

PRAKSISSOVERSIGTER • SAMLET UDGAVE

Praksis inden for *GDPR & compliance-dokumenter*

De lovpligtige compliance-dokumenter – databehandlersaftale, fortegnelse, privatlivspolitik, DPIA og whistleblowerordning.

OVERSIGTER

6

AFGØRELSE

93

PERIODE

2004–2026

6 OVERSIGTER

Indhold

01	Artikel 30-fortegnelse	17 afg.
02	Databehandleraftale	19 afg.
03	Konsekvensanalyse (DPIA)	14 afg.
04	Privatlivspolitik	16 afg.
05	Samtykkeerklæring (GDPR)	21 afg.
06	Whistleblowerpolitik og -ordning	6 afg.

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

01

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Artikel 30-fortegnelse

Det lovpligtige interne kartotek over al behandling af personoplysninger – dataansvarliges og databehandlers dokumentation efter GDPR artikel 30

Version 1 · Opdateret 21. jul. 2026 · 17 afgørelser · 2019-2026

[Læs online](#)

INTRODUKTION

En **artikel 30-fortegnelse** – i daglig tale bare "fortegnelsen" eller "behandlingsfortegnelsen" – er den skriftlige oversigt over samtlige behandlinger af personoplysninger i en organisation. Den blev indført med [databeskyttelsesforordningen artikel 30](#) som afløser for den gamle anmeldelsesordning under persondataloven: hvor man tidligere anmeldte visse behandlinger til Datatilsynet, skal man i dag selv føre en intern fortegnelse over dem alle. Justitsministeriets betænkning nr. 1565/2017 beskriver skiftet præcist som en forpligtelse til "at opbevare intern dokumentation for behandling, der udføres under deres ansvar, i stedet for en generel anmeldelse til tilsynsmyndigheden".

Der er to parter og to varianter. Den **dataansvarlige** – den der afgør formål og hjælpemidler, jf. [artikel 4, nr. 7](#) – fører en fortegnelse efter artikel 30, stk. 1, med syv indholdskrav. **Databehandleren** – den der behandler på den dataansvarliges vegne – fører sin egen efter stk. 2 med fire indholdskrav. Begge fortegelser skal foreligge skriftligt eller elektronisk og udleveres til Datatilsynet på anmodning. Både dataansvarlige og databehandlere er selvstændige ansvarssubjekter, og begge kan straffes for at mangle deres fortegnelse.

Oversigten nedenfor er ordnet som selve dokumentet: først hvornår pligten indtræder (og hvorfor undtagelsen for virksomheder under 250 ansatte næsten aldrig kan bruges), derefter checklisten over hvad fortegnelsen skal indeholde punkt for punkt med hjemmel, så de typiske fejl med deres konsekvenser, og til sidst uddybende afsnit om rollefordelingen, undtagelsen, sletnings- og sikkerhedsoplysningerne, håndhævelsen og forholdet til privatlivspolitikken og databehandleraftalen.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Fortegnelsen er **lovpligtig for både dataansvarlige og databehandlere** – det er ikke ét dokument i en kæde, men ét dokument hos hver part, med forskelligt indhold efter henholdsvis artikel 30, stk. 1, og stk. 2.
- 02** **Undtagelsen for under 250 ansatte er i praksis illusorisk:** den bortfalder allerede, hvis behandlingen ikke er lejlighedsvis – og løn- og kundeadministration er efter Justitsministeriets betænkning nr. 1565/2017 aldrig lejlighedsvis.

- 03** Fortegnelsen er **ansvarlighedsprincippetets rygrad**: uden den kan den dataansvarlige normalt ikke påvise overholdelse, som [artikel 5, stk. 2](#) og [artikel 24, stk. 1](#) kræver.
- 04** Den **skal foreligge skriftligt eller elektronisk** og stilles til rådighed for Datatilsynet efter anmodning – det er rutinemæssigt det første dokument, tilsynet beder om, og manglende udlevering er selvstændigt strafbart.
- 05** Fortegnelsen er et **internt dokument**: den er ikke omfattet af den registreredes indsigtret efter artikel 15, men offentlige myndigheders fortegnelser kan der begæres aktindsigt i efter **offentlighedsloven**.
- 06** **Manglende eller mangelfuld fortegnelse er en selvstændig overtrædelse** – strafbar med bøde eller fængsel indtil 6 måneder efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#), og placeret i den øvre bødekategori på 10 mio. EUR/2 % efter GDPR artikel 83, stk. 4, litra a.
- 07** **Undtagelsesvurderingen foretages pr. behandlingsaktivitet**, ikke pr. organisation – man kan altså ikke fritage hele virksomheden, fordi én aktivitet er lejlighedsvis.
- 08** Fortegnelse, privatlivspolitik og databehandlaftalens bilag er **samme kartotek i tre visninger** – de skal derfor bygge på samme kortlægning, ellers modsiger de hinanden i en tilsynssag.

§ 1 Hvornår er dokumentet påkrævet?

Lovpligtig som klart udgangspunkt. [Databeskyttelsesforordningen artikel 30, stk. 1](#) pålægger *hver* dataansvarlig at føre fortegnelser over behandlingsaktiviteter under sit ansvar, og [artikel 30, stk. 2](#) pålægger *hver* databehandler det samme for de kategorier af behandling, der foretages på vegne af en dataansvarlig. Pligten gælder uanset om du er en offentlig myndighed, et aktieselskab, en forening, en enkeltmandsvirksomhed eller en it-leverandør, og den er ikke betinget af anmeldelse, tilladelse eller henvendelse fra nogen. Efter [artikel 30, stk. 3](#) skal fortegnelsen foreligge skriftligt, herunder elektronisk – en mundtlig eller "i hovedet"-forteegnelse opfylder ikke kravet.

Den betingede fritagelse – og hvorfor den sjældent holder. [Artikel 30, stk. 5](#) fritager et foretagende eller en organisation med under 250 beskæftigede – *medmindre* behandlingen (1) sandsynligvis vil medføre en risiko for registreredes rettigheder og frihedsrettigheder, (2) ikke er lejlighedsvis, eller (3) omfatter særlige kategorier af oplysninger efter [artikel 9, stk. 1](#) eller oplysninger om straffedomme og lovovertrædelser efter [artikel 10](#). De tre indskrænkninger er alternative: én af dem er nok til at pligten består. Justitsministeriets betænkning nr. 1565/2017 konkluderer direkte, at bestemmelsen "i praksis [må] antages at få et meget snævert anvendelsesområde", og at behandling i forbindelse med "sædvanlig personaleadministration under normale omstændigheder ikke vil kunne undtages efter artikel 30, stk. 5", fordi den foregår oftere end blot lejlighedsvis. Løn-, personale- og kundedata er derfor i praksis altid fortegnelsespligtige – også i den lille virksomhed.

Vurderingen sker pr. behandlingsaktivitet, ikke pr. virksomhed. Betænkningen understreger, at nogle af en virksomheds behandlingsaktiviteter kan være undtaget, mens andre ikke kan. Selv den virksomhed, der reelt kan påberåbe sig undtagelsen for en enkelt lejlighedsvis behandling, skal derfor føre fortegnelse over resten – og skal kunne redegøre for, hvorfor netop den ene aktivitet er lejlighedsvis. Konsekvensen er, at det stort set altid er billigere og sikrere at føre én komplet fortegnelse end at forsøge at dokumentere en fritagelse.

Frivilligt, men retssikrende, er kun det der ligger ud over minimumskravene. Artikel 30 kræver ikke, at fortegnelsen angiver behandlingsgrundlaget (hjemlen) for hver aktivitet, systemnavne, risikoniveau eller henvisning til databehandlafter. Datatilsynets egne skabeloner og almindelig praksis medtager dem alligevel, fordi de gør fortegnelsen brugbar som styringsværktøj og som dokumentation efter ansvarlighedsprincippet i [artikel 5, stk. 2](#). Betænkning nr. 1565 bemærker udtrykkeligt, at "den dataansvarlige [er] naturligvis ikke afskåret fra ved egen drift at dokumentere flere oplysninger, end hvad der følger af kravet".

§ 2 Det skal dokumentet indeholde

1. Navn på og kontaktoplysninger for den dataansvarlige og – hvor det er relevant – den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren (DPO). (*Databeskyttelsesforordningen § 30, stk. 1*)
2. Formålene med hver behandling. Aktiviteter med ét samlet, logisk sammenhængende formål kan efter betænkning nr. 1565/2017 samles i én post – men vage formål som "drift" eller "sikkerhed" er ikke tilstrækkeligt udtrykkeligt angivne. (*Databeskyttelsesforordningen § 30, stk. 1*)
3. En beskrivelse af kategorierne af registrerede (fx medarbejdere, kunder, ansøgere, borgere) og kategorierne af personoplysninger (fx identifikations-, kontakt-, økonomi- og helbredsoplysninger). (*Databeskyttelsesforordningen § 30, stk. 1*)
4. De kategorier af modtagere, som oplysningerne er eller vil blive videregivet til – herunder databehandlere, offentlige myndigheder, koncernselskaber og modtagere i tredjelande. (*Databeskyttelsesforordningen § 30, stk. 1*)
5. Hvor det er relevant: overførsler til tredjeland eller international organisation med angivelse af landet/organisationen, og ved overførsler efter artikel 49, stk. 1, andet afsnit, tillige dokumentation for de passende garantier. (*Databeskyttelsesforordningen § 30, stk. 1*)
6. Hvis det er muligt: de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger. Fristerne skal være reelle og efterleves i systemerne – ikke blot noteret på papir. (*Databeskyttelsesforordningen § 30, stk. 1*)
7. Hvis det er muligt: en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger efter artikel 32, stk. 1 – fx adgangsstyring, kryptering, logning og backup. (*Databeskyttelsesforordningen § 32, stk. 1*)
8. Databehandlerens variant skal indeholde kontaktoplysninger på databehandleren og på hver dataansvarlig, kategorierne af behandling foretaget for den enkelte dataansvarlige, eventuelle tredjelandsoverførsler samt en generel beskrivelse af sikkerhedsforanstaltningerne. (*Databeskyttelsesforordningen § 30, stk. 2*)
9. Fortegnelsen skal foreligge skriftligt, herunder elektronisk. Elektronisk opbevaring er tilstrækkelig, når den kan udprintes og udleveres. (*Databeskyttelsesforordningen § 30, stk. 3*)
- 10.

Fortegnelsen skal efter anmodning stilles til rådighed for Datatilsynet – der skal derfor være en navngiven ansvarlig, som kan fremfinde og udlevere den aktuelle version uden forsinkelse. (*Databeskyttelsesforordningen § 30, stk. 4*)

11. Fortegnelsen skal holdes ajour, så den til enhver tid afspejler de faktiske behandlinger – ellers kan den dataansvarlige ikke påvise overholdelse efter ansvarlighedsprincippet. (*Databeskyttelsesforordningen § 5, stk. 2*)
12. Ud over minimumskravene bør fortegnelsen angive behandlingsgrundlaget (hjemlen) pr. aktivitet, det anvendte system, den relevante databehandlersaftale og eventuel DPIA-status – det er ikke krævet af artikel 30, men gør fortegnelsen anvendelig som styringsværktøj og som dokumentation ved tilsyn.

LOV

[Databeskyttelsesforordningen § 5, stk. 2](#)[Databeskyttelsesforordningen § 30, stk. 1, 2, 3, 4](#)[Databeskyttelsesforordningen § 32, stk. 1](#)

§ 3 Dataansvarlig eller databehandler – to fortegnelser, ikke én

Det første spørgsmål er aldrig, hvad fortegnelsen skal indeholde, men hvilken rolle man har. En **dataansvarlig** er efter [artikel 4, nr. 7](#) den, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der behandles personoplysninger. En **databehandler** er efter nr. 8 den, der behandler oplysninger på den dataansvarliges vegne. Rollen afgør, hvilken af de to fortegnelsesvarianter man skal føre – og de fleste virksomheder er begge dele på én gang: dataansvarlig for egne medarbejdere og kunder, databehandler for de kunder man leverer en tjeneste til. Så skal der føres to fortegnelser, eller én fortegnelse med to klart adskilte dele.

Den dataansvarliges fortegnelse efter [artikel 30, stk. 1](#) beskriver *behandlingsaktiviteter* – formål, registrerede, oplysningstyper, modtagere, tredjelande, slettefrister og sikkerhed. Databehandlerens fortegnelse efter [artikel 30, stk. 2](#) beskriver derimod *kategorier af behandling foretaget for hver enkelt dataansvarlig* – altså hvem man arbejder for, og hvad man gør for dem. Betænkning nr. 1565/2017 fremhæver, at databehandlerens fortegnelsespligt er en egentlig nyskabelse i forhold til persondataloven, hvor kun edb-servicebureauer var anmeldelsespligtige; efter GDPR er *alle* databehandlere omfattet.

Rollen kan skifte undervejs. Overtræder en databehandler forordningen ved selv at fastlægge formål og hjælpemidler, anses den efter [artikel 28, stk. 10](#) for dataansvarlig for den pågældende behandling – og skal dermed føre den fulde stk. 1-fortegnelse for den. Er der derimod tale om **fælles dataansvar** efter [artikel 26](#), skal begge parter fremgå af fortegnelsens litra a. Er den dataansvarlige eller databehandleren etableret uden for EU, skal også repræsentanten efter [artikel 27](#) angives, og er der udpeget en databeskyttelsesrådgiver efter [artikel 37](#) – hvilket altid er obligatorisk for offentlige myndigheder – skal dennes kontaktoplysninger med.

LOV

[Databeskyttelsesforordningen § 4](#)[Databeskyttelsesforordningen § 26](#)[Databeskyttelsesforordningen § 30, stk. 1, 2](#)[Databeskyttelsesforordningen § 37, stk. 1](#)

§ 4 250-ansatte-undtagelsen: hvorfor den næsten aldrig kan bruges

[Artikel 30, stk. 5](#) er skrevet som en lempelse for små organisationer, men er konstrueret som en undtagelse med tre selvstændige tilbagefald. Fritagelsen gælder kun, hvis foretagendet beskæftiger under 250 personer **og**

ingen af følgende tre forhold foreligger: at behandlingen sandsynligvis vil medføre en risiko for registreredes rettigheder og frihedsrettigheder, at behandlingen ikke er lejlighedsvis, eller at den omfatter særlige kategorier af oplysninger efter [artikel 9, stk. 1](#) eller straffedomsoplysninger efter [artikel 10](#).

Det er kriteriet "ikke lejlighedsvis", der i praksis lukker døren. Justitsministeriets betænkning nr. 1565/2017 formulerer det utvetydigt: man skal som dataansvarlig "under alle omstændigheder leve op til fortegnelseskravet i artikel 30, stk. 1-2 – også selvom man beskæftiger under 250 personer", hvis behandlingen vil foregå oftere end blot lejlighedsvis. Og betænkningen tilføjer, at behandling i forbindelse med sædvanlig personaleadministration "under normale omstændigheder ikke vil kunne undtages efter artikel 30, stk. 5", fordi den må antages normalt at foregå oftere end blot lejlighedsvis. Udvalget konkluderer samlet, at bestemmelsen "i praksis [må] antages at få et meget snævert anvendelsesområde".

En anden ofte overset detalje er, at vurderingen ikke er organisationsdækkende. Efter betænkningen må det antages, at "nogle af en virksomheds eller organisations behandlingsaktiviteter vil kunne undtages fra fortegnelseskravet, mens andre behandlingsaktiviteter ikke kan" – det afgørende er den enkelte behandlingsaktivitet. Den virksomhed, der vil bruge undtagelsen, skal derfor kunne udpege præcis hvilke aktiviteter der er lejlighedsvis, risikofri og uden følsomme oplysninger, og føre fortegnelse over alle andre. I praksis kræver det samme kortlægningsarbejde som at føre den fulde fortegnelse – og det er derfor, langt de fleste rådgivere anbefaler simpelthen at føre den.

Endelig er tærsklen "beskæftiger under 250 personer", ikke antal ansatte i selskabsretlig forstand. Vikarer, konsulenter og deltidsansatte tæller med i den vurdering, og tallet skal måles løbende – en vækstvirksomhed kan altså krydse grænsen uden at bemærke det.

LOV

[Databeskyttelsesforordningen § 9, stk. 1](#)[Databeskyttelsesforordningen § 10](#)[Databeskyttelsesforordningen § 30, stk. 5](#)

Slettefrister og sikkerhedsbeskrivelse – de to punkter praksis hænger folk op på

Litra f og g i [artikel 30, stk. 1](#) er formuleret med forbeholdet "hvis det er muligt", og det læses ofte som en frivillighed. Det er en misforståelse. Slettefristerne hænger uløseligt sammen med opbevaringsbegrænsningen i [artikel 5, stk. 1, litra e](#), og sikkerhedsbeskrivelsen hænger sammen med [artikel 32, stk. 1](#). Betænkning nr. 1565/2017 bemærker netop om litra g, at kravet "i vidt omfang allerede følger af gældende ret og forordningen, hvorfor nyskabelsen alene består i, at disse overvejelser skal dokumenteres elektronisk og skriftligt".

Danmarks skarpeste praksis på området er sletningssagerne. I sagen mod IDdesign A/S fra 2019 konstaterede Datatilsynet ved et uanmeldt tilsynsbesøg, at et udfaset ERP-system indeholdt oplysninger om ca. 385.000 tidligere kunder helt tilbage fra 2010 uden fastsatte slettefrister, at en selvfastsat frist i et andet system ikke var effektueret, og at der manglede dokumenterede sletteprocedurer i to øvrige systemer. Datatilsynet udtalte alvorlig kritik, politianmeldte virksomheden og indstillede en bøde på 1,5 mio. kr. Tilsynet formulerede standarden sådan, at den dataansvarlige "skal fastlægge og dokumentere procedurer for opfølgning på, at sletning af personoplysninger er foretaget korrekt og som forventet".

Den kommunale linje er den samme. I sagen om Mariagerfjord Kommune (2022) gav Datatilsynet påbud om at udarbejde en liste over systemer med personoplysninger inklusive slettefunktioner og fastsatte slettefrister, at

slette overskredne oplysninger og at lægge en plan med leverandørerne for resten – og afviste udtrykkeligt, at manglende systemteknisk understøttelse kan tilsidesætte opbevaringsbegrænsningen. Da Aalborg Kommunes egen DPO-årsrapport i 2026 viste, at ingen af kommunens syv forvaltninger havde løst sletteopgaven, meddelte Datatilsynet et enslydende påbud og henviste udtrykkeligt til Mariagerfjord-afgørelsen som "en detaljeret køreplan". Også over for Udlændinge- og Integrationsministeriet har tilsynet kritiseret, at der ikke blev ført kontrol med, om en automatisk slettemekanisme rent faktisk virkede.

Pointen for fortegnelsen er direkte: den systemliste med slettefrister, som Datatilsynet påbyder i disse sager, er reelt indholdet af litra f. Fører man fortegnelsen ordentligt fra begyndelsen – med reelle, systemunderstøttede og kontrollerede frister – har man allerede leveret det, tilsynet ellers udsteder påbud om.

LOV	Databeskyttelsesforordningen § 5, stk. 1	Databeskyttelsesforordningen § 30, stk. 1
	Databeskyttelsesforordningen § 32, stk. 1	
PRAKSIS	Datatilsynet · Datatilsynet meddeler Aalborg Kommune påbud om systemoverblik og sletning af personoplysninger	05.05.2026
	Datatilsynet · Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	10.07.2024
	Datatilsynet · Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	15.07.2022
	Datatilsynet · Alvorlig kritik og bødeindstilling til IDdesign for overtrædelse af princippet om opbevaringsbegrænsning	03.06.2019

§ 6 Når Datatilsynet banker på: udlevering, tilsyn og sanktioner

Fortegnelsens praktiske funktion viser sig i tilsynssituationen. Efter [artikel 30, stk. 4](#) skal fortegnelserne stilles til rådighed for tilsynsmyndigheden efter anmodning, og præambelbetragtning 82 forklarer hvorfor: fortegnelserne skal kunne bruges "til at føre tilsyn med sådanne behandlingsaktiviteter". Dertil kommer den generelle samarbejdspligt i [artikel 31](#), tilsynets undersøgelsesbeføjelser i [artikel 58, stk. 1](#) og de nationale beføjelser i [databeskyttelsesloven § 29](#), hvorefter Datatilsynet kan kræve enhver oplysning af betydning for dets virksomhed og uden retskendelse har adgang til alle lokaler, hvorfra der behandles personoplysninger. Tilsynskompetencen følger af [§ 27](#).

Datatilsynet har ført dedikerede tilsyn netop med artikel 30-fortegnelser. I august 2020 afsluttede tilsynet en serie sager rettet direkte mod kommunernes fortegnelser efter artikel 30, stk. 1 – herunder Varde Kommune (hvor også artikel 32, stk. 1, indgik), Holstebro Kommune og Ringkøbing-Skjern Kommune, hvor tilsynet efter en gennemgang ikke fandt anledning til kritik. I de bredere modenhedstilsyn med statslige myndigheder og private virksomheder i 2020-2021 indgik fortegnelsen som en af parametrene; over for Udlændingestyrelsen bemærkede tilsynet udtrykkeligt, at opdatering af fortegnelse, risikovurderinger og beredskabsplaner kun var delvist implementeret, og over for både Odense Kommune, Udviklings- og Forenklingsstyrelsen og siden Esbjerg Kommune har tilsynet fremhævet, at manglende dokumentation gør det svært inden for rimelig tid at *påvise* overholdelse.

