

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 bodegrunde, 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 rygrad:

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 sigtetlignende 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 forvaltnings 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 trafikikkerheden, 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 Tryk 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 · Tryk 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 glemmt](#), 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 angrebepunkt 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 databehandlertaften 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 databehandlertaften 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 databehandlertaften	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

§ 11 gebyrforbuddet

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 indsig 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 indsichtsbehandling 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

Bødeindstillingerne: niveau, kriterier og Datatilsynets

§ 12 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

Fra tilsynets indstilling til domstolens 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: flerkfaktorautentifikation ved fjernadgang, kryptering af bærbare 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 databehandlaftaler	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	Tryk 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	Tryk 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	Fødevarestyrelsens 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