på et andet retsgrundlag ([forordningens artikel 17](#)) end den nationale særregulering i kapitel 5.

LOV

[Databeskyttelsesloven § 16, stk. 1-3](#)
[Databeskyttelsesloven § 17, stk. 1, 2](#)
[Databeskyttelsesloven § 20, stk. 1, 3](#)
[Databeskyttelsesloven § 21, stk. 3](#)

PRAKSIS	EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmigheder	27.02.2025
	EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
	EU-Domstolen · Automatisk kreditscoring som en individuel afgørelse efter GDPR	07.12.2023
	Det finansielle ankenævn · Danske Bank frifundet for RKI-indberetning foretaget ti år efter misligholdelse	21.08.2018
	Det finansielle ankenævn · Krav om erstatning for uberettiget RKI-registrering foretaget 23 år efter gældens opståen	20.08.2015
	Ankenævnet for Forsikring · Afvisning af dækning efter urigtige oplysninger om RKI-registrering ved tegning af bilforsikring	29.11.2023

§ 13 Sammenfatning – hvor står retsstillingen efter SCHUFA-dommene?

Kapitel 5 i databeskyttelsesloven er et af de få steder, hvor dansk ret opretholder en **strengere** national ramme end forordningen selv. Den ramme har rødder helt tilbage til [betænkning nr. 687/1973](#) og videreførtes stort set uændret gennem [betænkning nr. 1345/1997](#) til den gældende lov. Kontinuiteten er lovgivers udtrykkelige valg: forarbejderne til [§§ 19-21](#) gentager for hver bestemmelse, at »[d]en gældende praksis på området vil dermed fortsat være af betydning«. Ældre Registertilsyns- og Datatilsynspraksis er derfor stadig relevant retskilde.

Registerudvalget begrundede i [betænkning nr. 1345/1997, s. 272](#) hvorfor særreguleringen blev bevaret, selvom direktivet ikke krævede den:

»Det er af meget væsentlig betydning for såvel enkeltpersoner som virksomheder, at behandling af oplysninger i kreditoplysningsøjemed sker på en saglig og lovlig måde. Ulovlige handlinger på dette område vil kunne medføre meget alvorlige skadevirkninger for de involverede parter.«

Tre forhold præger retsstillingen i dag.

For det første er tyngdepunktet forskudt mod EU-retten. Frem til 2023 var kapitel 5 i praksis et rent nationalt anliggende. Med [C-26/22](#), [C-634/21](#) og [C-203/22](#) er kreditoplysningsvirksomhed blevet et EU-retligt reguleret felt, hvor lagringsfristen skal bestå en interesseafvejning efter [artikel 6](#), scoringen er en artikel 22-afgørelse, og indsigtsretten ikke kan afvises med et blankt forretningshemmelighedsargument. Femårsreglen i [§ 20, stk. 3](#) sætter fortsat et loft, men den kan ikke længere alene begrunde en registrering nedad – interesseafvejningen skal bestå selvstændigt.

For det andet er der en vedvarende asymmetri mellem ansvarsgrundlag og retsvirkning. [292/2014 \(292/2014-\)](#) er sigende: indberetteren handlede ansvarspådragende, Datatilsynet underkendte registreringen, banken erkendte fejlen – og klageren fik alligevel intet. Bevisbyrden for kausalitet og tab er den reelle barriere. [C-300/21 \(C-300/21\)](#) fjerner alvorstærsklen, men fastholder kravet om faktisk skade og årsagsforbindelse. Den registrerede, der vil have mere end en sletning, skal dokumentere tabet samtidigt.

For det tredje er kompetencefordelingen en selvstændig faldgrube. [137/2021 \(137/2021\)](#) viser, at sletningskravet hverken hører hjemme i Det Finansielle Ankenævn eller under fogedrettens udlægssag. Datatilsynet er den rette adressat – men efter [C-768/21 \(C-768/21\)](#) er tilsynet ikke forpligtet til at sanktionere, og klageren har ingen ret til at kræve en bøde. Til gengæld er tilsynets afgørelse efter [C-26/22](#) undergivet fuld domstolsprøvelse, og efter [C-655/23 \(C-655/23\)](#) kan der nedlægges forebyggende undladelsespåbud.

Den praktiske konklusion: sletningssagen vindes sjældent på generelle betragtninger om proportionalitet, men på præcise formelle brist – bestridt fordring uden retsligt fundament, manglende underretning, overskredet frist, beløb under tærsklen, eller genregistrering af en allerede slettet fordring. Det er formkravene i [§§ 16, 17, 20 og 21](#), der bærer, og de er i vidt omfang objektive og efterprøvelige. Hvor de er overtrådt, er sletningen svær at komme uden om – hvad enten bureauet vil eller ej.