Sanktionerne er reelle. Overtrædelse af artikel 30 falder i kategorien i [artikel 83, stk. 4, litra a](#) – bøder på op til 10 mio. EUR eller 2 % af den globale årsomsætning. I Danmark udmøntes det gennem straffesystemet: efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#) straffes overtrædelse af den dataansvarliges og databehandlerens forpligtelser efter forordningens artikel 25-39 – hvilket omfatter artikel 30 – med bøde eller fængsel indtil 6 måneder. Undlader man at efterkomme Datatilsynets krav om oplysninger eller et påbud, straffes det særskilt

efter § 41, stk. 2, nr. 5 og 6. Juridiske personer kan straffes efter § 41, stk. 6, og bestemmelsen fraviger udtrykkeligt straffelovens § 27, stk. 2, så også offentlige myndigheder kan straffes for overtrædelser begået ved udøvelse af virksomhed, der ikke svarer til privat virksomhed. Forældelsesfristen er 5 år, jf. § 41, stk. 7, og mindre sager kan afgøres med bødeforelæg efter [§ 42](#).

Manglende samarbejde er i sig selv skærpende. I sagen mod JobTeam A/S politianmeldte Datatilsynet virksomheden og indstillede en bøde på 50.000 kr., blandt andet fordi den ikke besvarede tilsynets gentagne skriftlige og telefoniske henvendelser – tilsynet betragtede den manglende respons som "en alvorlig hindring for håndhævelsen af databeskyttelsesreglerne". Et nærmere billede af tilsynets reaktionsmønster og bødeniveau findes i vores [oversigt over Datatilsynets afgørelser](#) og i [oversigten over datatilsynsbøder og GDPR-overtrædelser](#).

LOV

[Databeskyttelsesforordningen § 30, stk. 4](#)[Databeskyttelsesforordningen § 58, stk. 1](#)[Databeskyttelsesforordningen § 83, stk. 4](#)[Databeskyttelsesloven § 29, stk. 1](#)[Databeskyttelsesloven § 41, stk. 1](#)[Databeskyttelsesloven § 42](#)

PRAKSIS	Datatilsynet · Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	22.12.2023
	Datatilsynet · Alvorlig kritik af kommunes sene anmeldelse af brud på persondatasikkerheden vedrørende følsomme oplysninger	31.08.2023
	Datatilsynet · Kritik af offentlig myndighed for utilstrækkelig sikkerhed og for sen anmeldelse af brud på persondatasikkerheden	31.08.2023
	Datatilsynet · Datatilsynet finder ingen grundlag for kritik af Udlændingestyrelsens behandlingssikkerhed vedrørende adgangsstyring og logning	15.01.2021
	Datatilsynet · Tilsyn med Udviklings- og Foreklingsstyrelsens behandlingssikkerhed fører ikke til kritik	15.01.2021
	Datatilsynet · Datatilsynets kontrol af informationssikkerhed og risikostyring i Odense Kommune	15.01.2021
	Datatilsynet · Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter	10.08.2020
	Datatilsynet · Datatilsynets tilsyn med Holstebro Kommunes fortegnelser over behandlingsaktiviteter	10.08.2020
	Datatilsynet · Datatilsynets tilsyn med Ringkøbing-Skjern Kommunes fortegnelser resulterer i ingen kritik	10.08.2020
	Datatilsynet · JobTeam politianmeldt og indstillet til bøde for manglende samarbejde og tilsidesættelse af indsichtsret	15.05.2020

§ 7 Samme kartotek, tre visninger: fortegnelse, privatlivspolitik og databehandleraftale

Fortegnelsen står ikke alene. Den bygger på den samme kortlægning som to andre dokumenter, men vender den mod tre forskellige modtagere – og det er netop derfor, uoverensstemmelser mellem dem er så farlige i en tilsynssag.

Fortegnelsen er den interne, fuldstændige visning rettet mod Datatilsynet. Betænkning nr. 1565/2017 er meget klar på dens retlige karakter: "en fortegnelse er **ikke** omfattet af den registreredes ret til indsigt", og "med forordningens artikel 30 skabes alene en forpligtelse til at udarbejde en **intern** fortegnelse – til erstatning for den eksterne anmeldelse efter gældende ret". For offentlige myndigheder tilføjer betænkningen dog, at der "vil være mulighed for at få aktindsigt i fortegnelser efter de nærmere regler i **offentlighedsloven**" – en fortegnelse i en kommune eller styrelse er altså ikke fortrolig i samme grad som i en privat virksomhed.

Privatlivspolitikken er den eksterne, forkortede visning rettet mod de registrerede og opfylder oplysningspligten i [artikel 13](#) og artikel 14. Indholdsmæssigt overlapper den fortegnelsen på formål, oplysningstyper, modtagere, tredjelande og opbevaringstid – men den tilføjer behandlingsgrundlag, rettighedsbeskrivelse og klagevejledning, og udelader sikkerhedsbeskrivelsen. Datatilsynet har i sit tematiske tilsyn med ejendomsadministratorer i 2025 fastslået, at det ikke er tilstrækkeligt blot at henvise til privatlivspolitikken på hjemmesiden, når konkrete oplysninger skal gives til en registreret – og i sagen mod SIF Gruppen A/S udtalte tilsynet alvorlig kritik af, at skiltning ved tv-overvågning og lokalaftaler om GPS-sporing ikke oplyste om kontrolformål, retsgrundlag og rettigheder. Er behandlingen ikke ordentligt beskrevet i fortegnelsen, bliver privatlivspolitikken næsten uundgåeligt også mangelfuld.

Databehandleraftalens bilag er den kontraktuelle visning mellem parterne og skal efter [artikel 28, stk. 3](#) fastsætte behandlingens genstand, varighed, karakter og formål samt typen af personoplysninger og kategorierne af registrerede – altså præcis de oplysninger, der også står i fortegnelsens litra b og c. Datatilsynet har i 2026 over for det fælleskommunale Databehandlersekretariat præciseret, at oversigten over underdatabehandlere skal være retvisende, vedvarende tilgængelig og ajourført, og at det ikke er nok at angive leverandørens virksomhedsadresse, hvis behandlingen faktisk sker et andet sted. En fortegnelse, der angiver andre modtagere eller andre lokationer end databehandleraftalens bilag, er derfor et selvstændigt problem.

Endelig hænger fortegnelsen sammen med konsekvensanalysen: viser en behandlingsaktivitet i fortegnelsen sig at indebære høj risiko, udløser det pligten til en DPIA efter [artikel 35](#). Fortegnelsen er i praksis den liste, man screener for DPIA-pligt – endnu en grund til at den skal være fuldstændig og ajour.

LOV	Databeskyttelsesforordningen § 13, stk. 1	Databeskyttelsesforordningen § 28, stk. 3
	Databeskyttelsesforordningen § 30, stk. 3	Databeskyttelsesforordningen § 35, stk. 1
PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	23.01.2026
	Datatilsynet · Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	12.12.2025
	Datatilsynet · Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	07.08.2020

§ 8 Typiske faldgruber

"Vi er under 250 ansatte, så vi er fritaget". Det er den hyppigste og dyreste misforståelse. Undtagelsen i [artikel 30, stk. 5](#) bortfalder allerede, når behandlingen ikke er lejlighedsvis – og Justitsministeriets betænkning nr. 1565/2017 fastslår, at sædvanlig personaleadministration normalt ikke kan undtages, netop fordi den foregår løbende. Enhver virksomhed med lønudbetaling, kundekartotek eller ansøgninger er derfor fortegnelsespligtig, uanset antal ansatte. Resultatet af fejlen er, at man ved første tilsyn står helt uden det dokument, tilsynet efterspørger.

Fortegnelsen laves én gang i 2018 og ajourføres aldrig. En fortegnelse, der ikke afspejler nye systemer, nye leverandører eller ændrede formål, dokumenterer intet – den dokumenterer tværtimod, at organisationen ikke har styr på sine behandlinger. Datatilsynet har i sine modenhedstilsyn med statslige myndigheder udtrykkeligt noteret, at opdatering af fortegnelsen kun var delvist implementeret, og har generelt vurderet, at manglende dokumentation gør det svært "inden for rimelig tid" at påvise overholdelse efter [artikel 5, stk. 2](#). Uden ajourføring mister fortegnelsen sin bevisværdi præcis når man har brug for den.

Slettefrister står i fortegnelsen, men effektueres ikke i systemerne. Artikel 30, stk. 1, litra f, kræver, at de forventede slettefrister fremgår – men opbevaringsbegrænsningen i artikel 5, stk. 1, litra e, kræver, at de også overholdes. Datatilsynet politianmeldte IDdesign og indstillede en bøde på 1,5 mio. kr., fordi oplysninger om ca. 385.000 tidligere kunder lå uden fastsatte eller effektuerede slettefrister, og har givet både Mariagerfjord Kommune og Aalborg Kommune påbud om at udarbejde en systemliste med slettefrister og faktisk slette de overskredne data. Datatilsynet har samtidig afvist, at manglende systemteknisk understøttelse hos leverandøren kan undskylde manglende sletning.

Privatlivspolitikken bruges som fortegnelse – eller omvendt. De to dokumenter har forskellige adressater og forskelligt indhold: privatlivspolitikken opfylder oplysningspligten over for de registrerede efter [artikel 13](#) og [artikel 14](#), mens fortegnelsen er et internt dokument til brug for tilsynet. En privatlivspolitik indeholder fx ikke sikkerhedsbeskrivelsen efter litra g, og en fortegnelse indeholder ikke klagevejledning. Bruger man den ene som den anden, mangler man krævet indhold i begge ender – og risikerer kritik for både artikel 30 og oplysningspligten.

Databehandleren fører slet ingen fortegnelse. Fortegnelsespligten for databehandlere var en nyskabelse med GDPR, og mange it- og servicevirksomheder tror stadig, at ansvaret alene ligger hos kunden. Det er forkert: [artikel 30, stk. 2](#) er en selvstændig pligt, og databehandleren er selvstændigt ansvarssubjekt efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#). Databehandleren skal især kunne oplyse, hvilke dataansvarlige den arbejder for, og hvilke kategorier af behandling der udføres for hver af dem.

Modtagerkategorier, underdatabehandlere og behandlingslokationer springes over. Litra d og e er de punkter, der oftest udelades – netop dem tilsynet bruger til at kortlægge datastrømme. Datatilsynet har i 2026 over for det fælleskommunale Databehandlersekretariat fastslået, at listen over (under)databehandlere skal være "retvisende, vedvarende tilgængelig og ajourført", og at det ikke er nok blot at angive leverandørens virksomhedsadresse, hvis behandlingen faktisk sker et andet sted. Uklare modtagerangivelser fører let til, at tredjelandsoverførsler bliver overset – og de sanktioneres i den høje bødekategori.

Fortegnelsen kan ikke fremskaffes, når Datatilsynet spørger. Efter [artikel 30, stk. 4](#) og samarbejdspligten i [artikel 31](#) skal fortegnelsen stilles til rådighed på anmodning, og [databeskyttelsesloven § 29, stk. 1](#) giver tilsynet ret til at kræve enhver oplysning af betydning for dets virksomhed. Manglende svar er ikke en passiv fejl: Datatilsynet politianmeldte JobTeam A/S og indstillede en bøde på 50.000 kr., netop fordi virksomheden ikke besvarede tilsynets gentagne henvendelser, og lagde vægt på manglende samarbejde som skærpende omstændighed.

Offentlige myndigheder glemmer, at fortegnelsen kan blive undergivet aktindsigt. Fortegnelsen er ikke omfattet af den registreredes indsichtsret efter artikel 15 – men for offentlige myndigheder kan der efter betænkning nr. 1565/2017 gives aktindsigt i den efter **offentlighedsloven**. Skriver man derfor interne kommentarer, leverandørkritik eller "husk at rydde op"-noter direkte i fortegnelsen, risikerer man at de bliver offentligt tilgængelige. Interne handlingsplaner bør holdes i et separat dokument.

§ 9 Relaterede dokumenter

- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
-

Privatlivspolitik – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på

- **Konsekvensanalyse (DPIA)** – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet
- **Samtykkeerklæring (GDPR)** – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)

REFERENCE Lovgrundlag

5 paragraffer

Databeskyttelsesforordningen § 5	stk. 2	Databeskyttelsesforordningen § 30	stk. 1, 2, 4, 5
Databeskyttelsesforordningen § 32	stk. 1	Databeskyttelsesloven § 29	stk. 1
Databeskyttelsesloven § 41	stk. 1		

MATERIALE Citerede afgørelser

17 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS

17

05.05.2026	Datatilsynet meddeler Aalborg Kommune påbud om systemoverblik og sletning af personoplysninger	2026-432-0055
23.01.2026	Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	2025-211-3556
12.12.2025	Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	2025-41-0139
10.07.2024	Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	2023-421-0015
22.12.2023	Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	2023-423-0006
31.08.2023	Alvorlig kritik af kommunes sene anmeldelse af brud på persondatasikkerheden vedrørende følsomme oplysninger	2021-423-0244
31.08.2023	Kritik af offentlig myndighed for utilstrækkelig sikkerhed og for sen anmeldelse af brud på persondatasikkerheden	2021-423-0247
15.07.2022	Alvorlig kritik og påbud til Mariagerfjord Kommune for brister i it-sikkerhed og logning	2022-423-0261
15.01.2021	Datatilsynet finder ingen grundlag for kritik af Udlændingestyrelsens behandlingssikkerhed vedrørende adgangsstyring og logning	2020-421-0077
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

10.08.2020	Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter	2018-423-0018
10.08.2020	Datatilsynets tilsyn med Holstebro Kommunes fortegnelser over behandlingsaktiviteter	2018-423-0019
10.08.2020	Datatilsynets tilsyn med Ringkøbing-Skjern Kommunes fortegnelser resulterer i ingen kritik	2018-423-0020
07.08.2020	Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	2019-41-0043
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

02

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Databehandleraftale

Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold, tilsynspligt og faldgruber

Version 1 · Opdateret 21. jul. 2026 · 19 afgørelser · 2019-2026

[Læs online](#)

INTRODUKTION

En **databehandleraftale** er den skriftlige kontrakt, der skal regulere forholdet, når en virksomhed eller myndighed (den *dataansvarlige*) lader en anden part (*databehandleren*) behandle personoplysninger på sine vegne – typisk hosting, cloud, lønsystem, CRM, //supportydelser, backup, nyhedsbrevsværktøj eller ekstern it-drift. Kravet følger direkte af [databeskyttelsesforordningen artikel 28, stk. 3](#), som er umiddelbart gældende i Danmark, og aftalen skal foreligge skriftligt, herunder elektronisk, jf. [artikel 28, stk. 9](#).

Parterne er altid to (eller flere) selvstændige juridiske enheder: den dataansvarlige, der efter [artikel 4, nr. 7](#) afgør formål og hjælpemidler, og databehandleren, der efter [artikel 4, nr. 8](#) alene behandler oplysningerne på den dataansvarliges vegne. Rollefordelingen afgøres af de faktiske forhold – ikke af hvad parterne kalder hinanden i kontrakten. Ligger der reelt et selvstændigt skøn hos leverandøren, er vedkommende selvstændigt dataansvarlig, og en databehandleraftale er da både overflødig og direkte vildledende.

Oversigten er ordnet efter dokumentets naturlige forløb: først *hvornår* pligten udløses, dernæst *hvad* aftalen som minimum skal indeholde (checklisten følger art. 28, stk. 3, litra a-h), og til sidst de fejl der i Datatilsynets praksis faktisk udløser kritik, påbud og bødeindstillinger. Undervejs uddybes rollefordelingen, instruksens betydning, underdatabehandlerkæden, tredjelandsoverførsler og den løbende tilsynspligt, der ikke ophører med aftalens underskrift.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Databehandleraftalen er **lovpligtig** efter [databeskyttelsesforordningen artikel 28, stk. 3](#), når en leverandør behandler personoplysninger på dine vegne – og den skal foreligge skriftligt (herunder elektronisk), inden behandlingen begynder.
- 02** Rollefordelingen afgøres af de **faktiske forhold**, ikke af kontraktens overskrift: har leverandøren eget skøn over formål og væsentlige midler, er vedkommende selvstændigt dataansvarlig, og en databehandleraftale er da forkert.
- 03** Aftalen skal som minimum indeholde alle otte elementer i art. 28, stk. 3, litra a-h – mangler ét af dem, er aftalen mangelfuld, uanset hvor omfangsrig den ellers er.

- 04** En databehandler, der behandler oplysninger til egne formål eller uden for instruksen, anses efter [artikel 28, stk. 10](#) selv for dataansvarlig for den behandling – med fuldt selvstændigt ansvar til følge.
- 05** Aftalen er ikke nok i sig selv: ansvarlighedsprincippet i [artikel 5, stk. 2](#) og [artikel 24, stk. 1](#) kræver, at du **fører løbende, dokumenteret tilsyn** med at aftalen faktisk overholdes.
- 06** Standardkontraktbestemmelser om tredjelandsoverførsel (SCC'er) kan **ikke stå alene** som databehandlersaftale – de dækker overførselsgrundlaget, ikke minimumskravene i art. 28, stk. 3.
- 07** Overtrædelse af art. 28 er omfattet af det høje bødeloft i [artikel 83, stk. 4](#) (op til 10 mio. EUR eller 2 % af global omsætning) og straffes i Danmark med bøde eller fængsel indtil 6 måneder efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#).
- 08** Både dataansvarlig og databehandler kan gøres erstatningsansvarlige over for den registrerede efter [artikel 82](#) – og de hæfter solidarisk, når begge er involveret i samme behandling.

§ 1 Hvornår er dokumentet påkrævet?

Lovpligtig – uden undtagelse og uden bagatelgrænse. Så snart en fysisk eller juridisk person behandler personoplysninger på den dataansvarliges vegne, *skal* behandlingen være reguleret af en kontrakt eller et andet retligt bindende dokument, jf. [artikel 28, stk. 3](#). Der er ingen undtagelse for små virksomheder, for få registrerede, for koncernforbundne selskaber eller for kortvarige forløb. Aftalen skal foreligge, **inden** behandlingen påbegyndes – en aftale indgået efterfølgende reparerer ikke den mellemliggende periode, hvor overladelsen var uhjemlet. Bemærk desuden, at kravet ikke kun rammer den dataansvarlige: databehandleren må efter [artikel 28, stk. 2](#) og [stk. 4](#) heller ikke selv anvende en underdatabehandler uden både godkendelse og en tilsvarende aftale i næste led.

Betinget – pligten udløses af rollen, ikke af kontrakttypen. Det afgørende er, om leverandøren behandler oplysninger *på vegne af* dig og efter din instruks. Er svaret ja – også selv om ydelsen primært er noget andet end databehandling – udløses aftalekravet. Typiske udløsende omstændigheder: leverandøren hoster, drifter, supporterer eller har fjernadgang til et system med personoplysninger; leverandøren opbevarer backup; leverandøren udfører opgaven efter en detaljeret og bindende instruks uden eget skøn. Omvendt udløses pligten *ikke*, når modparten fastlægger sit eget formål og selv bærer et fagligt eller retligt ansvar – revisor, advokat, ekstern rådgiver og typisk også rekrutteringsbureauer og eksterne whistleblower-administratorer med selvstændige vurderingsbeføjelser er som udgangspunkt selvstændigt dataansvarlige. Rene faciliteter uden adgang til data – fx colocation, hvor leverandøren alene leverer plads, strøm, køling og netværk – udløser heller ikke aftalekravet, men gør det, så snart der leveres tillægsydelser som backup, firewall eller hardwarehåndtering med indblik i data.

Særregel for retshåndhævelse. For politiet, anklagemyndigheden, kriminalforsorgen m.fl. gælder GDPR ikke, men et tilsvarende og lige så bindende krav i [retshåndhævelsesloven § 22, stk. 2](#), der oplister kravene til den skriftlige aftale, herunder at overladelse til en anden databehandler efter en generel aftale skal varsles senest 14 dage forud, jf. [§ 22, stk. 3](#).

Frivilligt, men retssikrende. Selve databehandleraftalen er aldrig frivillig, men det *er* frivilligt at gå videre end minimumskravene: fastsætte konkrete slettefrister, krav om kryptering, responstider ved indsigtsanmodninger, ISAE 3000-revisionserklæringer, bod ved misligholdelse og en egentlig exitplan. Uden sådanne vilkår står du med en aftale, der formelt opfylder art. 28, men som i praksis er svær at håndhæve. Er modparten derimod selvstændigt dataansvarlig, findes ingen aftalepligt efter art. 28 – her kan et fælles dataansvar efter [artikel 26](#) være påkrævet, og ellers er en fortrolighedsaftale eller en datadelingsaftale den frivillige, men anbefalelsesværdige løsning.

