

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 flerfaktorautentifikation 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 overtrædelsen 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 bødeloftet 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 overtrædelsen 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 flerfaktoraутентifikation:

»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 flerfaktoraутентifikation 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.«

Overtrædelsen 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

§ 6

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) tilregnelser** – 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		
	Byretten · Dom for overtrædelse af databeskyttelsesloven ved videregivelse af oplysninger om underslæb		
	Byretten · Taxiselskab idømt bøde for ulovlig opbevaring af oplysninger om 8,8 millioner køreture		
	Byretten · Retten i Lyngby: Afgørelse om overtrædelse af Databeskyttelsesforordningen vedrørende opbevaring af personoplysninger		

§ 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 tilregnelseskrav, 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 strafudmålingsregler.
- 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	Tvist 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