LOV	Databeskyttelsesforordningen § 82, stk. 1	Databeskyttelsesloven § 19
	Databeskyttelsesloven § 20, stk. 3	Databeskyttelsesloven § 21
PRAKSIS	EU-Domstolen · Erstatning for immateriel skade og forebyggende undladelsespåbud efter databeskyttelsesforordningen (GDPR)	
	04.09.2025	
	EU-Domstolen · Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR	
	26.09.2024	

EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
EU-Domstolen · Krav om faktisk skade og afvisning af alvorstærskler ved erstatning for immateriel skade under GDPR	04.05.2023
Det finansielle ankenævn · Afvisning af klage over gældsbrev og RKI-registrering grundet tidligere behandling i fogedretten	21.03.2022
Det finansielle ankenævn · Krav om erstatning for uberettiget RKI-registrering foretaget 23 år efter gældens opståen	20.08.2015

REFERENCE Lovgrundlag 8 paragraffer

Databeskyttelsesforordningen § 17		Databeskyttelsesloven § 16	stk. 3
Databeskyttelsesloven § 17	stk. 1	Databeskyttelsesloven § 19	
Databeskyttelsesloven § 20	stk. 3	Databeskyttelsesloven § 21	stk. 1
Databeskyttelsesloven § 22	stk. 1	Databeskyttelsesloven § 26	stk. 1

MATERIALE Citerede afgørelser 25 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL			13
04.09.2025	Erstatning for immateriel skade og forebyggende undladelerspåbud efter databeskyttelsesforordningen (GDPR)		C-655/23
27.02.2025	Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder		C-203/22
04.10.2024	Erstatning for immateriel skade efter GDPR: Undskyldning som godtgørelse og betydningen af den dataansvarliges skyld		C-507/23
26.09.2024	Tilsynsmyndigheders skønsbeføjelse ved brud på persondatasikkerheden under GDPR		C-768/21
20.06.2024	Retten til erstatning for immateriel skade ved databrud og fortolkningen af identitetstyveri under GDPR		C-182/22
20.06.2024	Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse		C-590/22
11.04.2024	Fortolkning af immateriel skade og dataansvarliges fritagelse for ansvar ved overtrædelse af GDPR		C-741/21
14.03.2024	Tilsynsmyndigheders beføjelse til ex officio at påbyde sletning af ulovligt behandlede personoplysninger under GDPR		C-46/23
14.12.2023	Ret til erstatning for immateriel skade under GDPR: Ingen bagatelgrænse for skadens alvor		C-456/22
07.12.2023	Automatisk kredit scoring som en individuel afgørelse efter GDPR		C-634/21

07.12.2023	Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	C-26/22
05.12.2023	Direkte bødeansvar for juridiske personer og krav om skyld efter databeskyttelsesforordningen	C-807/21
04.05.2023	Krav om faktisk skade og afvisning af alvorstærskler ved erstatning for immateriel skade under GDPR	C-300/21

SØ- OG HANDELSRET TEN · SPECIALRET 1

25.06.2002	Varemærkekrænkel se: Forvekslelighed mellem RKI og PKI i kreditoplysningsvirksomhed	V-0060-01
------------	---	-----------

DET FINANSIELLE ANKENÆVN · NÆVN / KLAGEINSTANS 8

21.03.2022	Afvisning af klage over gælds brev og RKI-registrering grundet tidligere behandling i fogedretten	137/2021
11.06.2021	Afslag på henstand med realkredit termin og udstedelse af dankort grundet RKI-registrering	193/2020
19.11.2019	Afslag på låneanmodning og indsigelse om forskelsbehandling i forbindelse med RKI-registrering	237/2019
21.08.2018	Danske Bank frifundet for RKI-indberetning foretaget ti år efter misligholdelse	66/2018
04.03.2016	Spørgsmål om berettigelse af inkassooverdragelse og videregivelse af oplysninger til kreditvurdering	69/2015
20.08.2015	Krav om erstatning for uberettiget RKI-registrering foretaget 23 år efter gældens opståen	292/2014
25.09.2008	Erstatningskrav mod bank for RKI-registrering efter misligholdelse af privatlån og kontoovertræk	129/2008
14.10.2003	Pengeinstituts afslag på netbankaftale til RKI-registreret kunde fundet berettiget	152/2003

ANKENÆVNET FOR FORSIKRING · NÆVN / KLAGEINSTANS 3

24.09.2025	Forældelse af indsigelse mod opsigelse af indboforsikring og krav om dækning grundet urigtige oplysninger om RKI-registrering	103672
29.11.2023	Afvisning af dækning efter urigtige oplysninger om RKI-registrering ved tegning af bilforsikring	100185
13.09.2023	Afgørelse om ophævelse af kaskoforsikring grundet urigtige oplysninger om RKI-registrering	99721

FORARBEJDE Betænkninger

6 referencer

Behandling af personoplysninger - Betænkning afgivet af udvalget om registerlovgivningen
nr. 1345 · 1997 · Justitsministeriet

Bilag til betænkning nr. 1345 om behandling af personoplysninger

nr. 1345 · 1997 · Justitsministeriet

Betænkning nr. 1509 om gennemførelse af forbrugerkreditdirektivet

nr. 1509 · 2009 · Justitsministeriet

Betænkning om modernisering og revision af reglerne om gældssanering, herunder implementering af rekonstruktions- og insolvensdirektivet

nr. 1578 · 2022 · Justitsministeriet

Betænkning om revision af konkurskarantænereglerne

nr. 1582 · 2023 · Justitsministeriet

Delbetænkning om private registre (Betænkning nr. 687)

nr. 687 · 1973 · Justitsministeriet

18

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over SMS-phishing / smishing-bedrageri