§ 2 Det skal dokumentet indeholde

1. Aftalen skal foreligge skriftligt, herunder elektronisk, og være et retligt dokument der er bindende for databehandleren i forhold til den dataansvarlige. Den kan udformes som selvstændig aftale eller som et afsnit/bilag i hovedkontrakten. (*Databeskyttelsesforordningen § 28, stk. 9*)
2. Aftalen skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger, kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Rammen skal være konkret nok til, at man kan se præcis hvilke oplysninger leverandøren behandler og hvorfor. (*Databeskyttelsesforordningen § 28, stk. 3*)
3. Det skal fremgå, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige – herunder for så vidt angår overførsel til tredjelande. Aftalen skal desuden pålægge databehandleren omgående at underrette den dataansvarlige, hvis en instruks efter databehandlerens opfattelse strider mod databeskyttelsesreglerne. (*Databeskyttelsesforordningen § 28, stk. 3*)
4. Databehandleren skal sikre, at de personer, der er autoriseret til at behandle oplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. (*Databeskyttelsesforordningen § 28, stk. 3*)
5. Databehandleren skal iværksætte alle sikkerhedsforanstaltninger, som kræves efter artikel 32 – pseudonymisering/kryptering, fortrolighed, integritet, tilgængelighed, robusthed samt regelmæssig afprøvning. Foranstaltningerne bør konkretiseres i et bilag, så de kan kontrolleres. (*Databeskyttelsesforordningen § 32, stk. 1*)
6. Aftalen skal fastsætte betingelserne for brug af underdatabehandlere: forudgående specifik eller generel skriftlig godkendelse, underretning om planlagte tilføjelser eller udskiftninger, og en reel mulighed for den dataansvarlige at gøre indsigelse. En "flydende" underdatabehandlerliste, som leverandøren ensidigt kan ændre, opfylder ikke kravet. (*Databeskyttelsesforordningen § 28, stk. 2*)
7. Databehandleren skal pålægge enhver underdatabehandler de samme databeskyttelsesforpligtelser via en tilsvarende aftale og forbliver fuldt ansvarlig over for den dataansvarlige for underdatabehandlerens opfyldelse. Beskyttelsesniveauet må ikke sænkes ned gennem leverandørkæden. (*Databeskyttelsesforordningen § 28, stk. 4*)
8. Databehandleren skal – under hensyn til behandlingens karakter og så vidt muligt ved passende tekniske og organisatoriske foranstaltninger – bistå den dataansvarlige med at besvare de registreredes anmodninger om indsigt, sletning, berigtigelse, dataportabilitet mv. efter forordningens kapitel III. (*Databeskyttelsesforordningen § 28, stk. 3*)
9. Databehandleren skal bistå den dataansvarlige med at overholde artikel 32-36, dvs. behandlingssikkerhed, anmeldelse og underretning ved brud på persondatasikkerheden samt konsekvensanalyser og forudgående

høring. Aftalen bør fastsætte konkrete frister for underretning ved brud, så den dataansvarliges 72-timers frist kan overholdes. (*Databeskyttelsesforordningen § 28, stk. 3*)

10. Det skal fremgå, at databehandleren efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger, når tjenesterne ophører, og sletter eksisterende kopier – medmindre EU-ret eller national ret kræver fortsat opbevaring. Format og frist for tilbagelevering bør aftales konkret. (*Databeskyttelsesforordningen § 28, stk. 3*)
11. Databehandleren skal stille alle oplysninger til rådighed, der er nødvendige for at påvise overholdelse af artikel 28, og give mulighed for og bidrage til revisioner og inspektioner udført af den dataansvarlige eller en bemyndiget revisor. Aftalen bør fastlægge tilsynsform og -frekvens (fx årlig ISAE 3000-erklæring) ud fra en risikovurdering. (*Databeskyttelsesforordningen § 28, stk. 3*)
12. Sker der overførsel til tredjelande – også som følge af underdatabehandlere eller en klausul om efterlevelse af udenlandske myndighedskrav – skal aftalen både indeholde instruksene herom og et gyldigt overførselsgrundlag efter forordningens kapitel V, typisk Kommissionens standardkontraktbestemmelser eller en tilstrækkelighedsafgørelse. (*Databeskyttelsesforordningen § 46, stk. 2*)
13. Aftalen bør herudover regulere de kommercielle og praktiske forhold, som forordningen ikke kræver: kontaktpunkter hos begge parter, vederlag for bistand og audits, ikrafttræden og ophør sammen med hovedkontrakten, misligholdelsesbeføjelser samt ansvars- og regresfordeling mellem parterne.

LOV

Databeskyttelsesforordningen § 28, stk. 2, 3, 4, 9

Databeskyttelsesforordningen § 32, stk. 1

Databeskyttelsesforordningen § 46, stk. 2

§ 3 Dataansvarlig, databehandler eller fælles dataansvarlig?

Alt afhænger af rollefordelingen, og den afgøres ikke af kontraktens overskrift, men af hvem der reelt bestemmer **formålet** med og de væsentligste **hjælpemidler** til behandlingen. Efter [databeskyttelsesforordningen artikel 4, nr. 7](#) er den dataansvarlige den, der alene eller sammen med andre afgør formål og hjælpemidler, mens databehandleren efter [artikel 4, nr. 8](#) alene behandler oplysningerne på den dataansvarliges vegne.

Datatilsynet har trukket grænsen skarpt op i en række vejledende udtalelser. I sagen om outsourcing af interne whistleblowerordninger (j.nr. 2021-211-6947) opstillede tilsynet tre scenarier: leverer tredjeparten alene en it-plattform, som arbejdsgiverens egne medarbejdere bruger, foreligger der utvivlsomt en databehandlerkonstruktion. Har leverandøren derimod skønsmæssige beføjelser til selv at vurdere, sortere eller afvise indberetninger, agerer parterne som udgangspunkt som **selvstændige dataansvarlige** – og det er ikke afgørende, at arbejdsgiveren har "igangsat" behandlingen ved at tilkøbe en ydelse. Samme logik forklarer, hvorfor revisor, advokat og eksterne rådgivere med eget fagligt ansvar normalt ikke er databehandlere.

Grænsen kan også gå den anden vej: i j.nr. 2022-212-3470 fastslog Datatilsynet, at en leverandør af ren colocation – plads i et serverskab, strøm, køling og netværk – **ikke** er databehandler, fordi ydelsen ikke består i behandling af personoplysninger. Databehandlerstatus indtræder først, hvis leverandøren får adgang til oplysningerne, håndterer hardware med indblik i data, eller leverer tillægsydelser som backup, firewall eller redundans. For netop de tillægsydelser skal der så indgås en databehandlersaftale.

Er rollen derimod delt – to parter fastlægger i fællesskab formål og hjælpemidler – gælder [artikel 26](#) om fælles dataansvar. Så skal der laves en *ordning* mellem parterne, der gennemsigtigt fastlægger deres respektive

ansvar, navnlig for de registreredes rettigheder og oplysningspligten, og ordningens væsentligste indhold skal gøres tilgængeligt for de registrerede. Det er en anden aftaletype end databehandleraftalen og kan ikke erstatte den. Datatilsynet påpegede i tilsynet med Varde Kommune (j.nr. 2018-423-0018), at begrebet fælles dataansvar retter sig mod eksterne juridiske enheder – interne ansvarsdelegeringer i egen organisation er ikke fælles dataansvar, og at kunne skelne mellem databehandlere og selvstændige dataansvarlige er samtidig en forudsætning for en korrekt artikel 30-fortegnelse.

LOV	Databeskyttelsesforordningen § 4	Databeskyttelsesforordningen § 26, stk. 1
	Databeskyttelsesforordningen § 28, stk. 1	Databeskyttelsesforordningen § 30, stk. 1
PRAKSIS	Datatilsynet · Vurdering af databehandlerstatus for leverandører af colocation-ydelser 17.03.2023 Datatilsynet · Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning? 13.10.2021 Datatilsynet · Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter 10.08.2020	

§ 4 Instruksen er aftalens kerne – og databehandlerens grænse

Alle otte krav i art. 28, stk. 3, litra a-h kredser om samme grundtanke: databehandleren behandler aldrig oplysninger til egne formål. Det udtrykkes både i [artikel 28, stk. 3, litra a](#) om dokumenteret instruks og i [artikel 29](#), hvorefter databehandleren og enhver, der udfører arbejde for parterne, kun må behandle oplysningerne efter instruks fra den dataansvarlige.

En instruks, der blot henviser til sig selv, er ubrugelig. Den skal beskrive, hvilke behandlinger leverandøren må foretage, i hvilke systemer, hvilke oplysningstyper der er omfattet, hvor længe, og hvad der udtrykkeligt ikke er tilladt. Modstykket er databehandlerens pligt efter art. 28, stk. 3, sidste afsnit til **omgående** at underrette den dataansvarlige, hvis en instruks efter databehandlerens opfattelse strider mod forordningen – en sikkerhedsventil, der kun virker, hvis instruksen er tilstrækkelig konkret til, at den kan vurderes.

Sanktionen for at gå uden for instruksen er indbygget i forordningen selv: overtræder databehandleren reglerne ved at fastlægge formålene med og hjælpemidlerne til behandlingen, anses vedkommende efter [artikel 28, stk. 10](#) for dataansvarlig for den pågældende behandling – med krav om selvstændigt behandlingsgrundlag, oplysningspligt og fuldt ansvar. Datatilsynet udtalte i j.nr. 2019-442-3996 alvorlig kritik af netop en databehandler, der behandlede personoplysninger uden for instruksen.

Instruksen dækker også sikkerheden. I Schultz-sagen (j.nr. 2019-431-0048) blev en sikkerhedskomponent i et kommunalt fagsystem deaktiveret under en opdatering og aldrig genaktiveret, hvorved medarbejdere i flere kommuner fik adgang til oplysninger om ca. 1,5 mio. borgere. Datatilsynet udtalte kritik direkte efter [artikel 28, stk. 3, litra f](#), jf. [artikel 32](#), fordi databehandleren ikke havde procedurer for at kontrollere ændringer. Tilsvarende fik KMD alvorlig kritik i j.nr. 2021-431-0126 for manglende end-to-end-test af en snitflade, hvor kommunerne netop havde en berettiget forventning baseret på databehandleraftalen. Bistandsforpligtelsen efter litra f rækker desuden ind i brudhåndteringen: databehandleren skal efter [artikel 33, stk. 2](#) underrette den dataansvarlige uden unødigt forsinkelse, og aftalen bør derfor sætte en konkret frist, så den dataansvarliges 72-timers frist kan overholdes.

LOV	Databeskyttelsesforordningen § 28, stk. 3, 10	Databeskyttelsesforordningen § 29
	Databeskyttelsesforordningen § 32, stk. 1	Databeskyttelsesforordningen § 33, stk. 2

PRAKSIS

Datatilsynet · Alvorlig kritik af virksomhed for utilstrækkelig sikkerhed omkring børns personoplysninger	25.08.2022
Datatilsynet · Kritik af Schultz efter sikkerhedshul i fagsystemet Expose	22.09.2020
Datatilsynet · Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	19.12.2019

§ 5 Underdatabehandlere: kæden af aftaler må ikke sænke beskyttelsen

Næsten alle moderne it-leverancer hviler på underleverandører, og forordningen følger kæden hele vejen ned. Efter [artikel 28, stk. 2](#) må databehandleren ikke anvende en anden databehandler uden forudgående **specifik eller generel skriftlig godkendelse**, og ved generel godkendelse skal databehandleren underrette om planlagte tilføjelser eller udskiftninger, så den dataansvarlige kan gøre indsigelse. Efter [artikel 28, stk. 4](#) skal underdatabehandleren pålægges de samme forpligtelser, og den oprindelige databehandler forbliver fuldt ansvarlig over for den dataansvarlige, hvis underleddet svigter.

Datatilsynet har udtalt, at forordningen ikke kræver, at samtlige underdatabehandlere står i selve aftaledokumentet – listen kan ligge i et tillæg – men at listen skal være retvisende, vedvarende tilgængelig og løbende ajourført. En "flydende" liste, som leverandøren ændrer uden at inddrage den dataansvarlige, vil normalt ikke være i overensstemmelse med reglerne, netop fordi den udhuler godkendelses- og indsigelsesretten. Grundtanken er, at de registreredes beskyttelse ikke må sænkes, blot fordi behandlingen overlades videre i kæden, og at resultaterne af leverandørens screening af underdatabehandlere skal kunne udleveres til den dataansvarlige.

Hvad der sker, når kæden ikke fungerer, illustreres af j.nr. 2022-431-0167, hvor Datatilsynet udtalte alvorlig kritik af en underdatabehandler, der nægtede at udlevere oplysninger til den dataansvarlige. Uden en aftale, der viderefører oplysnings- og auditforpligtelserne, står den dataansvarlige uden reel adgang til at kontrollere, hvordan oplysningerne behandles i sidste led – og kan dermed ikke løfte sin ansvarlighedsforpligtelse.

En ofte overset detalje: også databehandleren har selvstændige forpligtelser, som aftalen ikke kan fritage for. Databehandleren skal efter [artikel 30, stk. 2](#) føre sin egen fortegnelse over de kategorier af behandlinger, der foretages på vegne af hver enkelt dataansvarlig, herunder over tredjelandsoverførsler og de generelle sikkerhedsforanstaltninger.

LOV	Databeskyttelsesforordningen § 28, stk. 2, 4	Databeskyttelsesforordningen § 30, stk. 2
PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandlersaftaler	23.01.2026
	Datatilsynet · Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	07.02.2022

§ 6 Tredjelandsoverførsler – databehandlersaftalen er ikke i sig selv et overførselsgrundlag

Ligger databehandleren eller en underdatabehandler uden for EU/EØS, eller kan data tilgås derfra, gælder forordningens kapitel V oveni art. 28. Efter [artikel 44](#) må overførsel kun ske, hvis kapitlets betingelser er opfyldt, og beskyttelsesniveauet ikke undermineres. Grundlaget kan være en tilstrækkelighedsafgørelse efter [artikel 45](#) eller fornødne garantier efter [artikel 46, stk. 2, litra c](#) – Kommissionens standardkontraktbestemmelser (SCC'er).

De to regelsæt må ikke forveksles. I sagen om Aarhus Universitet (j.nr. 2023-421-0001) havde universitetet anvendt SCC'er over for en australsk databehandler uden en særskilt databehandleraftale. Datatilsynet fastslog, at det ikke er tilstrækkeligt alene at etablere et overførselsgrundlag: der skal også foreligge et retligt bindende dokument, der indholdsmæssigt opfylder minimumskraverne i art. 28, stk. 3. Tilsynet accepterede udtrykkeligt, at man samler det i **ét** dokument – men så skal dokumentet dække begge sæt krav, og standardbestemmelserne må ikke ændres i strid med deres indhold, da de derved bliver en ad hoc-aftale, der kræver Datatilsynets godkendelse.

Den praktisk farligste bestemmelse er den lille klausul om efterlevelse af udenlandsk lovgivning. I KOMBIT/AWS-sagen (j.nr. 2022-212-3529) indeholdt databehandleraftalen et vilkår om, at leverandøren kunne flytte data ud af den valgte region, hvis det var nødvendigt for at overholde "the law or binding order of a governmental body". Datatilsynet fandt, at der var tale om en **tilsigtet** overførsel for kommunernes vedkommende, netop fordi instruksens ikke var geografisk afgrænset – og at en tredjelandsmyndigheds anmodning ikke i sig selv udgør et overførselsgrundlag, medmindre den hviler på en international aftale, jf. [artikel 48](#). Datatilsynet har senest i j.nr. 2025-211-3556 taget stilling til rækkevidden af sådanne generelle tilladelser til tredjelandsoverførsler i databehandleraftaler.

Endelig kan cloudleverandørens egen brug af data give problemer, som databehandleraftalen ikke løser. I vurderingen af Region Syddanmarks påtænkte migrering til Microsoft 365 (j.nr. 2023-431-0012) understregede Datatilsynet, at en standardløsning eller markedsposition ikke fritager den dataansvarlige for at påvise lovlighed efter [artikel 5, stk. 2](#), og at der skal kortlægges, om leverandøren behandler oplysninger til **egne** formål – for i så fald er der tale om videregivelse, der kræver selvstændigt behandlingsgrundlag, og ikke om databehandling.

LOV	Databeskyttelsesforordningen § 28, stk. 3	Databeskyttelsesforordningen § 44
	Databeskyttelsesforordningen § 45, stk. 1	Databeskyttelsesforordningen § 46, stk. 2
PRAKSIS	Datatilsynet · Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	23.01.2026
	Datatilsynet · Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter	22.05.2024
	Datatilsynet · Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger	15.02.2024
	Datatilsynet · Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	29.03.2022

Aftalen er ikke nok – tilsynspligten, sanktioner og erstatningsansvaret

Den enkeltstående mest gentagne udtalelse i Datatilsynets praksis er, at den dataansvarlige **ikke** kan løfte ansvarlighedsprincippet ved blot at indgå en databehandleraftale. Kravet følger af [artikel 5, stk. 2](#) og [artikel 24, stk. 1](#) sammenholdt med [artikel 28, stk. 1](#), hvorefter man udelukkende må benytte databehandlere, der kan stille de fornødne garantier. Den dataansvarlige må derfor føre et større eller mindre tilsyn med, at aftalen faktisk overholdes, og – som Datatilsynet formulerede det i tilsynet med Hjemrejsestyrelsen (j.nr. 2021-421-0101) – jo større risici for de registrerede, jo større krav til tilsynets form og hyppighed.

Praksis viser en tydelig linje. Randers Kommune fik alvorlig kritik for mangelfuld styring af databehandlere (j.nr. 2018-423-0021). Region Hovedstaden (j.nr. 2020-422-0025) og Region Syddanmark (j.nr. 2020-422-0026) fik

kritik for slet ikke at have taget stilling til tilsynsniveauet eller for ikke at gennemføre det årlige tilsyn, deres egne retningslinjer krævede. Aarhus Universitet (j.nr. 2023-421-0001) og Styrelsen for International Rekruttering og Integration (j.nr. 2021-421-0102) fik kritik for manglende tilsyn. Omvendt slap Beskæftigelsesministeriet (j.nr. 2021-421-0097), Skatteforvaltningen (j.nr. 2021-421-0099), Sundhedsdatastyrelsen (j.nr. 2021-421-0100) og Hjemrejsestyrelsen (j.nr. 2021-421-0101) for kritik, fordi de kunne dokumentere en risikobaseret og faktisk gennemført tilsynsmodel. Konklusionen er praktisk: fastsæt tilsynsniveauet i selve aftalen, vælg et koncept (fx årlig ISAE 3000-revisionserklæring, certificering eller egen kontrol), og gem dokumentationen.

Sanktionsmæssigt hører overtrædelse af art. 28 til det lavere bødeloft i [artikel 83, stk. 4](#) – op til 10 mio. EUR eller 2 % af den samlede globale årlige omsætning, alt efter hvad der er højest. Danmark har ikke administrative bøder: Datatilsynet politianmelder og indstiller til bøde, og overtrædelse af den dataansvarliges og databehandlers forpligtelser efter forordningens artikel 25-39 – herunder art. 28 – straffes efter [databeskyttelsesloven § 41, stk. 1, nr. 1](#) med bøde eller fængsel indtil 6 måneder. Kriterierne i art. 83, stk. 2 skal følges ved strafudmålingen, jf. [§ 41, stk. 3](#), sager kan afgøres med bødeforelæg efter [§ 42](#), juridiske personer kan straffes, og offentlige myndigheder er efter [§ 41, stk. 6](#) undtaget fra straffelovens § 27, stk. 2. Forældelsesfristen er 5 år. Praksis for bødeniveauet og de øvrige overtrædelsestyper er samlet i [oversigten over Datatilsynets bødesager](#), og tilsynets afgørelsespraksis i bredere forstand i [oversigten over Datatilsynets afgørelser](#). Anvendes leverandørens løsning til automatiserede eller AI-baserede behandlinger, er der supplerende krav beskrevet i [oversigten om AI-systemer og GDPR](#).

Oveni straffen kommer det civilretlige: efter [artikel 82](#) har enhver, der har lidt materiel eller immateriel skade, ret til erstatning fra den dataansvarlige eller databehandleren, og er begge involveret i samme behandling, hæfter de **solidarisk** for hele skaden. Databehandleren hæfter navnlig, hvis vedkommende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser – endnu en grund til, at instruksen skal være skrevet ned og præcis.

LOV

[Databeskyttelsesforordningen § 5, stk. 2](#)
[Databeskyttelsesforordningen § 24, stk. 1](#)
[Databeskyttelsesforordningen § 82, stk. 2](#)
[Databeskyttelsesforordningen § 83, stk. 4](#)
[Databeskyttelsesloven § 41, stk. 1](#)
[Databeskyttelsesloven § 42](#)

PRAKSIS

Datatilsynet · Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter 22.05.2024

Datatilsynet · Kritik af Styrelsen for International Rekruttering og Integrations manglende tilsyn med databehandlere 16.12.2022

Datatilsynet · Datatilsynets kontrol med Sundhedsdatastyrelsens tilsyn med databehandlere 16.12.2022

Datatilsynet · Datatilsynets tilsyn med Hjemrejsestyrelsens kontrol af databehandlere resulterer i ingen kritik 15.12.2022

Datatilsynet · Beskæftigelsesministeriets tilsyn med databehandler: Datatilsynet udtaler ingen kritik 15.12.2022

Datatilsynet · Skatteforvaltningens tilsyn med databehandlere i overensstemmelse med reglerne 15.12.2022

Datatilsynet · Kritik af Region Syddanmark for mangelfuld kontrol med personoplysninger til forskning 20.07.2022

Datatilsynet · Kritik af Region Hovedstaden for manglende databehandleraftale og kontrol med underdatabehandlere i forskningsprojekt 16.02.2022

Datatilsynet · Alvorlig kritik af Randers Kommunes mangelfulde styring af databehandlere 05.08.2019

§ 8 Typiske faldgruber

Databehandleraftale med en, der slet ikke er databehandler. Revisor, advokat, ekstern rådgiver og typisk også rekrutteringsbureauer og whistleblower-administratorer med selvstændige vurderingsbeføjelser er som hovedregel **selvstændigt dataansvarlige** – de fastlægger selv formålet med deres behandling og bærer eget fagligt ansvar. Datatilsynet fastslog i j.nr. 2021-211-6947 om outsourcing af whistleblowerordninger, at parterne som udgangspunkt hver især agerer som selvstændige dataansvarlige, når leverandøren har skønsmæssige beføjelser. En databehandleraftale i den situation giver falsk tryghed: den dokumenterer en instruksbeføjelse, du ikke har, og skjuler at der reelt sker en videregivelse, som kræver selvstændig hjemmel.