Strafudmåling, sondringen mellem § 279 og § 279 a samt civilretlig hæftelse efter betalingsloven

Version 2 · Opdateret 24. jun. 2026 · 22 afgørelser · 2015-2026

[Læs online](#)

INTRODUKTION

SMS-phishing (smishing) er en af de mest udbredte former for IT-relateret økonomisk kriminalitet i Danmark. Gerningsmanden udsender SMS-beskeder, der efterligner afsendere som PostNord, MobilePay, Skat eller offerets egen bank, med et link til en falsk hjemmeside, hvor offeret narres til at indtaste kortoplysninger og MitID-legitimation. Retligt rejser smishing-bedrageri to hovedspørgsmål: (1) den strafferetlige kvalificering efter straffelovens § 279 (bedrageri) eller § 279 a (databedrageri), herunder strafudmåling og udvisning, og (2) den civilretlige fordeling af tab mellem kunde og bank efter betalingslovens § 100. Praksis viser, at organiserede smishing-operationer med mange ofre og store beløb medfører straffe i intervallet 1½–6 års fængsel, mens Finansielle Ankenævn systematisk anvender en selvrisiko på 8.000 kr. for ofre, der har godkendt transaktioner via MitID efter phishing-SMS.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** SMS-phishing kvalificeres som databedrageri efter straffelovens § 279 a, når offeret narres til at godkende en elektronisk transaktion via MitID, idet den tabsforvoldende disposition sker via elektronisk databehandling.
- 02** Klassisk bedrageri efter § 279 kan dog anvendes, hvor gerningsmanden telefonisk manipulerer offeret til at udlevere betalingskort, kontanter eller smykker – typisk ved vishing-opkald der følger efter SMS-kontakt.
- 03** Ved organiseret smishing med mere end 600 ofre og beløb over 27 mio. kr. udmåles straffen op til 5–6 års fængsel efter § 286, stk. 2 (særlig grov beskaffenhed).
- 04** En chauffør eller medhjælper i en organiseret bedragerigruppe straffes typisk med 1½–2 års fængsel, selv ved begrænset egen andel i bedrageriet.
- 05** Pengemuldyr (money mules), der stiller konti til rådighed for at modtage og videresende udbyttet, straffes selvstændigt for hvidvask efter § 290 a.

- 06** Sager om IT-relateret økonomisk kriminalitet, herunder smishing, behandles af NCIK (Nationalt Center for It-relateret økonomisk Kriminalitet) under NSK.
- 07** Manipulation af SMS-afsendernavne (A-nummer-spoofing) kan afdækkes via teledata, jf. Rigsadvokatmeddelelsen om teledata, afsnit 2.5.5.
- 08** Efter betalingslovens § 100, stk. 4, hæfter kunden med op til 8.000 kr. ved groft uforsvarlig adfærd – typisk godkendelse af MitID-transaktion efter phishing-SMS.
- 09** Kunden hæfter kun med 375 kr. efter § 100, stk. 3, hvis den uautoriserede transaktion skyldes andres uberettigede anvendelse af betalingsinstrumentet, og kunden ikke har handlet groft uforsvarligt.
- 10** Finansielle Ankenævn afviser hyppigt smishing-sager til domstolene, når bevisførelsen om kundens adfærd kræver mundtlige parts- og vidneforklaringer.
- 11** Udvisning af udenlandske gerningsmænd er hovedreglen ved organiseret smishing-bedrageri, medmindre EMRK art. 8 (privat- og familieliv) fører til et andet resultat.
- 12** Identitetsmisbrug i forbindelse med smishing kan tillige straffes efter straffelovens § 264 e, typisk i sammenstød med § 279 a.

Lovgrundlag: Bedrageri, databedrageri og betalingslovens hæftelsesregler

§ 1

SMS-phishing (smishing) rammes strafferetligt af to centrale bestemmelser i straffeloven:

Straffelovens § 279 (bedrageri) kræver, at gerningsmanden ved retsstridigt at fremkalde, bestyrke eller udnytte en *vildfarelse* bestemmer en anden til en handling eller undladelse, hvorved der påføres et formuetab. Bestemmelsen finder typisk anvendelse, når offeret telefonisk manipuleres ("vishing") til fysisk at udlevere betalingskort, kontanter eller smykker, eller til manuelt at foretage en bankoverførsel.

Straffelovens § 279 a (databedrageri) rammer den, der retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling, eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling. Bestemmelsen er central ved smishing, fordi den tabsforvoldende disposition – selve betalingstransaktionen – sker automatiseret via betalingssystemet, efter at gerningsmanden har fået adgang til offerets kortoplysninger og MitID-legitimation.

Sondringen i praksis afhænger af, hvem eller hvad der foretager den tabsforvoldende disposition. Når offeret narres til at godkende en betaling i MitID-appen uden at forstå, hvad der godkendes, er det betalingssystemet, der disponerer – og forholdet henføres under § 279 a. Når offeret derimod selv overfører penge eller udleverer fysiske genstande, er det offeret, der *bestemmes* til en handling – og forholdet er klassisk bedrageri efter § 279.

Ved grovere forhold anvendes **straffelovens § 286, stk. 2**, der hæver strafmaksimum til 8 års fængsel for bedrageri og databedrageri af *særlig grov beskaffenhed*. Ifølge **Rigsadvokatmeddelelsen om formueforbrydelser** vil forbrydelsen navnlig være af særlig grov beskaffenhed på grund af udførelsesmåden, fordi forbrydelsen er

udført af flere i forening, som følge af omfanget af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

På den civilretlige side regulerer [betalingslovens § 100](#) fordelingen af tab ved uautoriserede betalingstransaktioner mellem kunde og betalingstjenesteudbyder (bank). Bestemmelsen opererer med en trinmodel:

- **Stk. 3** (375 kr.): Kunden hæfter med op til 375 kr. for tab som følge af andres uberettigede anvendelse af betalingsinstrumentet, medmindre kunden har handlet groft uforsvarligt.
- **Stk. 4** (8.000 kr.): Kunden hæfter med op til 8.000 kr., hvis den uautoriserede transaktion skyldes, at kunden ved groft uforsvarlig adfærd har muliggjort misbruget.
- **Stk. 5** (ubegrænset): Kunden hæfter uden beløbsbegrænsning, hvis kunden har handlet svigagtigt eller forsætligt undladt at opfylde sine forpligtelser.

LOV

[Betalingsloven § 100, stk. 3-5](#)[Straffeloven § 279](#)[Straffeloven § 279a](#)[Straffeloven § 286, stk. 2](#)

§ 2 NCIK og efterforskning af smishing-sager

Siden 1. januar 2022 er sager om IT-relateret økonomisk kriminalitet, herunder smishing, centraliseret hos **Nationalt Center for It-relateret økonomisk Kriminalitet (NCIK)**, der er forankret i National enhed for Særlig Kriminalitet (NSK). [Rigsadvokatmeddelelsen om formueforbrydelser](#) oplyser, at NCIK's sagsområde dækker syv kategorier, herunder:

- Kontaktbedrageri mod borgere (kategori 3)
- Misbrug af betalingskort (kategori 5)
- Misbrug af adgang til netbank/betalingstjenester (kategori 6)

Smishing falder typisk under kategori 3 (kontaktbedrageri mod borgere) i kombinationen med kategori 5 og 6. Statsadvokaten for Særlig Kriminalitet (SSK) varetager tilsynsopgaver, og klager over centerets afgørelser kan indgives til SSK.

Et centralt teknisk element i smishing-sager er **A-nummer-spoofing** – manipulation af afsendernavnet i SMS-beskeder, så de fremstår som sendt fra fx "PostNord", "MobilePay" eller offerets bank.

[Rigsadvokatmeddelelsen om teledata](#) beskriver, at denne type manipulation kan afdækkes ved at indhente teledata vedrørende A-nummeret, idet det heraf vil fremgå, at nummeret ikke har været anvendt til den pågældende aktivitet.

§ 3 Strafudmåling ved organiseret smishing-bedrageri

Retspraksis viser, at strafudmålingen ved smishing-bedrageri afhænger af tre hovedfaktorer: (1) det samlede omfang (antal ofre og beløb), (2) gerningsmandenes organisationsgrad og rolle, og (3) individuelle formildende eller skærpende omstændigheder.

Hovedmanden i en stor phishing-operation: I [SS-6507/2023-ALB](#) blev en 21-årig mand idømt **5 års fængsel** for at have organiseret et omfattende svindelsystem over halvandet år. Tiltalte sendte SMS'er med links til falske MitID-sider til mere end 600 personer, og med de stjålne oplysninger foretog gerningsmændene over 2.900 onlinekøb af guld, luksusvarer og gavekort for mindst 27 mio. kr. Retten lagde særlig vægt på:

- Den lange periode (halvandet år)
- Den planlagte og organiserede karakter
- Det meget store antal ofre (over 600)
- Den enorme samlede beløbsstørrelse
- At tiltalte havde udnyttet unge kammerater til at stå for konti og firmaer

Tiltalte blev dømt efter [§ 279](#), [§ 279 a](#) og [§ 263, stk. 1 og 3](#), alle jf. [§ 286, stk. 2](#), samt [§ 21](#) (forsøg). Der skete konfiskation af luksusgenstande (Louis Vuitton, Prada, CELINE mv.) samt 17 sim-kort, og tiltalte blev pålagt erstatning for ca. 4,76 mio. kr.

Chaufføren i en vishing/smishing-gruppe: I [SS-634/2024-SVE](#) blev en 30-årig mand idømt **1 år og 9 måneders fængsel** for sin rolle som chauffør i en organiseret bedragerigruppe, der systematisk ringede ældre borgere op efter SMS-kontakt og fik dem til at udlevere betalingskort, kontanter og smykker. Der var tale om over 200 forhold mod ældre borgere i hele Jylland. Retten udtalte:

Retten har ved udmålingen af fængselsstraffen lagt vægt på kriminalitetens omfang og grovhed, herunder at tiltalte indgik i en veltilrettelagt organisation, der systematisk og målrettet gik efter at franske ældre medborgere deres opsparinger, kontanter, betalingskort, smykker mv.

I formildende retning indgik tiltaltes fulde tilståelse.