Aftalen indgås først efter, at behandlingen er gået i gang. Kravet i art. 28, stk. 3 er en forudsætning for overhovedet at måtte overlade oplysningerne – ikke en efterfølgende dokumentationsøvelse. I Datatilsynets tilsyn med Region Hovedstadens forskningsprojekter (j.nr. 2020-422-0025) blev det konstateret, at databehandleraftalen med et udenlandsk center først blev indgået længe efter, at centret var inkluderet i projektet. Perioden uden aftale kan ikke repareres bagudrettet og udgør en selvstændig overtrædelse.

Leverandørens standardaftale accepteres ukritisk. Store cloud- og SaaS-leverandører leverer standardvilkår med ensidig ændringsret, brede formålsbeskrivelser og "flydende" underdatabehandlerlister. Datatilsynet har udtalt, at en liste over underdatabehandlere, som leverandøren kan ændre uden løbende inddragelse af den dataansvarlige, normalt **ikke** vil være i overensstemmelse med reglerne, fordi det udhuler godkendelses- og indsigelsesretten i [artikel 28, stk. 2](#). Ansvar for at aftalen lever op til kravene ligger hos dig som dataansvarlig – også når leverandøren er markedsdominerende.

SCC'er bruges som erstatning for databehandleraftalen. Kommissionens standardkontraktbestemmelser er et *overførselsgrundlag* efter kapitel V – ikke en databehandleraftale. I Datatilsynets afgørelse om Aarhus Universitet (j.nr. 2023-421-0001) havde universitetet anvendt SCC'er over for en australsk databehandler uden at indgå en databehandleraftale, og tilsynet fastslog, at det ikke er tilstrækkeligt alene at etablere et overførselsgrundlag. De to sæt krav må gerne samles i ét dokument, men så skal dokumentet dække både overførselsgrundlaget og alle minimumskrav i art. 28, stk. 3 – og standardbestemmelserne må ikke ændres i strid med deres indhold, da de ellers bliver en ad hoc-aftale, der kræver Datatilsynets godkendelse.

Aftalen indgås – men der føres aldrig tilsyn. Dette er den hyppigste overtrædelse i Datatilsynets praksis. Tilsynet har gentagne gange udtalt, at den dataansvarlige **ikke** kan leve op til ansvarlighedsprincippet blot ved at indgå en databehandleraftale, men også må føre et større eller mindre tilsyn med, at aftalen faktisk overholdes. Randers Kommune fik alvorlig kritik (j.nr. 2018-423-0021) for mangelfuld styring af databehandlere, og både Region Hovedstaden, Region Syddanmark, Aarhus Universitet og Styrelsen for International Rekruttering og Integration har fået kritik for enten slet ikke at have fastsat et tilsynsniveau eller for ikke at have gennemført det tilsyn, de selv havde besluttet.

Instruksen er tom – og databehandleren bliver dataansvarlig. Skriver aftalen kun, at "databehandleren behandler oplysninger efter den dataansvarliges instruks", uden at instruksen nogensinde konkretiseres, er der ingen ramme at måle leverandøren imod. Behandler databehandleren derefter oplysninger til egne formål – analyse, produktudvikling, statistik, videresalg – anses vedkommende efter [artikel 28, stk. 10](#) selv for dataansvarlig for den behandling. Datatilsynet udtalte alvorlig kritik i j.nr. 2019-442-3996 netop af en databehandler, der behandlede personoplysninger uden for instruksen.

Tredjelandsklausulen i det små overses. Mange cloudaftaler indeholder en klausul om, at leverandøren kan flytte eller udlevere data uden for den valgte region, hvis det er nødvendigt for at overholde lovgivning eller bindende myndighedsafgørelser. Datatilsynet fastslog i KOMBIT/AWS-sagen (j.nr. 2022-212-3529), at en sådan geografisk ubegrænset instruks gør en eventuel udlevering til en **tilsigtet** overførsel, som udløser

kapitel V-kravene for den dataansvarlige – og at en tredjelandsmyndigheds anmodning ikke i sig selv er et overførselsgrundlag. Overses klausulen, mangler der et overførselsgrundlag, og det rammer det høje bødeloft i [artikel 83, stk. 5](#).

Ingen exitplan – data efterlades hos leverandøren. Art. 28, stk. 3, litra g kræver, at databehandleren efter dit valg sletter eller tilbageleverer alle oplysninger og sletter kopier ved ophør. Er format, frist og dokumentation for sletningen ikke aftalt på forhånd, står man ved leverandørskifte typisk uden reel mulighed for at få data ud i brugbar form – og uden dokumentation for, at backup og testmiljøer er ryddet. Fortsat opbevaring uden formål er samtidig en selvstændig overtrædelse af opbevaringsbegrænsningen i [artikel 5, stk. 1, litra e](#).

§ 9 Relaterede dokumenter

- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn
- [Konsekvensanalyse \(DPIA\)](#) – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet
- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Samtykkeerklæring \(GDPR\)](#) – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)
- [IT-kontrakt \(systemleverance/SaaS\)](#) – Kontrakten om softwareleverancer og cloud-drift – K-standarderne, agile leverancer, SLA'er og exit
- [Fortrolighedsaftale \(NDA\)](#) – Hemmeligholdelsesaftalen før forhandlinger og samarbejder – og dens samspil med forretningshemmelighedsloven
- [Whistleblowerpolitik og -ordning](#) – Den lovpligtige interne indberetningsordning for arbejdsgivere med 50+ ansatte – etablering, procedurer og fortrolighed

REFERENCE Lovgrundlag

7 paragraffer

Databeskyttelsesforordningen § 5	stk. 2	Databeskyttelsesforordningen § 26	stk. 1
Databeskyttelsesforordningen § 28	stk. 2, 3	Databeskyttelsesforordningen § 32	stk. 1
Databeskyttelsesforordningen § 46	stk. 2	Databeskyttelsesloven § 41	stk. 1
Retshåndhævelsesloven § 22	stk. 2		

MATERIALE Citerede afgørelser

19 afgørelser

23.01.2026	Datatilsynets vurdering af generelle tilladelser til tredjelandsoverførsler i databehandleraftaler	2025-211-3556
22.05.2024	Aarhus Universitet får kritik for mangelfuld håndtering af personoplysninger i tre forskningsprojekter	2023-421-0001
15.02.2024	Region Syddanmarks brug af Microsoft 365: Datatilsynets vurdering af rammerne for cloud-løsninger	2023-431-0012
17.03.2023	Vurdering af databehandlerstatus for leverandører af colocation-ydelser	2022-212-3470
16.12.2022	Datatilsynets kontrol med Sundhedsdatastyrelsens tilsyn med databehandlere	2021-421-0100
16.12.2022	Kritik af Styrelsen for International Rekruttering og Integrations manglende tilsyn med databehandlere	2021-421-0102
15.12.2022	Beskæftigelsesministeriets tilsyn med databehandler: Datatilsynet udtaler ingen kritik	2021-421-0097
15.12.2022	Skatteforvaltningens tilsyn med databehandlere i overensstemmelse med reglerne	2021-421-0099
15.12.2022	Datatilsynets tilsyn med Hjemrejsestyrelsens kontrol af databehandlere resulterer i ingen kritik	2021-421-0101
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
29.03.2022	Datatilsynets afklaring af utilsigtede overførsler og teknisk routing til tredjelande	2022-212-3529
16.02.2022	Kritik af Region Hovedstaden for manglende databehandleraftale og kontrol med underdatabehandlere i forskningsprojekt	2020-422-0025
07.02.2022	Alvorlig kritik af underdatabehandlers nægtelse af at udlevere oplysninger til dataansvarlig	2022-431-0167
13.10.2021	Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning?	2021-211-6947
22.09.2020	Kritik af Schultz efter sikkerhedshul i fagsystemet Expose	2019-431-0048
10.08.2020	Tilsyn med Varde Kommunes fortegnelser over behandlingsaktiviteter	2018-423-0018
19.12.2019	Alvorlig kritik af databehandler for behandling af personoplysninger uden for instruks	2019-442-3996
05.08.2019	Alvorlig kritik af Randers Kommunes mangelfulde styring af databehandlere	2018-423-0021

03

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Konsekvensanalyse (DPIA)

Databeskyttelseskonsekvensanalyse efter GDPR art. 35 – hvornår pligten udløses, mindstekravene til indholdet og forhåndshøring af Datatilsynet efter art. 36

Version 1 · Opdateret 21. jul. 2026 · 14 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

En **konsekvensanalyse vedrørende databeskyttelse** (DPIA – *Data Protection Impact Assessment*) er en struktureret, skriftlig forråndsanalyse af, hvad en planlagt behandling af personoplysninger gør ved menneskers rettigheder, og hvad man konkret gør for at nedbringe risikoen. Den er hverken en it-sikkerhedsrapport, en fortegnelse over behandlingsaktiviteter eller en privatlivspolitik: den er den proces, hvor man – inden systemet tændes – beskriver behandlingen, prøver nødvendigheden, sætter tal og ord på risikoen for de registrerede og beslutter, hvilke foranstaltninger der skal bygges ind.

Parterne er få og deres roller er skarpt fordelt. **Den dataansvarlige** ejer analysen, træffer beslutningerne og bærer ansvaret – pligten kan ikke outsources til leverandøren. **Databeskyttelsesrådgiveren (DPO)** skal rådføres og rådgive, men overtager ikke ansvaret. **Databehandleren/leverandøren** skal bistå med oplysninger og dokumentation. **Datatilsynet** er modtager, hvis restrisikoen fortsat er høj – så skal tilsynet høres, før behandlingen starter. Og **de registrerede** (eller deres repræsentanter, fx tillidsrepræsentanter) skal efter omstændighederne høres om den planlagte behandling.

Oversigten er ordnet efter dokumentets naturlige livscyklus: først hvornår pligten udløses (og hvornår den ikke gør), dernæst checklisten over det obligatoriske indhold med hjemmel punkt for punkt, så de typiske fejl med deres konsekvenser – og til sidst uddybende afsnit om tærskelvurderingen, rollefordelingen, metoden frem mod forhåndshøring, håndhævelsen i dansk praksis og samspillet med AI-forordningens konsekvensanalyse for grundlæggende rettigheder.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** DPIA er en **betinget** pligt, der udløses af behandlingens risikoprofil – ikke af virksomhedens størrelse. En lille klinik med biometrisk adgangskontrol kan have pligten, mens en stor koncern med almindelig lønadministration ikke har den.
- 02** Tre behandlingstyper er altid omfattet (profilering med retsvirkning, følsomme oplysninger i stort omfang og systematisk overvågning af offentligt tilgængeligt område), jf. art. 35, stk. 3 – suppleret af Datatilsynets offentliggjorte liste efter art. 35, stk. 4.
- 03** Analysen skal være **færdig, før behandlingen påbegyndes**. Datatilsynet har både politianmeldt og nedlagt forbud, hvor en konsekvensanalyse først blev færdiggjort efter, at behandlingen var sat i gang.

- 04** Art. 35, stk. 7, opstiller fire ufravigelige mindstekrav – beskrivelse, nødvendigheds- og proportionalitetsvurdering, risikovurdering og afhjælpende foranstaltninger. En it-sikkerhedsrisikovurdering efter art. 32 er ikke i sig selv en konsekvensanalyse.
- 05** Databeskyttelsesrådgiveren **skal** rådføres, når der laves DPIA (art. 35, stk. 2), og rådgivningen indgår i DPO'ens lovbestemte opgaver efter art. 39, stk. 1, litra c – men ansvaret bliver hos den dataansvarlige.
- 06** Er restrisikoen fortsat høj efter de planlagte foranstaltninger, er behandlingen **spærret**, indtil Datatilsynet er hørt efter art. 36 – høringen er en retssikkerhedsgaranti, ikke en godkendelsesstempling.
- 07** Manglende eller mangelfuld DPIA er strafbelagt i Danmark efter [databeskyttelseslovens § 41, stk. 1, nr. 1](#) (bøde eller fængsel indtil 6 måneder), og ligger i GDPR's høje bødeleje på 10 mio. EUR eller 2 % af global omsætning.
- 08** Én analyse kan dække flere lignende behandlinger – Datatilsynet har fx opfordret kommunerne til at udarbejde en **fælles** konsekvensanalyse for AULA i stedet for 98 enkeltstående.

§ 1 Hvornår er dokumentet påkrævet?

Betinget lovpligt – risikoen udløser pligten. En DPIA skal foretages, når en type behandling "sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder", jf. [databeskyttelsesforordningens artikel 35, stk. 1](#). Pligten er altså hverken knyttet til virksomhedens størrelse, omsætning eller antal ansatte, men til behandlingens **karakter, omfang, sammenhæng og formål** – navnlig ved brug af nye teknologier. Analysen skal foreligge **forud for behandlingen**; en enkelt analyse kan dække flere lignende behandlingsaktiviteter med lignende høje risici.

Altid – de tre formodningstilfælde i stk. 3. DPIA er navnlig påkrævet ved (a) systematisk og omfattende vurdering af personlige forhold baseret på automatisk behandling, herunder profilering, som er grundlag for afgørelser med retsvirkning eller tilsvarende betydelig påvirkning, (b) behandling i stort omfang af særlige kategorier af oplysninger efter [artikel 9](#) eller af oplysninger om straffedomme og lovovertrædelser, og (c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Datatilsynets lister. Tilsynsmyndigheden udarbejder og offentliggør efter artikel 35, stk. 4, en liste over behandlingstyper, hvor DPIA altid kræves – Datatilsynet henviser selv til denne liste i sin vejledning. Efter stk. 5 kan der tilsvarende offentliggøres en liste over behandlinger, hvor DPIA ikke kræves. Præambelbetragtning 91 til forordningen peger på de typiske udlødere: omfattende behandling af meget store datamængder, omfattende brug af ny teknologi, profileringsbaserede afgørelser, biometriske og genetiske data, oplysninger om straffedomme samt omfattende overvågning af offentligt tilgængelige områder.

Særligt om høj restrisiko. Viser analysen, at behandlingen fortsat vil føre til høj risiko *i mangel af* foranstaltninger, der begrænser risikoen, må behandlingen ikke sættes i gang: den dataansvarlige skal først høre Datatilsynet efter [artikel 36, stk. 1](#). Tilsynet har op til otte uger – der kan forlænges med seks uger ved kompleks behandling – til at give skriftlig rådgivning og kan undervejs bruge alle sine beføjelser.

Politi, anklagemyndighed og kriminalforsorg. Uden for GDPR's område gælder en parallel – og på ét punkt strengere – ordning: [retshåndhævelseslovens § 25](#) kræver konsekvensanalyse ved høj risiko, og [§ 26](#) kræver

forudgående høring af tilsynsmyndigheden inden behandling i **nye registre**, både når analysen viser høj restrisiko, og når behandlingstypen i sig selv indebærer høj risiko ved brug af nye teknologier, mekanismer eller procedurer.

Undtagelsen for lovregulerede behandlinger. Har en behandling efter artikel 6, stk. 1, litra c eller e, hjemmel i EU-ret eller national ret, som regulerer netop de pågældende behandlingsaktiviteter, og er der allerede foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen af retsgrundlaget, finder artikel 35, stk. 1-7, ikke anvendelse (artikel 35, stk. 10). I dansk lovgivningspraksis kan analysen efter Justitsministeriets *Vejledning om lov kvalitet* foretages i forbindelse med udformningen af et lovforslag eller en bekendtgørelse – men undtagelsen forudsætter, at analysen faktisk er lavet.

Frivilligt, men retssikrende. Er man i tvivl, er den dokumenterede **tærskelvurdering** (screening) den billige forsikring: ansvarlighedsprincippet i [artikel 5, stk. 2](#) kræver, at man kan *påvise* sine overvejelser – også når konklusionen blev, at DPIA ikke var nødvendig. Datatilsynet har i tilsynssager netop forudsat, at myndigheder afdækker, hvilke behandlingsaktiviteter der kræver konsekvensanalyse, og lægger en plan for at gennemføre dem. En frivillig DPIA er desuden ofte det bedste redskab til at dokumentere databeskyttelse gennem design efter [artikel 25](#).

Løbende pligt. DPIA'en er ikke et engangsdokument: den dataansvarlige skal foretage en fornyet gennemgang, i hvert fald når der sker en ændring af den risiko, behandlingsaktiviteterne udgør (artikel 35, stk. 11) – fx ved leverandørskifte, nyt modul, ny datakilde eller tilføjelse af AI-funktionalitet.

§ 2 Det skal dokumentet indeholde

1. En dokumenteret tærskelvurdering af, om behandlingen sandsynligvis indebærer høj risiko – inklusive begrundelsen, hvis konklusionen er, at DPIA ikke er påkrævet. Vurderingen skal kunne fremlægges over for Datatilsynet. (*Databeskyttelsesforordningen § 5, stk. 2*)
2. Analysen skal foreligge færdig forud for behandlingen og skal identificere den behandlingstype, den dækker; én analyse kan omfatte flere lignende behandlingsaktiviteter med lignende høje risici. (*Databeskyttelsesforordningen § 35, stk. 1*)
3. En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen – herunder i givet fald de legitime interesser, den dataansvarlige forfølger. (*Databeskyttelsesforordningen § 35, stk. 7*)
4. En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene – dvs. om formålet kunne nås med færre oplysninger eller mindre indgribende midler. (*Databeskyttelsesforordningen § 35, stk. 7*)
5. En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder, hvor både sandsynlighed og alvor vurderes for hvert risikoscenarie – ikke kun risici for organisationen. (*Databeskyttelsesforordningen § 35, stk. 7*)
6. De foranstaltninger, der påtænkes for at imødegå risiciene, herunder garantier, sikkerhedsforanstaltninger og mekanismer, der kan sikre beskyttelsen og påvise overholdelse – med tydelig sammenhæng mellem den enkelte risiko og den enkelte foranstaltning samt en angivelse af restrisikoen. (*Databeskyttelsesforordningen § 35, stk. 7*)
- 7.

Dokumentation for, at databeskyttelsesrådgiveren er rådført, og hvad rådgivningen gik ud på, hvis en DPO er udpeget. (*Databeskyttelsesforordningen § 35, stk. 2*)

8. En stillingtagen til, om de registreredes eller deres repræsentanters synspunkter skal indhentes om den planlagte behandling – og i givet fald resultatet heraf. (*Databeskyttelsesforordningen § 35, stk. 9*)
9. Inddragelse af eventuelle godkendte adfærdskodekser, der gælder for sektoren, ved vurderingen af behandlingens konsekvenser. (*Databeskyttelsesforordningen § 35, stk. 8*)
10. En udtrykkelig konklusion om, hvorvidt restrisikoen fortsat er høj, og dermed om Datatilsynet skal høres, før behandlingen påbegyndes – samt det materiale, der i så fald skal indgives (ansvarsfordeling, formål og hjælpemidler, foranstaltninger og garantier, DPO'ens kontaktoplysninger og selve konsekvensanalysen). (*Databeskyttelsesforordningen § 36, stk. 3*)
11. En plan for fornyet gennemgang: hvornår og på hvilken foranledning analysen revurderes, herunder i hvert fald ved ændringer i den risiko, behandlingsaktiviteterne udgør. (*Databeskyttelsesforordningen § 35, stk. 11*)
12. Dokumentet bør desuden være dateret og versionsstyret, angive hvem der har udarbejdet og godkendt det på ledelsesniveau, og henvise til den tilhørende artikel 30-fortegnelse og de relevante databehandleraftaler. Det er kutyme, men det er i praksis dét, der gør analysen til brugbar dokumentation.

LOV

Databeskyttelsesforordningen § 5, stk. 2

Databeskyttelsesforordningen § 35, stk. 1, 2, 7, 8, 9, 11

Databeskyttelsesforordningen § 36, stk. 3

§ 3 Tærskelvurderingen: hvornår er risikoen "høj"?

Ordlyden i artikel 35, stk. 1, er en sandsynlighedsvurdering: *vil* behandlingen sandsynligvis indebære en høj risiko? Vurderingen foretages på behandlingstypen – ikke på den enkelte registrerede – og de fire parametre er behandlingens karakter, omfang, sammenhæng og formål, med særlig vægt på brug af nye teknologier.