[Straffelovrådets betænkning nr. 1581/2023 om strafudmåling – Bind III](#) giver et samlet overblik over strafniveauet for databedrageri og bedrageri. For databedrageri i forbindelse med NemID/MitID-misbrug anføres i den lave ende 1 års fængsel (24 tilfælde af NemID-misbrug, lån for over 400.000 kr.) og i den høje ende 2–2½ års fængsel (systematisk misbrug over længere periode med beløb på 3–5 mio. kr.).

Rolle / omfang	Typisk strafniveau	Eksempel
Hovedmand, 600+ ofre, 27 mio. kr.	5 års fængsel	SS-6507/2023-ALB
Chauffør/medhjælper, 200+ forhold	1 år 9 mdr. fængsel	SS-634/2024-SVE
NemID-misbrug, 24 tilfælde, 400.000 kr.	1 års fængsel	Bet. 1581/2023
Stilling misbrug, systematisk, 3-5 mio. kr.	2–2½ års fængsel	Bet. 1581/2023

LOV

[Straffeloven § 21](#)[Straffeloven § 279](#)[Straffeloven § 279a](#)[Straffeloven § 286, stk. 2](#)

PRAKSIS

Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner

07.06.2024

Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere

15.04.2024

§ 4 Modus operandi: Typiske SMS-scenarier og teknisk forløb

Smishing-angreb følger i dansk praksis et genkendeligt mønster. Gerningsmanden udsender en SMS med et link, der efterligner en pålidelig afsender. De hyppigste scenarier i den fundne praksis er:

- **PostNord-SMS:** "Din pakke afventer betaling af fragt" med link til falsk PostNord-side, hvor offeret indtaster kortoplysninger.
- **MobilePay/bank-SMS:** "Din Online MitID-betaling er blevet deaktiveret" eller "Din konto er spærret" med link til falsk MitID-login.
- **DBA/handelsplatform-SMS:** I forbindelse med salg af varer sendes et link til en falsk DAO-betalingsside, der ser ud som en legitim fragt-/betalingsside.
- **Skat/Politi-SMS:** "Skat har en restance" eller "Politiet har en bøde" med link til falsk betalingsside.

Det tekniske forløb efter offeret klikker på linket er typisk:

1. **Indtastning af kortoplysninger** på den falske side – kortnummer, udløbsdato, CVC.
2. **MitID-godkendelse:** Gerningsmanden bruger de indtastede oplysninger til at initiere en betaling eller korttilknytning, som udløser en MitID-godkendelsesanmodning i offerets MitID-app.
3. **Aktivering af ny MitID-app:** I mere avancerede tilfælde narres offeret til at godkende oprettelsen af en ny MitID-app på en fremmed enhed, hvorved gerningsmanden får fuld kontrol over offerets digitale identitet.
4. **Udnyttelse:** Med adgang til MitID og kortoplysninger foretager gerningsmanden onlinekøb, bankoverførsler eller tilknytning af offerets kort til Apple Pay/Google Pay.

I sagen [507/2022](#) havde klageren dagen forinden selv ændret sit MitID-bruger-id, hvilket gjorde hende mindre mistænksom over for en SMS om, at hendes "Online MitID-betaling" var deaktiveret. Banken oplyste, at transaktionen blev godkendt via klagerens MitID-app, men IP-adressen var lokaliseret til Marokko.

I [357/2023](#) blev en ny MitID-app aktiveret på en fremmed enhed (iPhone 12 mini) efter validering af en SMS-pinkode sendt til klagerens telefon. Kort efter blev to transaktioner på hver 5.200 kr. gennemført til en kryptovalutabørs i Litauen.

Disse sager illustrerer, at smishing-angrebene i stigende grad udnytter MitID-arkitekturen – særligt funktionen til aktivering af nye MitID-apps – som en central vektor. Se også [praksisoversigten om MitID/NemID-misbrug](#) for den videre udnyttelse efter den initiale phishing.

PRAKSIS	Det finansielle ankenævn · Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	18.04.2024
	Det finansielle ankenævn · Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	31.05.2023

Civilretlig hæftelse: Betalingslovens § 100 og Finansielle Ankenævns praksis

Når en forbruger har lidt tab som følge af smishing, er det centrale civilretlige spørgsmål, hvem der bærer tabet – kunden eller banken. [Betalingslovens § 100](#) regulerer dette med en trinmodel, og Finansielle Ankenævn har udviklet en omfattende praksis for smishing-sager.

Hovedmønstret i praksis: Bankerne godtgør som udgangspunkt hele tabet *minus* en selvrisiko på 8.000 kr. under henvisning til § 100, stk. 4 (groft uforsvarlig adfærd). Klagerne gør typisk gældende, at de højst bør

hæfte med 375 kr. (stk. 3). Ankenævnet afviser hyppigt at tage stilling til dette spørgsmål og henviser sagen til domstolene, fordi en afklaring af, om kunden ved groft uforsvarlig adfærd har muliggjort misbruget, kræver mundtlige parts- og vidneforklaringer.

I sagen [131/2023](#) – der direkte omhandlede en PostNord-SMS – havde klageren klikket på et link i en SMS, der angav, at en pakke ventede på betaling. Klageren indtastede kortoplysninger på den falske side, og der blev efterfølgende foretaget uautoriserede transaktioner. Banken anerkendte at godtgøre tabet med fradrag af 8.000 kr.

I [533/2023](#) modtog klageren en SMS, der fremstod som fra MobilePay. Hun trykkede på linket, indtastede kortoplysninger og anvendte sit MitID. Tre uautoriserede transaktioner blev gennemført. Banken fastholdt, at klageren hæftede for 8.000 kr. med den begrundelse, at MitID-appen specifikt viste teksten: *"Betal 10000,00 DKK til [B] fra kort xx1623"*, og at klageren ved at godkende en betaling til en ukendt modtager udviste groft uforsvarlig adfærd. Ankenævnet afviste sagen til domstolene.

Samme mønster ses i [304/2023](#), [409/2023](#), [530/2023](#) og [700/2023](#), hvor bankerne konsekvent anvender 8.000 kr.-selvrisikoen, og nævnet hyppigt afviser til domstolene ved bevistvivl.

Oversigt over hæftelsesniveauer:

Betalingslovens § 100	Hæftelsesbeløb	Typisk situation ved smishing
Stk. 3	Op til 375 kr.	Offeret har <i>ikke</i> handlet groft uforsvarligt – typisk rent automatiserede transaktioner uden MitID-godkendelse
Stk. 4	Op til 8.000 kr.	Offeret har godkendt MitID-transaktion efter at have klikket på phishing-link – bankernes standardposition
Stk. 5	Ubegrænset	Offeret har handlet svigagtigt – sjældent relevant ved smishing

LOV

[Betalingsloven § 100, stk. 3-5](#)

PRAKSIS

Det finansielle ankenævn · Hæftelse for 8.000 kr. efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse af MitID-transaktion	19.08.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS	18.04.2024
Det finansielle ankenævn · Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	18.04.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for phishing-transaktion på 3.726,25 kr. godkendt via MitID	19.03.2024
Det finansielle ankenævn · Indsigelse mod misbrug via Apple Pay efter phishing-SMS afvist grundet behov for bevisførelse	18.01.2024
Det finansielle ankenævn · Indsigelse mod hæftelse for Apple Pay-transaktioner efter indrullering af betalingskort i tredjemands wallet	22.12.2023
Det finansielle ankenævn · Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb	06.09.2023
Det finansielle ankenævn · Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	31.05.2023

§ 6 Landsretspraksis om bankens hæftelse ved phishing

Mens Finansielle Ankenævn ofte afviser smishing-sager til domstolene, har der dannet sig en vis landsretspraksis om fordelingen af tab.

I [BS-2380/2022-VLR](#) behandlede Vestre Landsret spørgsmålet om en banks hæftelse over for en kunde, der var blevet offer for phishing. Sagen illustrerer det centrale bevisspørgsmål: om kunden ved at reagere på en phishing-henvendelse og videregive autentifikationsoplysninger har handlet "groft uforsvarligt" i betalingslovens forstand.

I en anden landsretssag, [BS-28994/2022-OLR](#), tog Østre Landsret stilling til lignende spørgsmål om kundens hæftelse ved uautoriserede transaktioner initieret via phishing.

Praksis viser, at domstolene foretager en konkret vurdering af hændelsesforløbet, herunder:

- Om SMS'en/kommunikationen bar tydelige tegn på svindel, som kunden burde have genkendt
- Om MitID-godkendelsesteksten tydeligt angav modtager og beløb, som afveg fra det forventede
- Om kunden reagerede hurtigt med spærring efter at have fattet mistanke
- Om banken havde opfyldt sine forpligtelser til at levere tilstrækkelig autentifikation og advarsler

Landsretten har i de behandlede sager lagt vægt på, at phishing-angrebene ofte er *professionelt* udført og kan være vanskelige for selv opmærksomme forbrugere at gennemskue. Dette taler mod at skærpe kundens hæftelse til det ubegrænsede niveau i § 100, stk. 5.

LOV

[Betalingsloven § 100, stk. 4](#)

PRAKSIS

Landsretten · Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold) 11.04.2025

Landsretten · Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn 31.01.2023

§ 7 Udvisning af udenlandske gerningsmænd ved organiseret smishing

Organiseret smishing-bedrageri begås i mange tilfælde af udenlandske gerningsmænd, der indrejser i Danmark som led i en koordineret operation. Udvisningsspørgsmålet vurderes efter udlændingelovens § 22–§ 26, herunder proportionalitetsprincippet i EMRK art. 8 (retten til respekt for privat- og familieliv).

I Højesterets dom [U.2022.4567H](#) blev en udenlandsk statsborger udvist for organiseret databedrageri. Højesteret vurderede, at den organiserede karakter og det store omfang af bedrageriet udgjorde tungtvejende grunde for udvisning, som ikke blev opvejet af tiltaltes tilknytning til Danmark.

I byretsdomme vedrørende smishing-sager, herunder [SS-6507/2023-ALB](#), ses det, at gerningsmændene opererer internationalt – tiltalte i den konkrete sag blev anholdt på et hotel i Madrid, hvor spansk politi fandt 17 sim-kort og computere med phishing-skabeloner. Denne grænseoverskridende karakter er et fast træk ved organiseret smishing og har betydning for vurderingen af udvisning og indrejseforbud.