Ud over de tre formodningstilfælde i stk. 3 og Datatilsynets liste efter stk. 4 giver præambelbetragtning 91 de praktiske pejlemærker: meget store datamængder på regionalt eller nationalt plan, omfattende brug af ny teknologi, afgørelser truffet på grundlag af profilering, biometriske og genetiske data, oplysninger om straffedomme samt omfattende overvågning af offentligt tilgængelige områder. Datatilsynet peger i sin egen vejledning på de samme typer indgribende behandlinger – lokationsdata til kortlægning af personers adfærd, systematisk kontrolovervågning, profilering, automatiske afgørelser og samkøring af datasæt, der giver oplysninger ud over, hvad de registrerede med rimelighed kan forvente – og bemærker udtrykkeligt, at der er sammenfald med DPIA-pligten. De fælleseuropæiske retningslinjer (WP248), som Datatilsynet har lagt til grund i sin praksis, opstiller ni kriterier, og som tommelfingerregel peger to eller flere opfyldte kriterier på, at der skal laves en konsekvensanalyse.

Tærsklen er tydeligt lav på AI-området. I sagen om Uddannelses- og Forskningsstyrelsens AI-løsning til screening af SU-handicaptillæg lagde Datatilsynet vægt på store mængder følsomme data, en sårbar målgruppe og modellens evne til at finde sammenhænge ud over traditionel sagsbehandling – og fastslog, at der skal foretages en konsekvensanalyse efter artikel 35, stk. 1, før driften iværksættes. I sagen om det kommunale profileringsværktøj Asta blev profilering af ledige anset for så indgribende, at der stilles høje krav både til hjemmelsgrundlagets præcision og til beskyttelsesforanstaltningerne. Og da fodboldklubberne fik tilladelse til ansigtsgenkendelse efter [databeskyttelseslovens § 7, stk. 4](#), var det et udtrykkeligt vilkår, at

der skulle foreligge en konsekvensanalyse, der opfylder indholdskravene, før behandlingen måtte påbegyndes. Kontrolforanstaltninger over for medarbejdere – logning, tv-overvågning, GPS – ligger i samme felt; se den nærmere praksis i [oversigten om databeskyttelse i ansættelsesforhold](#).

LOV	Databeskyttelsesforordningen § 35, stk. 3, 4	Databeskyttelsesloven § 7, stk. 4	
PRAKSIS	Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere		16.07.2025
	Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre		03.07.2024
	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger		12.06.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse		30.01.2024
	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta		18.05.2022

§ 4 Hvem gør hvad: dataansvarlig, DPO, leverandør og Datatilsynet

Den dataansvarlige er eneansvarlig for, at analysen bliver lavet, bliver lavet i tide og opfylder mindstekravene. Det er også den dataansvarlige, der træffer beslutningen om at gennemføre foranstaltningerne – og som ifalder ansvaret, hvis de udebliver.

DPO'en skal rådføres, når der foretages en konsekvensanalyse, jf. artikel 35, stk. 2, og det er en af rådgiverens lovbestemte kerneopgaver at rådgive om analysen og overvåge dens opfyldelse, jf. [artikel 39, stk. 1, litra c](#). DPO'en er samtidig tilsynets kontaktpunkt ved forudgående høring. Er der pligt til at have en DPO efter [artikel 37](#) – typisk for offentlige myndigheder og ved kerneaktiviteter med systematisk overvågning eller følsomme oplysninger i stort omfang – er de to pligter i praksis to sider af samme risikoprofil: den, der skal have en DPO, skal som regel også lave DPIA'er.

Databehandleren har ikke selv pligten, men skal efter [artikel 28](#) bistå den dataansvarlige med at overholde artikel 35 og 36 – en pligt, der bør stå eksplicit i databehandleraftalen, og som i statslige delegationsordninger er skrevet direkte ind i cirkulærerne om fælles dataansvar. Bistandspligten fritager ikke for egen stillingtagen: i AULA-tilsynene var det ikke nok at henvise til leverandørens materiale.

Datatilsynet har to roller. Rådgiveren i forhåndshøringen efter artikel 36 – og håndhæveren bagefter. Endelig kan **de registrerede** skulle høres efter artikel 35, stk. 9; på arbejdspladsen sker det naturligt gennem medarbejderrepræsentanter, hvilket AI-forordningen på sit område har gjort til en selvstændig informationspligt.

Husk sammenhængen til de øvrige dokumenter: DPIA'en trækker på [artikel 30](#)-fortegnelsen som datagrundlag, forudsætter gyldige databehandleraftaler for hver leverandør og ender ofte i konkrete ændringer af privatlivspolitikken og af, hvordan et samtykke indhentes.

LOV	Databeskyttelsesforordningen § 35, stk. 2	Databeskyttelsesforordningen § 37, stk. 1	
	Databeskyttelsesforordningen § 39, stk. 1		
PRAKSIS	Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA		23.05.2024
	Datatilsynet · Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA		15.01.2024

§ 5 Metoden: fra beskrivelse til restrisiko og forhåndshøring

Artikel 35, stk. 7, er en minimumsstruktur, ikke en skabelon – men rækkefølgen er logisk og bør følges.

Først beskrives behandlingen systematisk: hvilke oplysninger, om hvem, hvorfra, til hvilke formål, hvor længe, med hvilke systemer og hvilke modtagere, herunder tredjelandsoverførsler. **Dernæst** prøves nødvendigheden og proportionaliteten: kan formålet nås med færre oplysninger, kortere opbevaring, pseudonymisering eller syntetiske data? Denne del er reelt en dokumentation af databeskyttelse gennem design efter artikel 25 og bliver ofte sprunget over. **Så** vurderes risikoen for de registrerede – scenarie for scenarie, med sandsynlighed og alvor, set fra borgerens synsvinkel og ikke fra organisationens. **Endelig** kobles hver risiko til de foranstaltninger, der skal nedbringe den, og restrisikoen efter foranstaltningerne opgøres.

Det er netop den sidste kobling, Datatilsynet efterprøver. I AULA-sagen mod Københavns Kommune anbefalede tilsynet, at risikovurderingerne struktureres, så de kan sammenlignes før og efter implementering af foranstaltningerne, og så sammenhængen mellem foranstaltninger og de enkelte risici fremgår tydeligt – kommunen havde ikke fuldt ud godtgjort, at der var implementeret passende foranstaltninger mod alle identificerede risici.

Er restrisikoen fortsat høj, indtræder høringspligten. Til Datatilsynet indgives efter artikel 36, stk. 3, ansvarsfordelingen mellem dataansvarlige, fælles dataansvarlige og databehandlere, den planlagte behandlingsformål og hjælpemidler, foranstaltninger og garantier, DPO'ens kontaktoplysninger, selve konsekvensanalysen og de yderligere oplysninger, tilsynet beder om. Tilsynet svarer inden for otte uger, der kan forlænges med seks; fristerne kan suspenderes, mens tilsynet afventer supplerende oplysninger. Sagen mod Nationalt Genom Center viser konsekvensen af at springe trinnet over: centret indsendte selv en konsekvensanalyse, der viste høj risiko og oplyste, at behandlingen allerede var i gang – tilsynet nedlagde midlertidigt forbud mod yderligere indsamling og endte med bødeindstilling og forbud mod andre formål end klinisk diagnostik, indtil en tilstrækkelig analyse forelå.

Er risikoen omvendt nedbragt til et acceptabelt niveau, er der ingen høringspligt – men analysen skal gemmes som dokumentation og revurderes ved ændringer.

LOV

Databeskyttelsesforordningen § 25, stk. 1

Databeskyttelsesforordningen § 35, stk. 7

Databeskyttelsesforordningen § 36, stk. 3

PRAKSIS **Datatilsynet** · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024

Datatilsynet · Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling 25.03.2022

§ 6 Håndhævelsen: hvad det koster at springe analysen over

Danmark har ikke administrative bøder på databeskyttelsesområdet. Datatilsynet udtaler kritik eller alvorlig kritik, meddeler påbud og forbud – og politianmelder med en bødeindstilling, hvorefter bøden pålægges af domstolene. Hjemlen er [databeskyttelseslovens § 41](#), hvis stk. 1, nr. 1, netop kriminaliserer overtrædelse af den dataansvarliges og databehandlerens forpligtelser efter forordningens artikel 25-39 – dvs. både artikel 35 og artikel 36 – med bøde eller fængsel indtil 6 måneder. Bødeniveauet fastlægges efter kriterierne i [artikel 83, stk. 4](#), hvor rammen er 10 mio. EUR eller 2 % af den samlede globale årlige omsætning, og efter forordningens artikel 83, stk. 2, om overtrædelsens karakter, alvor og varighed. Også offentlige myndigheder kan straffes, jf. § 41, stk.

6 – bøden til Nationalt Genom Center blev fastsat under hensyn til de budgetmæssige rammer for offentlige myndigheder.

De to tungeste danske eksempler handler begge om konsekvensanalyse. Nationalt Genom Center blev indstillet til en bøde på 600.000 kr. og fik forbud mod behandling, fordi behandlingen af genetiske data var påbegyndt uden en fyldestgørende analyse og uden forudgående høring. Netcompany blev efter sikkerhedsbruddet på mit.dk politianmeldt og indstillet til den hidtil største danske bøde på 15 mio. kr., hvor det indgik, at der ikke var udarbejdet en konsekvensanalyse, selv om platformens formål, omfang og datakarakter indebar høj risiko. Tilsynet formulerede pointen skarpt: udarbejdelse af en konsekvensanalyse er ikke en formalitet, men en væsentlig retssikkerhedsgaranti, og analysen skal være lavet, inden behandlingen går i gang.

I tilsynssporet er reaktionen typisk alvorlig kritik og påbud: AULA-tilsynene med kommunerne endte med kritik og påbud for mangelfuld behandlingssikkerhed og manglende eller utilstrækkelige konsekvensanalyser – bl.a. over for Frederikshavn, Lolland, Esbjerg og Københavns Kommune. Datatilsynet anbefalede samtidig, at kommunerne udarbejder en **fælles** konsekvensanalyse for AULA, da behandlingsaktiviteterne er ens og indebærer lignende høje risici. Beslægtede sager om manglende risikovurdering før videregivelse og om utilstrækkelig test før idriftsættelse af Digital Post viser samme linje: risikoarbejdet skal ligge før driften. En bredere gennemgang findes i [oversigten over Datatilsynets afgørelser](#).

LOV	Databeskyttelsesforordningen § 83, stk. 4	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Datatilsynet · Alvorlig kritik til Digitaliseringsstyrelsen for utilstrækkelig sikkerhed ved brug af personoplysninger i testmiljøer	24.06.2025
	Datatilsynet · Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA	15.01.2024
	Datatilsynet · Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	12.01.2024
	Datatilsynet · Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	22.12.2023
	Datatilsynet · Alvorlig kritik og påbud til Lolland Kommune for mangelfuld behandlingssikkerhed og manglende konsekvensanalyser	22.12.2023
	Datatilsynet · Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	22.12.2023
	Datatilsynet · Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling	25.03.2022
	Datatilsynet · Alvorlig kritik af manglende risikovurdering ved videregivelse af personoplysninger	05.03.2020

§ 7 DPIA og AI-forordningens konsekvensanalyse for grundlæggende rettigheder (FRIA)

Fra den 2. august 2026 finder AI-forordningen anvendelse, jf. [artikel 113](#) (forpligtelserne knyttet til artikel 6, stk. 1, dog først fra 2. august 2027). Den introducerer et nyt dokument ved siden af DPIA'en: **konsekvensanalysen vedrørende grundlæggende rettigheder** (FRIA) i [AI-forordningens artikel 27](#). Pligten rammer idriftsættere, der er offentligretlige organer eller private enheder, som leverer offentlige tjenester, samt idriftsættere af højrisikosystemer til kreditvurdering og risikovurdering/prisfastsættelse i livs- og sygeforsikring – og den skal opfyldes **inden** idriftsættelse.

De to analyser overlapper, men er ikke identiske. FRIA'en kræver bl.a. en beskrivelse af idriftsætterens processer, anvendelsesperiode og -hyppighed, de berørte persongrupper, de specifikke risici for skade, gennemførelsen

af menneskeligt tilsyn og de foranstaltninger og klagemekanismer, der skal aktiveres, hvis risiciene opstår. Resultatet skal meddeles markedsovervågningsmyndigheden. Forholdet mellem de to dokumenter er reguleret udtrykkeligt: er nogle af FRIA-forpligtelserne allerede opfyldt gennem DPIA'en efter GDPR artikel 35, **supplerer** FRIA'en den analyse, jf. artikel 27, stk. 4 – og omvendt skal idriftsætteren efter [artikel 26, stk. 9](#) bruge udbyderens oplysninger efter artikel 13 til at opfylde sin DPIA-pligt. Den ene erstatter altså ikke den anden; i praksis bygges de mest hensigtsmæssigt som ét samlet dokument med to spor.

Datatilsynets praksis peger allerede i den retning: udvikling og drift af AI-løsninger indebærer ofte høj risiko og udløser DPIA-pligt, og tilsynet har samtidig understreget, at den dataansvarlige skal kunne påvise, at anvendelsen af personoplysninger til træning af algoritmer ikke overstiger det nødvendige. Se den samlede fremstilling i [oversigten om AI-systemer og GDPR](#).

LOV

[AI-forordningen om harmoniserede regler for brug af kunstig intelligens § 26, stk. 9](#)[AI-forordningen om harmoniserede regler for brug af kunstig intelligens § 27, stk. 1](#)[Databeskyttelsesforordningen § 35, stk. 1](#)

PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	12.06.2024
	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	18.05.2022

§ 8 Typiske faldgruber

DPIA'en skrives efter idriftsættelsen. Den hyppigste og dyreste fejl. Artikel 35, stk. 1, kræver, at analysen foretages **forud for** behandlingen – og en analyse, der først færdiggøres, når systemet kører, kan pr. definition ikke bruges til at vælge foranstaltninger til. Datatilsynet indstillede Nationalt Genom Center til en bøde på 600.000 kr. og nedlagde forbud mod behandlingen, netop fordi behandlingen var påbegyndt, mens analysen stadig var uafsluttet, og det blev anset for skærpende, at man gik i gang med kendskab til, at de lovpligtige analyser ikke var færdige.

It-sikkerhedsrisikovurdering forveksles med konsekvensanalyse. En risikovurdering efter artikel 32 handler om sikkerhedsniveauet; en DPIA skal derudover indeholde formålsbeskrivelse, nødvendigheds- og proportionalitetsvurdering og en vurdering af konsekvenserne for de registreredes **rettigheder**. I AULA-tilsynene udtalte Datatilsynet kritik af Københavns Kommune, fordi konsekvensanalysen ikke opfyldte alle mindstekravene, og efterlyste bl.a., at sammenhængen mellem de enkelte risici og de enkelte foranstaltninger fremgik tydeligt.

Høj restrisiko – men ingen forhåndshøring. Mange stopper, når risikoen er beskrevet, og betragter høringspligten som frivillig. Er restrisikoen efter foranstaltningerne fortsat høj, er behandlingen retligt spærret, indtil Datatilsynet er hørt efter artikel 36. Tilsynet har udtrykkeligt fremhævet, at tilsidesættelse af høringspligten underminerer tilsynets mulighed for at kontrollere lovligheden af behandlinger med stor risiko for borgerne – og at der er tale om en væsentlig retssikkerhedsgaranti.

Leverandørens materiale genbruges ukritisk. En standardanalyse eller et risikokatalog fra systemleverandøren er input, ikke opfyldelse af pligten. I AULA-sagerne henviste kommuner til risikovurderingsmateriale fra KOMBIT, men Datatilsynet fastholdt, at dokumentationsforpligtelsen indebærer, at den dataansvarlige selv skal kunne fremlægge materiale, der viser, hvordan og på hvilket grundlag de databeskyttelsesretlige overvejelser er truffet, og hvad de konkret har givet anledning til.

Ingen dokumenteret tærskelvurdering. Når DPIA fravælges uden skriftlig begrundelse, kan man ikke påvise noget som helst, og bevisbyrden efter ansvarlighedsprincippet vendes reelt mod én selv. Datatilsynet har i tilsyn forudsat, at den dataansvarlige systematisk afdækker, hvilke behandlingsaktiviteter der skal laves konsekvensanalyser for, og lægger en plan for gennemførelsen – en tom mappe er i sig selv et kritikpunkt.

DPO'en inddrages ikke – eller først til sidst. Artikel 35, stk. 2, er en skal-bestemmelse: er der udpeget en databeskyttelsesrådgiver, skal denne rådføres, når der laves DPIA. Sker inddragelsen først, når analysen skal underskrives, mister rådgivningen sin funktion, og manglen kan i sig selv indgå i tilsynets vurdering – i AULA-sagen mod Københavns Kommune indgik netop DPO'ens interne tilsynsrapport i Datatilsynets undersøgelse.

Analysen opdateres aldrig. Nyt modul, ny underleverandør, ny datakilde, tilføjet AI-funktion eller migrering til ny platform ændrer risikobilledet – og udløser pligten til fornyet gennemgang efter artikel 35, stk. 11. En DPIA fra idriftsættelsesåret, der aldrig er rørt siden, dokumenterer i praksis kun, at man ikke har fulgt risikoen.

Man regner med, at lovhjemmel automatisk fritager. Undtagelsen i artikel 35, stk. 10, gælder kun, hvis retsgrundlaget faktisk regulerer de pågældende specifikke behandlingsaktiviteter, **og** der allerede er foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen. At behandlingen har hjemmel i en lov er ikke i sig selv nok – og undtagelsen er kun relevant, hvis der ellers var DPIA-pligt efter stk. 1.

§ 9 Relaterede dokumenter

- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn
- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Samtykkeerklæring \(GDPR\)](#) – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)
- [IT-kontrakt \(systemleverance/SaaS\)](#) – Kontrakten om softwareleverancer og cloud-drift – K-standarderne, agile leverancer, SLA'er og exit

REFERENCE Lovgrundlag

6 paragraffer

Databeskyttelsesforordningen § 35 stk. 1, 3, 7	Databeskyttelsesforordningen § 36 stk. 1
Databeskyttelsesforordningen § 83 stk. 4	Databeskyttelsesloven § 7 stk. 4
Databeskyttelsesloven § 41 stk. 1	Retshåndhævelsesloven § 25

MATERIALE Citerede afgørelser

14 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS		14
16.07.2025	Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	2024-51-0014
24.06.2025	Alvorlig kritik til Digitaliseringsstyrelsen for utilstrækkelig sikkerhed ved brug af personoplysninger i testmiljøer	2023-442-0197
03.07.2024	Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	2023-31-0028
12.06.2024	Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	2024-212-0371
23.05.2024	Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	2023-423-0005
30.01.2024	Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	2023-211-0004
15.01.2024	Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA	2023-420-0001
12.01.2024	Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	
22.12.2023	Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	2023-423-0004
22.12.2023	Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	2023-423-0006
22.12.2023	Alvorlig kritik og påbud til Lolland Kommune for mangelfuld behandlingssikkerhed og manglende konsekvensanalyser	2023-423-0007
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676
25.03.2022	Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling	
05.03.2020	Alvorlig kritik af manglende risikovurdering ved videregivelse af personoplysninger	2019-441-3399

04

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Privatlivspolitik

Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på

Version 1 · Opdateret 21. jul. 2026 · 16 afgørelser · 2018-2025

[Læs online](#)

INTRODUKTION

En **privatlivspolitik** (også kaldet persondatapolitik eller privatlivsmeddelelse) er det dokument, hvormed en dataansvarlig opfylder oplysningspligten i [databeskyttelsesforordningens artikel 13](#) og [artikel 14](#). Forordningen kræver ikke et dokument med et bestemt navn – den kræver, at bestemte oplysninger *gives* til de registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form, jf. [artikel 12, stk. 1](#). For en virksomhed med en hjemmeside, kunder eller ansatte findes der i praksis ingen anden farbar måde at gøre det på end en skriftlig politik.

Parterne er den **dataansvarlige** (virksomheden, foreningen eller myndigheden, der afgør formål og hjælpemidler) på den ene side og de **registrerede** på den anden – kunder, hjemmesidebesøgende, leverandørkontakter, ansøgere, medarbejdere, lejere, patienter, medlemmer. Politikken er ensidig: den er en oplysning, ikke en aftale, og den kan derfor hverken "aftales væk" eller gøres til genstand for accept fra den registrerede. Det er også grunden til, at en privatlivspolitik aldrig i sig selv skaber et behandlingsgrundlag – hjemlen skal findes i [artikel 6](#) (og [artikel 9](#) for følsomme oplysninger) og blot *beskrives* i politikken.

Oversigten er bygget op efter dokumentets egen logik: først hvornår pligten indtræder og hvornår den kan udskydes eller undtages, derefter en checkliste over det indhold artikel 12-14 kræver punkt for punkt, dernæst de fejl Datatilsynets praksis viser er de hyppigste – og til sidst uddybende afsnit om afgrænsningen til fortegnelsen, databehandleraftalen og cookiebanneret, om medarbejderpolitikken som selvstændigt dokument og om håndhævelsen.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Oplysningspligten i artikel 13-14 er ufravigelig for enhver dataansvarlig – privatlivspolitikken er den praktiske opfyldelse af pligten, ikke et frivilligt tillidssignal.
- 02** Det er ikke nok, at politikken *ligger* på hjemmesiden eller intranettet: Datatilsynet har fastslået, at den registrerede skal henvises specifikt til den, og at det ikke må være nødvendigt selv aktivt at lede efter oplysningerne.
- 03** Retsgrundlaget skal angives konkret for hver behandling – en henvisning til, at man "behandler i overensstemmelse med GDPR", opfylder ikke [artikel 13, stk. 1, litra c](#).