Praksis viser, at udvisning med indrejseforbud i 6 år er udgangspunktet ved organiseret smishing, medmindre gerningsmanden har så stærk tilknytning til Danmark (børn, langvarigt ophold, sygdom), at det ville være uproportionalt efter EMRK art. 8.

LOV

[Straffeloven § 286, stk. 2](#)

PRAKSIS	Byretten · Mand idømt 6 års fængsel for organiseret 'smishing' og databedrageri for over 23 millioner kroner	26.08.2025
	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	07.06.2024

§ 8 Pengemuldyr og hvidvask i forbindelse med smishing

Et fast element i organiserede smishing-operationer er brugen af **pengemuldyr** (money mules) – personer der stiller deres bankkonti til rådighed for at modtage og videreoverføre udbyttet af bedrageriet. Pengemuldyrene rekrutteres ofte via sociale medier med løfter om let fortjeneste og straffes selvstændigt, typisk for hvidvask efter [straffelovens § 290 a](#) eller medvirken til bedrageri.

I den store smishing-sag [SS-6507/2023-ALB](#) havde hovedmanden instrueret flere unge bekendte i at oprette selskaber og bankkonti, som blev brugt til at modtage indbetalinger fra de falske webshops og phishing-operationen. Et af vidnerne forklarede, at han modtog indbetalinger på sin konto uden at vide hvorfra, og overførte dem til tiltalte efter pres.

I [SS-634/2024-SVE](#) fungerede flere navngivne medgerningsmænd som mellemed, der afhentede betalingskort fra ofre og misbrugte dem i hæveautomater og til varekøb.

Forsætsvurderingen for pengemuldyr er ofte et centralt stridspunkt: Anklagemyndigheden skal bevise, at pengemuldyret indså eller fandt det overvejende sandsynligt, at midlerne stammede fra en strafbar handling. I praksis er det afgørende, om der forelå omstændigheder, der burde have vakt mistanke – fx usædvanligt store indbetalinger fra ukendte personer, anmodning om straks at videreoverføre beløbet, eller åbenlys disproportion mellem den lovede betaling og den krævede indsats.

Se [praksisoversigten om databedrageri](#) for en bredere behandling af CEO-fraud og e-mail-baseret phishing mod virksomheder.

LOV [Straffeloven § 279a](#)

PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere	15.04.2024

§ 9 Identitetsmisbrug og hacking som selvstændige gerningsindhold

Smishing-bedrageri indebærer ofte overtrædelse af flere straffebestemmelser ud over § 279/§ 279 a. De vigtigste er:

Hacking – [straffelovens § 263, stk. 1](#): Uberettiget adgang til en andens oplysninger eller programmer i et informationssystem. Når gerningsmanden bruger de phishede MitID-oplysninger til at logge ind i offerets netbank, foreligger der hacking i sammenstød med databedrageri. I [SS-6507/2023-ALB](#) blev tiltalte dømt efter § 263, stk. 1 og 3 for at have skaffet sig uberettiget adgang til over 700 personers MitID-oplysninger.

Ulovlig adgang til MitID – [straffelovens § 263 a, stk. 1, nr. 3, litra a](#): Bestemmelsen rammer den, der uberettiget skaffer sig adgang til et andet datasystem. I [SS-634/2024-SVE](#) blev dette forhold medtaget i tiltalen vedrørende uberettiget adgang til ofres MitID.

Identitetsmisbrug – straffelovens § 264 e: Rigsadvokatmeddelelsen om freds- og ærekrænkelser fastslår, at der som udgangspunkt straffes i *sammenstød* i tilfælde, hvor der forud for, samtidigt med eller efter en overtrædelse af § 264 e foreligger en overtrædelse af fx § 279 om bedrageri eller § 279 a om databedrageri. Udgangspunktet for førstegangsbøden er 10.000 kr., men ved groft identitetsmisbrug kan der idømmes fængselsstraf.

LOV	Straffeloven § 263, stk. 1	Straffeloven § 263a, stk. 1	Straffeloven § 264e
PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner 07.06.2024 Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere 15.04.2024		

§ 10 Sammenfatning og centrale tendenser

SMS-phishing (smishing) er et dynamisk kriminalitetsområde, hvor dansk retspraksis stadig er under udvikling. De centrale tendenser kan opsummeres således:

- **Strafferetligt** kvalificeres smishing som databedrageri (§ 279 a), ofte i sammenstød med hacking (§ 263) og identitetsmisbrug (§ 264 e). Ved grovere organiseret kriminalitet med mange ofre og store beløb henføres forholdene under § 286, stk. 2, med strafmaksimum på 8 år. Praksis viser straffe i intervallet 1½–5 år afhængigt af rolle og omfang.
- **Civilretligt** bærer ofret som udgangspunkt en selvrisko på 8.000 kr. (betalingslovens § 100, stk. 4), når vedkommende har godkendt en MitID-transaktion efter en phishing-SMS. Finansielle Ankenævn afviser ofte at tage endelig stilling til hæftelsesniveauet og henviser sagen til domstolene, når der er tvivl om omstændighederne ved godkendelsen.
- **Organisatorisk** behandles sagerne centralt af NCIK under NSK, med SSK som tilsynsmyndighed. Den grænseoverskridende karakter af smishing – med gerningsmænd der opererer fra udlandet via spoofede SMS-afsendere – stiller særlige krav til det internationale politisamarbejde.
- **Pengemuldyr** rekrutteres til at vaske udbyttet og straffes selvstændigt for hvidvask. Forsætsvurderingen er central: det afgørende er, om pengemuldyret indså eller burde have indset, at midlerne stammede fra kriminalitet.
- **Udvisning** af udenlandske gerningsmænd er hovedreglen ved organiseret smishing, men proportionalitetsvurderingen efter EMRK art. 8 kan i konkrete tilfælde føre til et andet resultat.

For den bredere kontekst af digital bedrageri, se [praksisoversigten om databedrageri](#) (e-mail-baseret CEO-fraud og virksomhedsbedrageri) og [praksisoversigten om MitID/NemID-misbrug](#) (den videre udnyttelse efter den initiale phishing).

LOV	Betalingsloven § 100, stk. 3-4	Straffeloven § 279a	Straffeloven § 286, stk. 2	
PRAKSIS	Byretten · Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner			07.06.2024
	Byretten · Dom for omfattende bedrageri og databedrageri mod ældre borgere			15.04.2024
	Det finansielle ankenævn · Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS			18.04.2024
	Det finansielle ankenævn · Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb			06.09.2023

REFERENCE Lovgrundlag

6 paragraffer

Betalingsloven § 100	stk. 3-4	Straffeloven § 21	
Straffeloven § 263a	stk. 1	Straffeloven § 279	
Straffeloven § 279a		Straffeloven § 286	stk. 2

MATERIALE Citerede afgørelser

22 afgørelser

HØJESTERET · ØVERSTE INSTANS

3

28.06.2023	Højesterets vurdering af varetægtsfængsling ved omfattende databedrageri og påvirkningsrisiko	AM2023.06.28H
29.05.2017	Højesteret stadfæster dom for organiseret menneskehandel og databedrageri: Udnyttelse af identitet kræver ikke kendskab fra ofret	Sag 70/2017
30.06.2015	Højesteret stadfæster ubetinget udvisning i 12 år af serbisk statsborger for organiseret databedrageri af særlig grov beskaffenhed	Sag 85/2015

LANDSRETTE · ANKEINSTANS

3

11.04.2025	Betydelig fællesstraf og udvisning for omfattende bedrageri og databedrageri mod ældre borgere (ca. 42 forhold)	S-0009-25
31.01.2023	Bedrageri og medvirken til databedrageri: Frifindelse i Landsretten for lån optaget i andres navn	S-0930-22
09.12.2022	Afgørelse om hæftelse for tab ved phishing efter Betalingslovens § 100	2941-3487

BYRETTE · FØRSTE INSTANS

5

26.08.2025	Mand idømt 6 års fængsel for organiseret 'smishing' og databedrageri for over 23 millioner kroner	10075-11802
07.06.2024	Ung mand idømt fem års fængsel for omfattende phishing og databedrageri for over 27 millioner kroner	6168-7392
15.04.2024	Omfattende sag om bedrageri mod ældre borgere: Fængselsstraf og erstatningskrav	6568-7891
15.04.2024	Dom for omfattende bedrageri og databedrageri mod ældre borgere	6569-7892
15.12.2023	Omfattende dom for databedrageri: Fire tiltalte idømt lange fængselsstraffe	6497-7797

DET FINANSIELLE ANKENÆVN · NÆVN / KLAGESTANS

10

22.01.2026	Hæftelse for misbrug af betalingskort efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse i MitID	468/2025
17.01.2025	Hæftelse for 8.000 kr. ved phishing-svindler: Klager godkendte EUR-beløb i MitID i troen om fragtbetaling på 39 kr.	233/2024

19.08.2024	Hæftelse for 8.000 kr. efter phishing-mail: Groft uforsvarlig adfærd ved godkendelse af MitID-transaktion	700/2023
18.04.2024	Afvisning af sag om misbrug af MitID og korttransaktioner efter phishing-angreb via dba.dk	357/2023
18.04.2024	Indsigelse mod hæftelse for 8.000 kr. ved svindel-transaktion godkendt med MitID efter phishing-SMS	533/2023
19.03.2024	Indsigelse mod hæftelse for phishing-transaktion på 3.726,25 kr. godkendt via MitID	530/2023
18.01.2024	Indsigelse mod misbrug via Apple Pay efter phishing-SMS afvist grundet behov for bevisførelse	409/2023
22.12.2023	Indsigelse mod hæftelse for Apple Pay-transaktioner efter indrullering af betalingskort i tredjemands wallet	304/2023
06.09.2023	Groft uforsvarlig adfærd ved phishing-SMS: Hæftelse for 8.000 kr. efter godkendelse af MitID-anmodning på stort beløb	131/2023
31.05.2023	Afvisning af klage over kortmisbrug efter smishing-SMS grundet behov for bevisførelse	507/2022
PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS		1
28.04.2023	Kontrolafgift pålagt knallert for manglende p-tilladelse på privat område	park-3487

FORARBEJDE Betænkninger

1 reference

Betænkning om strafudmåling – Bind III

nr. 1581 · 2023 · Justitsministeriet