- 04** Opbevaring skal angives enten som en konkret periode eller som de kriterier, der bruges til at fastlægge den – "så længe det er nødvendigt" er hverken det ene eller det andet.
- 05** Bruges interesseafvejningsreglen i artikel 6, stk. 1, litra f, skal den konkrete legitime interesse beskrives – ikke bare hjemlen nævnes.
- 06** Privatlivspolitikken er ekstern og henvender sig til de registrerede; artikel 30-fortegnelsen er intern og henvender sig til Datatilsynet. De to dokumenter overlapper i data, men kan ikke erstatte hinanden.
- 07** Medarbejdere og jobansøgere er selvstændige grupper af registrerede – de kræver deres egen politik med egne formål, hjemler, kontrolforanstaltninger og slettefrister.
- 08** Overtrædelse af artikel 12-22 ligger i den høje bødekategori efter [artikel 83, stk. 5](#) og kan i Danmark straffes med bøde eller fængsel indtil 6 måneder efter [databeskyttelsesloven § 41, stk. 1, nr. 5](#).

§ 1 Hvornår er dokumentet påkrævet?

Lovpligtig – uden bagatelgrænse. Oplysningspligten gælder enhver dataansvarlig fra første behandling af personoplysninger. Der er ingen undtagelse for små virksomheder, foreninger eller enkeltmandsvirksomheder, og der findes ingen tærskel svarende til 250-ansattereglen i [artikel 30](#) om fortegnelsen. Har du en hjemmeside med kontaktformular, nyhedsbrev, webshop, kundekartotek eller bare én ansat, er du forpligtet.

Hvornår oplysningerne skal gives – to spor:

- *Artikel 13* (oplysninger indsamlet **hos den registrerede** selv – kontaktformular, ordre, ansøgning, ansættelse): oplysningerne skal gives **på det tidspunkt, hvor personoplysningerne indsamles**. Ikke senere, ikke ved lejlighed.
- *Artikel 14* (oplysninger indsamlet **andre steder fra** – CVR- og adresseleverandører, kreditoplysningsbureauer, henvisere, tidligere arbejdsgivere, offentlige registre, sociale medier): senest **inden for en måned** efter indsamlingen, eller – hvis det sker tidligere – senest ved den første kommunikation med den registrerede eller senest ved første videregivelse, jf. [artikel 14, stk. 3](#).

Betinget pligt – det der udløser opdatering eller et ekstra dokument:

- **Nyt formål:** vil du viderebehandle oplysningerne til et andet formål end det oprindelige, skal den registrerede informeres **forud** for viderebehandlingen, jf. artikel 13, stk. 3, og artikel 14, stk. 4.
- **Medarbejdere og ansøgere:** de er selvstændige grupper af registrerede med egne formål, hjemler og opbevaringsperioder – det kræver i praksis en særskilt medarbejder-/rekrutteringspolitik, som ikke kan rummes i den kundevedtatte politik.
- **Fælles dataansvar:** fastlægger I formål og hjælpemidler sammen med en anden, skal det væsentligste indhold af jeres ordning gøres tilgængeligt for de registrerede, jf. [artikel 26, stk. 2](#).
- **Cookies og lignende teknologier:** informations- og samtykkekravet i [cookiebekendtgørelsen § 3](#) er et *selvstændigt* krav ved siden af artikel 13 – cookiebanneret erstatter ikke privatlivspolitikken, og omvendt.

Hvornår pligten kan begrænses. Artikel 13, stk. 4, og artikel 14, stk. 5, litra a, undtager kun i det omfang den registrerede **allerede er bekendt** med oplysningerne. Artikel 14, stk. 5, litra b-d, undtager ved uforholdsmæssigt stor indsats, ved indsamling/videregivelse udtrykkeligt fastsat i lov og ved lovbestemt tavshedspligt. Dertil kommer de danske begrænsninger i [databeskyttelsesloven § 22](#) (afgørende hensyn til private eller offentlige interesser) og [§ 23](#). Undtagelserne fortolkes snævert og skal vurderes konkret – de er ikke en generel fritagelse.

Frivilligt, men retssikrende. Interne dokumenter – persondatapolitik for medarbejdere om håndtering af data, slettepolitik, oversigt over databehandlere, procedure for rettighedsanmodninger – er ikke selvstændigt påbudt, men er det materiale, der gør det muligt at *påvise* overholdelse efter ansvarlighedsprincippet i [artikel 5, stk. 2](#). Uden dem står du med en politik, du ikke kan dokumentere er sand.

§ 2 Det skal dokumentet indeholde

1. Politikken skal være kortfattet, gennemsigtig, letforståelig og lettilgængelig og skrevet i et klart og enkelt sprog – særligt hvis den retter sig mod børn. Oplysningerne skal gives gratis og aktivt, ikke blot være mulige at finde. (*Databeskyttelsesforordningen § 12, stk. 1*)
2. Identitet på og kontaktoplysninger for den dataansvarlige (og en eventuel repræsentant) skal fremgå, sammen med kontaktoplysninger på databeskyttelsesrådgiveren, hvis der er udpeget en. (*Databeskyttelsesforordningen § 13, stk. 1*)
3. For hver enkelt behandlingsaktivitet skal både formålet og retsgrundlaget angives – altså hvilken bestemmelse i artikel 6 (og artikel 9 ved følsomme oplysninger) behandlingen hviler på. Én samlet hjemmelsliste uden kobling til de enkelte formål er ikke tilstrækkelig. (*Databeskyttelsesforordningen § 13, stk. 1*)
4. Bygger en behandling på interesseafvejningsreglen i artikel 6, stk. 1, litra f, skal den konkrete legitime interesse, der forfølges af virksomheden eller en tredjemand, beskrives. (*Databeskyttelsesforordningen § 13, stk. 1*)
5. Er oplysningerne ikke indsamlet hos den registrerede selv, skal politikken desuden angive de berørte kategorier af personoplysninger og hvilken kilde de stammer fra, herunder om kilden er offentligt tilgængelig. (*Databeskyttelsesforordningen § 14, stk. 1*)
6. Modtagere eller kategorier af modtagere skal oplyses – typisk it-leverandører og databehandlere, koncernselskaber, revisor, inkasso, offentlige myndigheder og betalingsudbydere. (*Databeskyttelsesforordningen § 13, stk. 1*)
7. Overføres oplysninger til tredjelande eller internationale organisationer, skal det fremgå – sammen med om overførslen sker på grundlag af en tilstrækkelighedsafgørelse eller fornødne garantier, og hvordan den registrerede kan få en kopi af garantierne. (*Databeskyttelsesforordningen § 13, stk. 1*)
8. Opbevaringsperioden skal angives – enten som et konkret tidsrum eller, hvis det ikke er muligt, som de kriterier, der bruges til at fastlægge perioden (fx bogføringslovens 5-årsfrist eller forældelsesfristen for det pågældende krav). (*Databeskyttelsesforordningen § 13, stk. 2*)
9. Hele rettighedskataloget skal beskrives: indsigt, berigtigelse, sletning, begrænsning af behandling, indsigelse og dataportabilitet – og ved samtykkebaserede behandlinger retten til når som helst at trække samtykket tilbage med virkning fremadrettet. (*Databeskyttelsesforordningen § 13, stk. 2*)

10. Retten til at klage til Datatilsynet skal fremgå, og det bør gøres let at finde tilsynets kontaktoplysninger. (*Databeskyttelsesforordningen § 13, stk. 2*)
11. Det skal oplyses, om afgivelsen af oplysningerne er lovpligtig eller et krav for at indgå en kontrakt, om den registrerede har pligt til at give dem, og hvad konsekvensen er ved ikke at gøre det. (*Databeskyttelsesforordningen § 13, stk. 2*)
12. Træffes der automatiske afgørelser, herunder profilering, med retsvirkning eller tilsvarende betydelig påvirkning, skal politikken oplyse om det og som minimum give meningsfulde oplysninger om logikken samt om behandlingens betydning og forventede konsekvenser. (*Databeskyttelsesforordningen § 22, stk. 1*)
13. Politikken bør dateres og versionsstyres, og det bør fremgå, hvordan væsentlige ændringer kommunikeres til de registrerede – det er ikke et selvstændigt formkrav, men det er den eneste måde at kunne dokumentere, hvilken information der blev givet hvornår.

LOV

Databeskyttelsesforordningen § 12, stk. 1

Databeskyttelsesforordningen § 13, stk. 1, 2

Databeskyttelsesforordningen § 14, stk. 1

Databeskyttelsesforordningen § 22, stk. 1

Privatlivspolitik, fortegnelse og databehandlersaftale – tre dokumenter, tre adressater

Begreberne blandes konstant sammen, men dokumenterne har hver deres adressat og hver deres hjemmel.

Privatlivspolitikken er ekstern. Den er rettet mod de registrerede og skal indeholde præcis de oplysninger, artikel 13 og 14 opregner. Den kaldes i praksis også persondatapolitik, privatlivsmeddelelse eller privacy notice – navnet er uden retlig betydning, indholdet er alt.

Artikel 30-fortegnelsen er intern. Den er den dataansvarliges eget arbejdsdokument og skal på anmodning stilles til rådighed for Datatilsynet, jf. [artikel 30, stk. 4](#). Den indeholder oplysninger, der aldrig hører hjemme i en offentlig politik – fx en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger. Omvendt indeholder privatlivspolitikken oplysninger, fortegnelsen ikke kræver, fx den fulde rettighedsbeskrivelse og klagevejledningen. I praksis bygges politikken *ovenpå* fortegnelsen: har man ikke kortlagt sine behandlinger, kan man ikke skrive en sand politik.

Databehandlersaftalen er kontraktuel. Den regulerer forholdet mellem den dataansvarlige og leverandøren efter [artikel 28, stk. 3](#) og giver ikke de registrerede nogen information. Til gengæld er det databehandlersaftalerne og deres underdatabehandlere, der leverer indholdet til politikens afsnit om modtagere og tredjelandsoverførsler.

Samtykkeerklæringen er noget fjerde. Den er selve hjemlen for de behandlinger, der hviler på [artikel 6, stk. 1, litra a](#). Politikken skal beskrive, at samtykket kan trækkes tilbage – men den kan ikke selv indhente et samtykke, og en henvisning til politikken gør ikke et samtykke informeret. I sagen om JP/Politikens Hus A/S var det uden betydning, at et behandlingsformål fremgik af persondatapolitikken, når brugeren kunne trykke "Acceptér alle" uden at have set det.

Er I **fælles dataansvarlige** med en anden – fx om en fælles platform eller et fælles arrangement – skal det væsentligste indhold af jeres ordning efter artikel 26, stk. 2, gøres tilgængeligt for de registrerede. Det gøres i praksis i privatlivspolitikken, med angivelse af hvem der er kontaktpunkt for rettighedsanmodninger.

LOV

[Databeskyttelsesforordningen § 26, stk. 2](#)[Databeskyttelsesforordningen § 28, stk. 3](#)[Databeskyttelsesforordningen § 30, stk. 1](#)PRAKSIS **Datatilsynet** · Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk

27.10.2022

§ 4 Artikel 13 eller artikel 14 – kilden bestemmer både indhold og frist

Valget mellem de to bestemmelser er ikke redaktionelt. Det afgør, hvilke oplysninger politikken skal indeholde, hvornår de skal gives, og hvilke undtagelser der er i spil.

Artikel 13 gælder, når oplysningerne kommer fra den registrerede selv – en bestilling, en kontaktformular, en jobansøgning, et ansættelsesforhold. Informationen skal gives *samtidig med indsamlingen*, og der gælder ingen frist at løbe på: er informationen ikke givet ved indsamlingen, er pligten allerede tilsidesat.

Artikel 14 gælder, når oplysningerne kommer andre steder fra. Ud over artikel 13's punkter skal politikken her også angive **hvilke kategorier af personoplysninger** der behandles, og **hvilken kilde** de stammer fra, herunder om kilden var offentligt tilgængelig. Fristen er senest én måned, jf. artikel 14, stk. 3, litra a – men skal oplysningerne bruges til at kommunikere med den registrerede eller videregives, indtræder pligten allerede ved henholdsvis første kommunikation og første videregivelse.

Undtagelserne er reelle, men snævre. Artikel 13, stk. 4, og artikel 14, stk. 5, litra a, gælder kun i det omfang den registrerede *allerede er bekendt* med samtlige oplysninger. Artikel 14, stk. 5, litra b, om uforholdsmæssigt stor indsats kræver en konkret vurdering – Datatilsynet har bl.a. behandlet spørgsmålet, hvor en kommune ville registrere pårørendes kontaktoplysninger til krisehåndtering. Og i en vejledende udtalelse til Uddannelses- og Forskningsstyrelsen fastslog tilsynet, at undtagelsen i artikel 14, stk. 5, litra c, forudsætter en egentlig lovbestemt forpligtelse til at indsamle eller videregive, hvoraf det fremgår, hvilke oplysninger der er tale om; en bestemmelse, der blot giver *mulighed* for at indhente, giver ikke den registrerede tilstrækkelig klarhed.

De danske begrænsninger i [databeskyttelsesloven § 22](#) kan endelig udskyde eller undtage oplysningspligten, hvor afgørende hensyn til private eller offentlige interesser gør sig gældende. I tilsynet med Tryg Forsikring A/S fandt Datatilsynet, at selskabets procedurer for at opfylde artikel 14 ved personovervågning i forbindelse med formodet svindel lå inden for rammerne af artikel 5, stk. 1, artikel 14 og databeskyttelseslovens § 22 – men det forudsætter en dokumenteret, konkret afvejning i den enkelte sag, og pligten genopstår, når hensynet ikke længere gør sig gældende.

LOV

[Databeskyttelsesforordningen § 13, stk. 4](#)[Databeskyttelsesforordningen § 14, stk. 3](#)[Databeskyttelsesloven § 22, stk. 2](#)[Databeskyttelsesloven § 23](#)PRAKSIS **Datatilsynet** · Tryg Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger

02.01.2024

Datatilsynet · Vurdering af undtagelser til oplysningspligten for offentlige myndigheder

04.12.2023

Datatilsynet · Kritik af Det Konservative Folkepartis manglende opfyldelse af oplysningspligten

22.12.2021

Datatilsynet · Behandling af pårørendes kontaktoplysninger til brug for krisehåndtering i Herning Kommune

30.07.2021

§ 5 Gennemsigtighed i praksis: aktiv formidling, lagdeling og sprog

Artikel 12, stk. 1, er den bestemmelse, der oftest overses, fordi den ikke handler om *hvad* der skal stå, men om *hvordan* det skal gives. Kravene er kumulative: kortfattet, gennemsigtigt, letforståeligt, lettilgængeligt – og i et klart og enkelt sprog.

Aktiv formidling. Datatilsynet har i NCC-sagen slået fast, at det ikke skal være nødvendigt for den registrerede selv aktivt at søge efter oplysningerne, og at en persondatapolitik på intranettet ikke opfylder artikel 13 og 14, hvis den registrerede ikke er blevet specifikt henvist til den. Det samme gælder eksternt: i sagen mod Det Konservative Folkeparti blev en informationsside, der først blev lagt på hjemmesiden efter borgerhenvendelser, ikke anset for en formel privatlivspolitik. Konklusionen er praktisk: der skal linkes fra det sted og på det tidspunkt, hvor oplysningerne indsamles.

Lagdeling er tilladt – men det bærende skal frem i første lag. En lagdelt løsning, hvor overskrifterne står øverst og detaljerne foldes ud, er anerkendt god praksis. Men i sagen om JP/Politikens Hus A/S var det ikke nok, at et behandlingsformål fremgik af andet lag og af persondatapolitikken, når langt de fleste brugere accepterede i første lag. Det, brugeren realistisk læser, er det, der afgør, om informationskravet er opfyldt – og designet må ikke skubbe valget i en bestemt retning.

Gennemsigtighed kan række videre end artikel 13's liste. Artikel 13 er en udmøntning af princippet i [artikel 5, stk. 1, litra a](#). Er en behandling uventet for den registrerede, kan princippet derfor kræve information, som ikke direkte er nævnt i artikel 13's opregning – Datatilsynet har fx udtalt alvorlig kritik af en tandlægevirksomhed, der optog samtaler med en ansat uden at informere om det, netop med henvisning til gennemsigtighedsprincippet.

Cookies er et selvstændigt spor. [Cookiebekendtgørelsen § 3](#) stiller egne krav til informationens indhold: klart sprog, formålet med lagringen, identiteten på enhver der foranstalter lagringen, en umiddelbart tilgængelig adgang til at afslå eller tilbagekalde samtykket og vedvarende tilgængelighed på tjenesten. Kravene ligger *ved siden af* artikel 13 og skal håndteres i cookiebanner og cookiepolitik – ikke gemmes i privatlivspolitikken. I sagen om golf.dk fastslog Datatilsynet, at fortsat brug af hjemmesiden ikke udgør et samtykke, og at manglende mulighed for at fravælge de enkelte formål gør samtykket ugyldigt.

LOV

[Cookiebekendtgørelsen § 3](#)
[Databeskyttelsesforordningen § 5, stk. 1](#)
[Databeskyttelsesforordningen § 12, stk. 1](#)

PRAKSIS	Datatilsynet · Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	27.10.2022
	Datatilsynet · Kritik af Det Konservative Folkepartis manglende opfyldelse af oplysningspligten	22.12.2021
	Datatilsynet · Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	13.11.2020
	Datatilsynet · Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse	18.06.2020

§ 6 Medarbejder- og ansøgerpolitikken som selvstændigt dokument

Den kundevedte politik kan ikke bære ansættelsesforholdet. Formålene er andre (personaleadministration, løn, ferie, sygefravær, kontrol), hjemlerne er andre (kontrakt, retlig forpligtelse, [databeskyttelsesloven § 12](#) og interesseafvejning frem for samtykke), og opbevaringsperioderne er andre.

Rekruttering. Ansøgere skal informeres på ansøgningstidspunktet efter artikel 13 – herunder om hvor længe materialet gemmes, hvis ansøgeren ikke ansættes. I tilsynet med Fødevarestyrelsen accepterede Datatilsynet 24

måneders opbevaring af ansøgeroplysninger med henblik på at kunne dokumentere udvælgelsen ved indsigelser om diskrimination, men henstillede samtidig, at både formålet og hjemmelsgrundlaget skulle fremgå utvetydigt af den information, ansøgerne fik, jf. artikel 13, stk. 1, litra c. Indhentes straffeattest, referencer eller paskopi, skal også det fremgå – Datatilsynet vurderede i sagen om Parken Services A/S netop nødvendigheden og tidspunktet for sådanne indhentelser konkret.

Kontrolforanstaltninger. Logning, tv-overvågning, gps, e-mail- og internetkontrol er behandlinger, der skal beskrives på forhånd. I tilsynet med tre politikredses logkontrol bemærkede Datatilsynet udtrykkeligt, at arbejdsgivere skal iagttage oplysningspligten efter artikel 13 eller 14, når kontrolforanstaltninger iværksættes – og tilføjede, at orientering om løbende logkontrol i sig selv har en forebyggende effekt. Manglende forudgående information er derfor ikke bare en formfejl; den underminerer også lovligheden af selve kontrollen.

Nyansatte og fratrådte. Politikken skal udleveres eller linkes ved ansættelsen – ikke blot ligge på intranettet, jf. NCC-sagen – og den bør beskrive, hvad der sker med oplysningerne efter fratræden. Se også den samlede gennemgang af praksis om [databeskyttelse i ansættelsesforhold](#).

LOV	Databeskyttelsesforordningen § 13, stk. 2	Databeskyttelsesloven § 12, stk. 1	
PRAKSIS	Datatilsynet · Tre politikredse får kritik for utilstrækkelig logning af personoplysninger		17.05.2024
	Datatilsynet · Fødevarestyrelsens overholdelse af databeskyttelsesreglerne i forbindelse med rekrutteringsprocesser		02.03.2021
	Datatilsynet · Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse		18.06.2020

§ 7 Håndhævelse: hvad Datatilsynet slår ned på, og hvad det koster

Oplysningspligten er ikke en blød forpligtelse. Overtrædelse af de registreredes rettigheder i artikel 12-22 ligger i den **høje** bødekategori efter artikel 83, stk. 5, litra b – op til 20 mio. EUR eller 4 % af den samlede globale årlige omsætning. I Danmark udsteder Datatilsynet ikke selv bøder: tilsynet politianmelder og indstiller til en bødestørrelse, hvorefter domstolene fastsætter straffen, jf. artikel 83, stk. 9, og [databeskyttelsesloven § 41, stk. 1, nr. 5](#), hvorefter strafferammen er bøde eller fængsel indtil 6 måneder. Forældelsesfristen er 5 år, og juridiske personer kan pålægges strafansvar.

Den typiske sanktion i praksis er dog **kritik** eller **alvorlig kritik**, ofte kombineret med påbud. Datatilsynet har udtalt alvorlig kritik af mangelfuld opfyldelse af oplysningspligten over for både private virksomheder (SIF Gruppen A/S) og offentlige/§ 60-lignende aktører (Fynbus I/S), ligesom en offentlig myndighed er blevet kritiseret for manglende overholdelse af oplysningspligten, og Kriminalforsorgen har fået alvorlig kritik på retshåndhævelseslovens tilsvarende regler.

De tunge sanktioner falder, når politikkenes løfter ikke holder i systemerne. Gyldendal A/S blev politianmeldt med indstilling om en bøde på 1 mio. kr. for at opbevare oplysninger om ca. 685.000 tidligere bogklubmedlemmer uden sagligt formål, i flere tilfælde i over ti år; i en anden sag blev en virksomhed politianmeldt med indstilling om 150.000 kr., bl.a. fordi interne slettefrister ikke var eksekveret i et legacy-system. Pointen er den samme: en slettepolitik på papir er ikke en slettepolitik.

Endelig gennemføres oplysningspligten i stigende grad via **tematiske tilsyn**. I 2025 gennemførte Datatilsynet tilsyn med fem ejendomsadministratorer – DAB, KAB, DAB-Lejerbo, DEAS og Boligexperten – med fokus på retten til indsigt, retten til sletning og oplysningspligten efter artikel 14, når oplysninger indsamles fra

tredjeparter; det gennemgåede materiale viste generelt god efterlevelse, og tilsynet blev afsluttet med et samlet notat med observationer. Forbered dig derfor på, at politikken skal kunne holdes op mod skriftlige interne procedurer og konkrete afgørelser.

Baggrund og bredere praksis findes i oversigterne over [Datatilsynets afgørelser](#) og [retten til at blive glemt](#).

LOV	Databeskyttelsesforordningen § 83, stk. 5	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Datatilsynet · Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	12.12.2025
	Datatilsynet · Politianmeldelse af privat virksomhed for manglende sletning af kundedata	02.12.2022
	Datatilsynet · Politianmeldelse af Gyldendal for manglende sletning af 800.000 kunders personoplysninger	22.06.2022
	Datatilsynet · Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	07.08.2020
	Datatilsynet · Alvorlig kritik af Fynbus I/S for mangelfuld oplysningspligt og håndtering af de registreredes rettigheder	06.07.2020
	Datatilsynet · Kritik af offentlig myndighed for manglende overholdelse af oplysningspligten	22.05.2020
	Datatilsynet · Alvorlig kritik af Kriminalforsorgen for manglende overholdelse af oplysningspligten	12.12.2018

§ 8 Typiske faldgruber

Skabelonpolitik, der ikke beskriver virksomhedens faktiske behandlinger. Den hyppigste fejl er en politik hentet fra en konkurrent eller en generator, som nævner behandlinger virksomheden ikke foretager – og udelader dem, den rent faktisk foretager. Datatilsynet har udtalt alvorlig kritik af både private og offentlige dataansvarlige for mangelfuld opfyldelse af oplysningspligten, bl.a. i sagen mod SIF Gruppen A/S og i sagen mod Fynbus I/S. Ud over kritikken indebærer en usand politik, at man ikke kan påvise overholdelse efter ansvarlighedsprincippet i artikel 5, stk. 2.

Politikken ligger bare på hjemmesiden eller intranettet. At gøre politikken tilgængelig er ikke det samme som at give oplysningerne. I NCC-sagen fastslog Datatilsynet, at det ikke er tilstrækkeligt, at persondatapolitikken er tilgængelig på intranettet, hvis den registrerede ikke er blevet specifikt henvist til den – det skal ikke være nødvendigt selv aktivt at søge efter oplysningerne. Konsekvensen var alvorlig kritik. Praktisk betyder det, at der skal linkes direkte fra formularen, ansættelsesbrevet, ordrebekræftelsen eller det brev, hvor oplysningerne indsamles.

Manglende eller forkert hjemmelsangivelse. "Vi behandler dine oplysninger i overensstemmelse med databeskyttelsesforordningen" er ikke en retsgrundlagsangivelse. Datatilsynet henstillede i tilsynet med Fødevarestyrelsen udtrykkeligt, at hjemmelsgrundlaget skal fremgå utvetydigt af den information, der gives, jf. artikel 13, stk. 1, litra c. Særligt farligt er det at angive samtykke som hjemmel, når behandlingen reelt hviler på kontrakt, retlig forpligtelse eller interesseafvejning – så er både informationen og et eventuelt indhentet samtykke forkert, og i ansættelsesforhold vil samtykket sjældent være frivilligt.

"Så længe det er nødvendigt" i stedet for periode eller kriterier. Artikel 13, stk. 2, litra a, kræver enten et tidsrum eller de kriterier, der fastlægger tidsrummet – en formulering som "så længe det er nødvendigt" er ingen af delene. Endnu værre er det at love slettefrister, systemerne ikke overholder: Datatilsynet indstillede Gyldendal A/S til en bøde på 1 mio. kr. for opbevaring af ca. 685.000 tidligere bogklubmedlemmers oplysninger uden sagligt formål, og i en anden sag blev en virksomhed politianmeldt med indstilling om 150.000 kr., bl.a. fordi en slettepolitik på papir ikke var eksekveret teknisk.

Ingen politik for medarbejdere og jobansøgere. Mange virksomheder har en kundevendt politik, men intet til de ansatte og ansøgere – selv om det ofte er dér, de mest indgribende behandlinger ligger: rekruttering, straffeattester, sygefravær, logning og andre kontrolforanstaltninger. Datatilsynet har i tilsyn med politikredsenes logkontrol udtrykkeligt bemærket, at arbejdsgivere skal iagttage oplysningspligten efter artikel 13 eller 14, når der iværksættes kontrolforanstaltninger. Manglende information gør ikke kun kontrollen uoplyst – den kan gøre den ulovlig.

Artikel 14-fristen overskrides, eller undtagelserne strækkes for langt. Indsamles oplysninger fra andre kilder – adresseleverandører, kreditoplysningsbureauer, offentlige registre – er fristen senest én måned, jf. artikel 14, stk. 3. Datatilsynet udtalte kritik af Det Konservative Folkeparti for manglende opfyldelse af artikel 14 ved segmenteret direct mail, hvor en informationsside på partiets hjemmeside ikke blev anset for tilstrækkelig. Og i en vejledende udtalelse fastslog tilsynet, at undtagelsen i artikel 14, stk. 5, litra c, kræver en egentlig lovbestemt *forpligtelse* til at indsamle eller videregive, hvor det fremgår hvilke oplysninger der er tale om – en "kan"-bestemmelse rækker ikke.

Cookiebanneret forveksles med privatlivspolitikken. De to dokumenter har forskellig hjemmel: cookiebekendtgørelsen § 3 for lagring og adgang til oplysninger i brugerens udstyr, artikel 13 for den efterfølgende behandling af personoplysninger. Datatilsynet udtalte alvorlig kritik af JP/Politikens Hus A/S, bl.a. fordi et behandlingsformål først fremgik af andet lag og af persondatapolitikken, mens 72-75 % trykkede "Acceptér alle" i første lag – og fordi et trafiklyslignende farvevalg udgjorde nudging i strid med gennemsigtighedsprincippet. I DGU-sagen var fortsat brug af hjemmesiden ikke et gyldigt samtykke.

Politikken opdateres aldrig. Nye systemer, nye leverandører, nye tredjelandsoverførsler, ny brug af AI-værktøjer og nye formål gør en politik forældet på få måneder. Skal oplysningerne bruges til et andet formål end det oprindelige, skal den registrerede informeres *forud* for viderebehandlingen efter artikel 13, stk. 3. En udateret politik uden versionsstyring gør det desuden umuligt at bevise, hvilken information der faktisk blev givet på indsamlingstidspunktet.

§ 9 Relaterede dokumenter

- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og Datatilsynets første anmodning ved tilsyn
- [Databehandlaftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Samtykkeerklæring \(GDPR\)](#) – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)
- [Konsekvensanalyse \(DPIA\)](#) – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet

- [Personalehåndbog](#) – Virksomhedens interne regelsæt – hvad der binder, hvad der kræver varsel at ændre, og de lovpligtige politikker indeni
- [Handelsbetingelser \(webshop/B2C\)](#) – Vilkårene bag købsknappen – forbrugeraftalelovens oplysningskrav, fortrydelsesret og de vilkår der ikke binder
- [Whistleblowerpolitik og -ordning](#) – Den lovpligtige interne indberetningsordning for arbejdsgivere med 50+ ansatte – etablering, procedurer og fortrolighed

REFERENCE Lovgrundlag

8 paragraffer

Databeskyttelsesforordningen § 5	stk. 1	Databeskyttelsesforordningen § 12	stk. 1
Databeskyttelsesforordningen § 13	stk. 1	Databeskyttelsesforordningen § 14	stk. 1
Databeskyttelsesforordningen § 22	stk. 1	Databeskyttelsesforordningen § 83	stk. 5
Databeskyttelsesloven § 22	stk. 1	Databeskyttelsesloven § 41	stk. 1

MATERIALE Citerede afgørelser

16 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS

16

12.12.2025	Datatilsynets tematiske tilsyn med ejendomsadministratorers behandling af personoplysninger	2025-41-0139
17.05.2024	Tre politikredse får kritik for utilstrækkelig logning af personoplysninger	2023-813-0002
02.01.2024	Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	2022-431-0204
04.12.2023	Vurdering af undtagelser til oplysningspligten for offentlige myndigheder	2023-212-0030
02.12.2022	Politianmeldelse af privat virksomhed for manglende sletning af kundedata	
27.10.2022	Alvorlig kritik af JP/Politikens samtykkeløsning på eb.dk	2021-41-0149
22.06.2022	Politianmeldelse af Gyldendal for manglende sletning af 800.000 kunders personoplysninger	
22.12.2021	Kritik af Det Konservative Folkepartis manglende opfyldelse af oplysningspligten	2019-431-0031
30.07.2021	Behandling af pårørendes kontaktoplysninger til brug for krisehåndtering i Herning Kommune	2021-212-2937
02.03.2021	Fødevarestyrelsens overholdelse af databeskyttelsesreglerne i forbindelse med rekrutteringsprocesser	2019-421-0033
13.11.2020	Alvorlig kritik af virksomheds indhentelse af samtykke til behandling af personoplysninger på hjemmeside	2020-31-3354
07.08.2020	Alvorlig kritik af SIF Gruppen A/S for mangelfuld opfyldelse af oplysningspligten	2019-41-0043

06.07.2020	Alvorlig kritik af Fynbus I/S for mangelfuld oplysningspligt og håndtering af de registreredes rettigheder	Journalnummer: 2019-41-0047
18.06.2020	Alvorlig kritik af virksomheds håndtering af følsomme personoplysninger efter afskedigelse	2019-31-2250
22.05.2020	Kritik af offentlig myndighed for manglende overholdelse af oplysningspligten	
12.12.2018	Alvorlig kritik af Kriminalforsorgen for manglende overholdelse af oplysningspligten	J.nr. 2018-421-0001

05

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Samtykkeerklæring (GDPR)

Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)

Version 1 · Opdateret 21. jul. 2026 · 21 afgørelser · 2004-2025

[Læs online](#)

INTRODUKTION

En samtykkeerklæring er den dataansvarliges dokumentation for, at en person frivilligt har sagt ja til en konkret behandling af sine personoplysninger. Parterne er den **dataansvarlige** – virksomheden, foreningen eller myndigheden, der bestemmer formål og hjælpemidler – og den **registrerede**, som oplysningerne handler om. I modsætning til en aftale binder samtykket ikke den registrerede: det kan trækkes tilbage når som helst, uden begrundelse og uden omkostninger.

Retligt er samtykket ét af seks ligestillede behandlingsgrundlag i [GDPR artikel 6, stk. 1, litra a](#). Det er hverken finere eller mere sikkert end de øvrige – tværtimod er det det mest skrøbelige, fordi behandlingsgrundlaget forsvinder i samme sekund, den registrerede fortryder. Definitionen i [artikel 4, nr. 11](#) stiller fire kumulative krav: samtykket skal være **frivilligt, specifikt, informeret og utvetydigt** og gives ved erklæring eller klar bekræftelse.

Oversigten følger dokumentets livsforløb: først hvornår samtykke overhovedet er det rigtige – og undertiden det eneste lovlige – grundlag, dernæst en checkliste over hvad erklæringen skal indeholde, og til sidst de fejl, der i praksis gør samtykket ugyldigt. Den danske håndhævelse illustreres især af Forbrugerombudsmandens spam- og telefonsalgssager, hvor manglende eller ugyldige samtykker har kostet bøder fra 10.000 kr. til 850.000 kr.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Samtykke er ét af seks ligestillede behandlingsgrundlag – ikke det fineste. Det er det mest skrøbelige, fordi det kan trækkes tilbage når som helst, og behandlingen så skal ophøre.
- 02** Et gyldigt samtykke skal være frivilligt, specifikt, informeret og utvetydigt og gives ved erklæring eller klar bekræftelse – tavshed, forudafkrydsede felter og "fortsat brug af tjenesten" tæller ikke.
- 03** Bevisbyrden er vendt: den dataansvarlige skal kunne **påvise**, at samtykket er givet, jf. [GDPR artikel 7, stk. 1](#). Kan du ikke det, findes samtykket juridisk set ikke.
- 04** Det skal være lige så let at trække samtykket tilbage som at give det, og den registrerede skal oplyses om tilbagetrækningsretten **inden** samtykket gives (artikel 7, stk. 3).

- 05** Gøres en ydelse eller en kontrakt betinget af et samtykke, der ikke er nødvendigt for ydelsen, er frivilligheden som udgangspunkt væk (artikel 7, stk. 4).
- 06** Følsomme oplysninger kræver et **udtrykkeligt** samtykke – en generel accept af vilkår eller et enkelt afkrydsningsfelt uden særskilt stillingtagen er ikke nok.
- 07** Samtykke gives til ét formål og til én bestemt dataansvarlig: nyt formål, ny afsender eller en koncernsøster kræver et nyt samtykke.
- 08** Ved informationssamfundstjenester rettet mod børn er den danske aldersgrænse 15 år siden 1. januar 2024 – under den grænse skal forældremyndighedsindehaveren give eller godkende samtykket.
- 09** Bøder for ugyldige samtykker pålægges i Danmark af domstolene efter politianmeldelse – både efter [databeskyttelsesloven § 41](#) og, ved markedsføring, efter markedsføringsloven.

§ 1 Hvornår er dokumentet påkrævet?

Der findes **ingen generel pligt** til at have en samtykkeerklæring. Pligten er **betinget** og udløses i det øjeblik samtykke er – eller nødvendigvis må være – behandlingsgrundlaget. Vælger du samtykke, skifter kravene fra "kan" til "skal": erklæringen skal opfylde alle fire gyldighedskrav i [GDPR artikel 4, nr. 11](#), og du skal bagefter kunne påvise, at samtykket blev givet.

Situationer der udløser pligten:

- **Elektronisk markedsføring.** E-mails, sms'er og automatiske opkald med markedsføring kræver forudgående samtykke efter [markedsføringsloven § 10, stk. 1](#) – medmindre den snævre "soft opt-in"-undtagelse i stk. 2 om egne tilsvarende produkter til eksisterende kunder er opfyldt.
- **Cookies og lignende teknologier.** Lagring af eller adgang til oplysninger i brugerens udstyr kræver samtykke efter fyldestgørende information, jf. [cookiebekendtgørelsen § 3](#) – undtagen rent tekniske nødvendigheder.
- **Følsomme oplysninger** (helbred, fagforening, religion, biometri, seksuelle forhold m.v.), hvor ingen af de øvrige undtagelser passer. Her kræves **udtrykkeligt** samtykke efter [GDPR artikel 9, stk. 2, litra a](#), jf. [databeskyttelsesloven § 7, stk. 1](#).
- **Oplysninger om strafbare forhold.** Private må som udgangspunkt kun behandle og videregive dem med den registreredes udtrykkelige samtykke, jf. [databeskyttelsesloven § 8, stk. 3](#).
- **CPR-numre hos private** – og navnlig offentliggørelse af dem, jf. [databeskyttelsesloven § 11, stk. 2, nr. 2](#).
- **Billeder, videoer og udtalelser** af kunder, elever, medlemmer eller ansatte på hjemmeside og sociale medier, hvor der ikke er en legitim interesse, der går forud.
- **Børn under 15 år** ved udbud af informationssamfundstjenester direkte til børn: samtykket skal gives eller godkendes af forældremyndighedsindehaveren, jf. [databeskyttelsesloven § 6, stk. 2](#). Grænsen var 13 år indtil 1. januar 2024 og er nu 15 år.

Hvornår du IKKE skal bruge samtykke: Hvis behandlingen alligevel vil ske – fordi den er nødvendig for at opfylde kontrakten, for at overholde en retlig forpligtelse (bogføring, ansættelsesretlige krav) eller for at forfølge

en legitim interesse – er samtykket illusorisk. Et samtykke, den registrerede reelt ikke kan sige nej til, er ikke frivilligt og dermed ugyldigt, og du står tilbage uden behandlingsgrundlag overhovedet.

Frivilligt, men retssikrende: Forordningen stiller ingen formkrav – et samtykke kan gives mundtligt eller ved en klar bekræftende handling. Men fordi bevisbyrden ligger hos den dataansvarlige, er en skriftlig eller digital erklæring med tidsstempel, versioneret ordlyd og log i praksis den eneste farbare vej. Uden dokumentation eksisterer samtykket ikke juridisk.

§ 2 Det skal dokumentet indeholde

1. Erklæringen skal entydigt identificere den dataansvarlige med navn og kontaktoplysninger – og enhver anden virksomhed, der skal kunne støtte ret på samtykket. Et samtykke til "os og vores samarbejdspartnere" uden navngivning er ikke specifikt nok. (*Databeskyttelsesforordningen § 13, stk. 1*)
2. Hvert formål skal beskrives præcist og adskilt, så den registrerede kan sige ja til ét formål og nej til et andet, og det skal fremgå hvilke kategorier af oplysninger der behandles til formålet. (*Databeskyttelsesforordningen § 6, stk. 1*)
3. Indgår samtykket i et dokument, der også vedrører andre forhold (handelsbetingelser, ansættelseskontrakt, købsaftale), skal anmodningen forelægges klart adskilt fra det øvrige, i letforståelig og lettilgængelig form og i et klart og enkelt sprog. (*Databeskyttelsesforordningen § 7, stk. 2*)
4. Samtykket skal afgives ved en aktiv, utvetydig handling fra den registrerede. Forhåndsafkrydsede felter, on-slidere som standard, passivitet eller fortsat brug af tjenesten opfylder ikke kravet. (*Databeskyttelsesforordningen § 4*)
5. Omfatter behandlingen følsomme oplysninger, skal samtykket være udtrykkeligt – dvs. den registrerede skal tage særskilt og udtrykkelig stilling til netop disse oplysninger. (*Databeskyttelsesforordningen § 9, stk. 2*)
6. Det skal fremgå, hvem oplysningerne videregives til (modtagere eller kategorier af modtagere), og om de overføres til et tredjeland – samt på hvilket grundlag. (*Databeskyttelsesforordningen § 13, stk. 1*)
7. Erklæringen skal oplyse om opbevaringsperioden eller kriterierne for den, om de registreredes rettigheder (indsigt, berigtigelse, sletning, indsigelse) og om retten til at klage til Datatilsynet. (*Databeskyttelsesforordningen § 13, stk. 2*)
8. Inden samtykket gives, skal den registrerede oplyses om retten til at trække det tilbage, om hvordan det konkret gøres, og om at tilbagetrækning ikke berører lovligheden af den behandling, der allerede er sket. Tilbagetrækning skal være lige så let som afgivelsen. (*Databeskyttelsesforordningen § 7, stk. 3*)
9. Erklæringen må ikke gøre levering af en vare, tjeneste eller kontrakt betinget af samtykke til behandling, der ikke er nødvendig for netop den ydelse – ellers er samtykket som udgangspunkt ikke frivilligt. (*Databeskyttelsesforordningen § 7, stk. 4*)
10. Retter tjenesten sig mod børn under 15 år, skal samtykket gives eller godkendes af indehaveren af forældremyndigheden, og den dataansvarlige skal gøre rimelige bestræbelser på at kontrollere dette. (*Databeskyttelsesloven § 6, stk. 3*)
11. Skal samtykket bære elektronisk markedsføring, skal det tillige specificere hvilke kommunikationsformer (e-mail, sms, telefon), hvilke produkttyper og hvilke afsendere det dækker – og der skal gives mulighed for let og gebyrfri tilbagekaldelse. (*Markedsføringsloven § 10, stk. 1*)
- 12.

Der skal etableres et dokumentationsspor, der viser hvem der gav samtykke, hvornår, ad hvilken kanal og efter hvilken ordlyd – ellers kan samtykket ikke påvises. (*Databeskyttelsesforordningen § 7, stk. 1*)

13. Samtykketeksterne bør versioneres og gemmes, og dokumentationen bør opbevares, så længe samtykket anvendes og i en rimelig periode derefter, så et bestridt samtykke fortsat kan dokumenteres.

LOV

Databeskyttelsesforordningen § 4

Databeskyttelsesforordningen § 6, stk. 1

Databeskyttelsesforordningen § 7, stk. 1, 2, 3, 4

Databeskyttelsesforordningen § 9, stk. 2

Databeskyttelsesforordningen § 13, stk. 1, 2

Databeskyttelsesloven § 6, stk. 3

Markedsføringsloven § 10, stk. 1

§ 3 Samtykke eller en anden hjemmel? Valget, der afgør alt

Det første – og hyppigst forkerte – valg er selve hjemlen. [GDPR artikel 6, stk. 1](#)

opregner seks sidestillede grundlag: samtykke, kontraktopfyldelse, retlig forpligtelse, vitale interesser, samfundsinteresse/myndighedsudøvelse og legitim interesse. Ingen af dem rangerer over de andre, og valget skal træffes én gang for alle, inden behandlingen begynder – man kan ikke skifte til en anden hjemmel, når samtykket viser sig at holde dårligt.

Samtykkets pris er dets skrøbelighed. Trækkes det tilbage, forsvinder grundlaget, og behandlingen skal ophøre; oplysningerne skal som udgangspunkt slettes, medmindre en anden hjemmel selvstændigt kan bære en fortsat opbevaring. Derfor egner samtykket sig til det, der reelt er valgfrit for den registrerede – nyhedsbreve, billeder til markedsføring, deltagelse i undersøgelser, offentliggørelse af portrætter – og dårligt til driftskritiske behandlinger. Er behandlingen nødvendig for at levere det, kunden har købt, er kontraktgrundlaget det rigtige, og et samtykke ovenpå er både overflødigt og vildledende.

I ansættelsesforhold er billedet særligt: [databeskyttelsesloven § 12, stk. 3](#) slår fast, at samtykke kan anvendes før, under og efter ansættelsen, og forarbejderne henviser til, at forordningen udtrykkeligt overlader medlemsstaterne at regulere netop dette. Men hjemlen ændrer ikke frivillighedskravet. Magtubalancen mellem arbejdsgiver og medarbejder betyder, at et samtykke kun holder, hvis et nej er reelt konsekvensfrit – og arbejdsgiveren bør derfor altid have en reservehjemmel, typisk § 12, stk. 1 eller 2, når behandlingen udspringer af lovgivning eller kollektiv overenskomst.

Frivillighedens grænse er i dansk praksis blevet trukket i konkrete sager. Forbrugerombudsmanden accepterede, at indmeldelse i et fordelsprogram kunne betinges af markedsføringssamtykke, fordi bonusserne svarede til en rabat, og fravalg ikke havde negative konsekvenser – men afviste en model, hvor adgangen til nyhedsartikler alene kunne "betales" med et samtykke til markedsføring fra tredjeparter. Testen er, om den registrerede har et reelt, ligeværdigt alternativ.

LOV

Databeskyttelsesforordningen § 6, stk. 1

Databeskyttelsesforordningen § 7, stk. 4

Databeskyttelsesloven § 12, stk. 3

PRAKSIS **Forbrugerombudsmanden** · Samtykke til markedsføring som betingelse for adgang til nyheder er ikke frivilligt 24.07.2020

Forbrugerombudsmanden · Betinget samtykke til markedsføring ved indmeldelse i fordelsprogram 21.06.2019

§ 4 De fire gyldighedskrav i praksis

Frivilligt. Ved vurderingen tages der efter artikel 7, stk. 4, størst muligt hensyn til, om opfyldelsen af en kontrakt er gjort betinget af samtykke til behandling, der ikke er nødvendig for kontrakten. Vildledning ødelægger også frivilligheden: et forsikringsselskab fik i 2024 indskærpet både vildlednings- og aggressivitetsforbuddet, fordi kunder, der sagde nej til markedsføring, blev mødt af en advarsel om, at selskabet så ikke kunne rådgive optimalt – en påstand uden hold i virkeligheden. Samtykkerne blev anset for ugyldige og efterfølgende slettet.

Specifikt. Samtykket skal knytte sig til ét eller flere klart angivne formål. Formuleringer som "produkter, aktuelle tilbud og informationer" er for brede, og en samtykkeformular skal angive både kommunikationsform og hvor mange henvendelser der kan komme, når den bærer markedsføring. Fremgår det ikke, hvilke virksomheder der vil kontakte forbrugeren, er samtykket ligeledes ugyldigt – det så man i en sag om en prissammenligningsside for elaftaler.

Informeret. Den registrerede skal på afgivelsestidspunktet have de oplysninger, [artikel 13, stk. 2, litra c](#) og de øvrige led i artikel 13 kræver – herunder formål, retsgrundlag, modtagere, opbevaringstid og retten til at trække samtykket tilbage. Informationen skal efter [artikel 12](#) gives kortfattet, gennemsigtigt og i et klart og enkelt sprog – særligt når den er rettet mod børn. At kunden blot udfylder sine kontaktoplysninger, er ikke et tilstrækkeligt informeret samtykke.

Utvetydigt. Der skal foreligge en erklæring eller en klar bekræftelse. Forhåndsafkrydsede felter er afvist gang på gang: ved online booking af bilsyn, ved oprettelse på et nyhedsmedie, i et bilag til en købsaftale om fast ejendom og i en spamsag i 2025. Et samtykke, der afgives samtidig med accept af forretningsbetingelser, er heller ikke utvetydigt.

Ovenpå de fire krav gælder de almindelige principper i [artikel 5, stk. 1](#) – lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning og dataminimering. Et samtykke kan ikke legitimere indsamling af flere oplysninger, end formålet kræver.

LOV

[Databeskyttelsesforordningen § 4](#)
[Databeskyttelsesforordningen § 5, stk. 1](#)
[Databeskyttelsesforordningen § 12, stk. 1](#)
[Databeskyttelsesforordningen § 13, stk. 2](#)

PRAKSIS

Forbrugerombudsmanden · Online tøjvirksomheds udsendelse af spam og brug af ugyldigt samtykke ved forhåndsafkrydsning	24.11.2025
Forbrugerombudsmanden · Virksomheds samtykkeindhentning til betalingsoplysninger levede ikke op til krav i Betalingsloven	17.12.2024
Forbrugerombudsmanden · Vildledende samtykkeflow: Forsikringsselskab indskærpes for aggressiv markedsføringspraksis	19.02.2024
Forbrugerombudsmanden · Ugyldigt forhåndsafkrydset samtykke til alarmselskab ved ejendomshandel	09.01.2023
Forbrugerombudsmanden · Forhåndsafkrydset samtykkeboks til markedsføring ved online booking er ulovlig	26.10.2015
Forbrugerombudsmanden · Ulovlig indhentning af samtykke til markedsføring via forhåndsafkrydset felt og manglende konkretisering	13.07.2015
Forbrugerombudsmanden · Forbrugerombudsmandens krav til tydelighed ved indhentning af samtykke til markedsføring fra tredjeparter	17.07.2014

Tilbagetrækning og bevisbyrde – de to krav, der oftest vælter samtykket

§ 5

Artikel 7, stk. 3, indeholder fire selvstændige krav, som en samtykkeerklæring skal håndtere: den registrerede kan **til enhver tid** trække samtykket tilbage; tilbagetrækningen virker kun fremadrettet og berører ikke lovligheden af det, der allerede er sket; den registrerede skal oplyses om retten **inden** samtykket gives; og det skal være **lige så let** at trække tilbage som at give. Er samtykket givet med ét klik i et cookiebanner eller en tilmeldingsformular, skal afmeldingen kunne ske lige så enkelt – typisk via et permanent, synligt link eller ikon.

Dokumentationskravet i artikel 7, stk. 1, er det, der i praksis afgør sagerne. Forbrugerombudsmandens spamvejledning – se [Spamvejledningen 2018](#) – kræver, at virksomheden kan dokumentere ikke blot, at samtykket blev givet, men også **under hvilke omstændigheder** og **hvilke oplysninger personen fik** på afgivelsestidspunktet. Registrering af navn, adresse og tidspunkt er ikke nok, og en IP-adresse er efter Forbrugerombudsmandens opfattelse ikke tilstrækkelig dokumentation for, at en bestemt person har givet samtykke. Vejledningen anbefaler en dobbelt opt-in-model, hvor tilmeldingen bekræftes ved et klik i en efterfølgende mail, og at dokumentationen – herunder en udskrift eller billedserie af det sted, hvor samtykket blev givet – opbevares, så længe samtykket bruges, og i mindst to år derefter.

Sagerne følger et fast mønster: virksomheden hævder at have samtykke, kan ikke fremlægge det, og bøden falder. En virksomhed vedtog et administrativt bødeforelæg, fordi kunder, der alene havde oplyst deres e-mailadresse for at få en faktura, blev tilmeldt markedsføring; en anden fik bøde for 347 e-mails til 74 forbrugere; en tredje kunne ikke lægge ansvaret over på sit affiliatenetværk. Bødeniveauet for spam er efter fast praksis 10.000 kr. for op til 100 ulovlige henvendelser og derefter 100 kr. pr. overtrædelse.

LOV	Databeskyttelsesforordningen § 7, stk. 1, 3	Markedsføringsloven § 10, stk. 1
PRAKSIS	Forbrugerombudsmanden · Forbrugerombudsmanden undersøger leadvirksomheders brug af konkurrencer til at indhente samtykke til markedsføring 13.12.2021 Forbrugerombudsmanden · Elselskab vedtager bøde for uanmodede telefoniske henvendelser trods påstået samtykke 19.08.2021 Forbrugerombudsmanden · Virksomhed straffes for uanmodet elektronisk markedsføring uden samtykke 19.08.2020 Forbrugerombudsmanden · Bøde for uanmodet telefonsalg trods manglende samtykke 10.08.2020 Forbrugerombudsmanden · Virksomhed idømmes bøde for spamming uden gyldigt samtykke 04.06.2019 Forbrugerombudsmanden · Bøde for overtrædelse af markedsføringsloven ved udsendelse af e-mails uden samtykke 20.05.2019	

Børn, følsomme oplysninger, CPR og strafbare forhold – de danske særregler

§ 6

Dansk ret udnytter flere af forordningens nationale råderum, og de rammer samtykkeerklæringen direkte.

Børn. [GDPR artikel 8, stk. 1](#) sætter udgangspunktet ved 16 år ved informationssamfundstjenester udbudt direkte til børn, men tillader medlemsstaterne at gå ned til 13 år. Danmark valgte oprindeligt 13 år, men grænsen blev **hævet til 15 år med virkning fra 1. januar 2024**. Er barnet under 15 år, er behandlingen kun lovlig, hvis samtykket gives eller godkendes af forældremyndighedsindehaveren, og den dataansvarlige skal under hensyntagen til tilgængelig teknologi gøre rimelige bestræbelser på at kontrollere dette. Skabeloner og

aldersporte, der stadig opererer med 13 år, er dermed forældede. Uden for informationssamfundstjenester – fx en skoles eller forenings brug af børnebilleder – gælder ingen fast aldersgrænse, men forældresamtykke er den praktiske hovedregel for de yngste.

Følsomme oplysninger. Forbuddet i artikel 9, stk. 1, kan efter [databeskyttelsesloven § 7, stk. 1](#) løftes ved udtrykkeligt samtykke. "Udtrykkeligt" betyder, at den registrerede skal tage særskilt stilling netop til de følsomme oplysninger – ikke blot acceptere en generel erklæring, hvor helbredsoplysninger indgår i en opremsning.

Strafbare forhold. Private må efter [databeskyttelsesloven § 8, stk. 3](#) behandle oplysninger om strafbare forhold, hvis den registrerede har givet udtrykkeligt samtykke – og videregivelse kræver som udgangspunkt udtrykkeligt samtykke efter stk. 4. Det har praktisk betydning ved straffeattester i rekruttering.

CPR-nummer. Private kan behandle personnummer på grundlag af samtykke efter [databeskyttelsesloven § 11, stk. 2, nr. 2](#), og offentliggørelse af et personnummer kræver altid samtykke i overensstemmelse med artikel 7, jf. § 11, stk. 3.

Børn fortjener særlig omhu også i markedsføringen: allerede før GDPR fandt Forbrugerombudsmanden det i strid med god markedsføringsskik at lokke unge til at oplyse kammeraters navne og adresser og sende dem adresserede reklamebreve uden forældrenes samtykke.

LOV

[Databeskyttelsesforordningen § 8, stk. 1](#)[Databeskyttelsesloven § 6, stk. 2](#)[Databeskyttelsesloven § 7, stk. 1](#)[Databeskyttelsesloven § 8, stk. 3](#)[Databeskyttelsesloven § 11, stk. 2](#)

PRAKSIS

Forbrugerombudsmanden · Tøjforretnings brug af børns oplysninger til direkte markedsføring:
Overtrædelse af god markedsføringsskik

24.05.2004

§ 7 Markedsføring og cookies: to samtykkeregimer oveni GDPR

Samtykke til markedsføring og til cookies reguleres af to selvstændige regelsæt, der gælder **ved siden af** GDPR – og som ofte er dem, der først udløser sanktioner.

Spamforbuddet. Efter markedsføringsloven må en erhvervsdrivende ikke rette henvendelse med henblik på direkte markedsføring via e-mail, sms eller automatiske opkaldssystemer uden forudgående samtykke. Samtykkebegrebet er defineret i [markedsføringsloven § 2, nr. 14](#) med samme fire krav som i forordningen: frivillig, specifik, informeret og utvetydig viljetilkendegivelse. Loven kræver desuden, at der oplyses om tilbagetrækningsretten, inden samtykket gives, og at tilbagekaldelse kan ske let og gebyrfrit. Den snævre undtagelse i § 10, stk. 2, tillader markedsføring af egne **tilsvarende** produkter til en eksisterende kunde, hvis kunden både ved afgivelsen af adressen og ved hver senere henvendelse let og gebyrfrit kan frabede sig det. Ved telefonisk henvendelse gælder desuden det selvstændige forbud i [forbrugeraftaleloven § 4](#).

Cookies. Cookiebekendtgørelsen kræver samtykke efter fyldestgørende information, før der lagres oplysninger i eller hentes oplysninger fra brugerens udstyr. Informationen er kun fyldestgørende, når den bl.a. er i klart og letforståeligt sprog, angiver formålet, identificerer alle, der foranstalter lagringen, og giver en umiddelbart tilgængelig adgang til at afslå eller tilbagekalde samtykket. Rent tekniske og nødvendige formål er undtaget efter [cookiebekendtgørelsen § 4](#). Datatilsynet fører i dag tilsyn med området og har både politianmeldt en virksomhed for ulovlig cookiebrug og fulgt op på et påbud i en sag om cookie wall, hvor tilsynet accepterede løsningen, fordi

brugere, der sagde nej, kunne få adgang til i det væsentlige tilsvarende indhold. Dybere gennemgang findes i praksisoversigten om [cookies og samtykke](#).

Samtykkets rækkevidde er snæver også her: Forbrugerombudsmanden har fastslået, at markedsføringssamtykker ikke uden videre kan overtages af et andet selskab i koncernen, og at gamle abonnentlister ikke kan genbruges til et nyt elektronisk nyhedsbrev. Grænsen mellem markedsføring og redaktionelt indhold behandles i oversigten om [skjult reklame og influencemarkedsføring](#).

LOV

[Cookiebekendtgørelsen § 3](#)[Cookiebekendtgørelsen § 4](#)[Markedsføringsloven § 2](#)[Markedsføringsloven § 10, stk. 2](#)

PRAKSIS	Forbrugerombudsmanden · Vildledende samtykkeflow: Forsikringsselskab indskræpes for aggressiv markedsføringspraksis	19.02.2024
	Forbrugerombudsmanden · Elhandelsvirksomhed krævede accept af unødvendige cookies for adgang til kundekonto: Tilsidesættelse af god skik	18.01.2022
	Forbrugerombudsmanden · Overtagelse af markedsføringssamtykker ved delvis virksomhedsoverdragelse i den finansielle sektor	08.06.2018
	Forbrugerombudsmanden · Udsendelse af elektronisk nyhedsbrev kræver aktivt samtykke i henhold til markedsføringsloven	21.07.2017

§ 8 Håndhævelse: hvem straffer hvad

Overtrædelse af betingelserne for samtykke hører til forordningens alvorligste kategori. [GDPR artikel 83, stk. 5, litra a](#) placerer "de grundlæggende principper for behandling, herunder betingelserne for samtykke, i artikel 5, 6, 7 og 9" i det øverste bødeleje: op til 20 mio. EUR eller 4 % af den samlede globale årlige omsætning.

I Danmark udmøntes det gennem [databeskyttelsesloven § 41](#). Efter stk. 1, nr. 4, straffes overtrædelse af artikel 5-7 og 9 med bøde eller fængsel indtil 6 måneder, og efter stk. 3 skal kriterierne i artikel 83, stk. 2, følges ved strafudmålingen. Datatilsynet udsteder ikke selv administrative bøder; tilsynet reagerer med kritik, alvorlig kritik, påbud og forbud og politianmelder de groveste sager, hvorefter bøden fastsættes af domstolene. Forældelsesfristen er 5 år, jf. § 41, stk. 7. Datatilsynets afgørelsespraksis er samlet i oversigten over [Datatilsynets afgørelser](#).

På markedsføringssiden er sanktionssporet mere brugt i praksis. Overtrædelse af spamforbuddet straffes med bøde efter [markedsføringsloven § 37, stk. 3](#), og bøden udmåles efter overtrædelsens **varighed eller omfang**, jf. stk. 7, nr. 2. Bødeniveauerne er reelle: et energiselskab og dets direktør blev ved Retten i Roskilde idømt henholdsvis 850.000 kr. og 200.000 kr. for uanmodet telefonsalg til 83 forbrugere og vildledning i 73 tilfælde, et elselskab vedtog en udenretlig bøde på 400.000 kr., og i en leadsag fik elselskab, callcenter og leadmægler hver 135.000 kr.

Endelig har ugyldige samtykker en civilretlig slagside: er behandlingen sket uden gyldigt grundlag, kan den registrerede kræve sletning, og efter artikel 7, stk. 2, er den del af en samtykkeerklæring, der strider mod forordningen, ikke bindende – også selv om den registrerede har underskrevet den.

LOV

[Databeskyttelsesforordningen § 83, stk. 5](#)[Databeskyttelsesloven § 41, stk. 1](#)[Markedsføringsloven § 37, stk. 3](#)

PRAKSIS	Forbrugerombudsmanden · Energiselskab idømt bøde for uanmodet telefonsalg og vildledning	30.10.2024
---------	---	------------

Forbrugerombudsmanden · Elselskab idømt bøde for uanmodet telefonsalg og vildledning	12.04.2024
Forbrugerombudsmanden · Bøde for uanmodet telefonsalg trods manglende samtykke	10.08.2020
Forbrugerombudsmanden · Bøde for overtrædelse af markedsføringsloven ved udsendelse af e-mails uden samtykke	20.05.2019

§ 9 Typiske faldgruber

Samtykke valgt, hvor en anden hjemmel var den rigtige. Mange virksomheder indhenter rutinemæssigt samtykke til behandlinger, der alligevel skal ske – fakturering, lønudbetaling, bogføring, opfyldelse af kontrakten. Samtykket er da ikke frivilligt, fordi den registrerede reelt ikke kan sige nej, og det er derfor ugyldigt. Resultatet er ikke, at man "også" har et samtykke, men at man slet intet behandlingsgrundlag har, og at behandlingen er ulovlig fra dag ét.

Forhåndsafkrydsede felter, on-slidere og passivitet. Et samtykke kræver en aktiv, utvetydig handling. Forbrugerombudsmanden har gentagne gange fastslået, at forhåndsafkrydsede felter ikke opfylder kravet – både ved online booking, ved brugeroprettelse på nyhedsmedier, i ejendomshandler og senest i 2025 over for en online tøjvirksomhed, hvor tilmelding til lagerstatus automatisk medførte et afkrydset felt til produktnyheder. Datatilsynet har tilsvarende afvist "fortsat brug af tjenesten" som gyldigt cookiesamtykke. Konsekvensen er ugyldige samtykker og en selvstændig overtrædelse af spamforbuddet, hver gang de bruges.

Samtykket bundtet med handelsbetingelser eller anden aftale. Gives samtykket samtidig med accept af generelle forretningsbetingelser, er det hverken utvetydigt eller klart adskilt fra de øvrige forhold. Forbrugerombudsmanden nåede netop dette resultat i en sag om samtykke til indsamling af betalingsoplysninger via MitID, hvor samtykket blev afgivet sammen med accepten af virksomhedens betingelser. Efter [GDPR artikel 7, stk. 2](#) er den del af erklæringen, der strider mod forordningen, desuden ikke bindende.

Samtykke gjort til adgangsbillet. Betinges adgangen til en ydelse af et samtykke, der ikke er nødvendigt for ydelsen, ryger frivilligheden. Forbrugerombudsmanden afviste således en model, hvor brugere kun kunne læse nyhedsartikler mod at give samtykke til markedsføring fra tredjeparter, og fandt det i strid med god skik, at en elhandelsvirksomhed krævede accept af markedsføringsscookies for adgang til kundens egne forbrugsdata. Omvendt kan et rabatprogram lovligt betinges af markedsføringssamtykke, når fravalg ikke har negative konsekvenser – grænsen går ved, om der findes et reelt ligeværdigt alternativ.

Ingen dokumentation – så findes samtykket ikke. Bevisbyrden ligger hos den dataansvarlige. I flere sager har virksomheder hævdet at have indhentet samtykke i butikken eller pr. telefon uden at kunne fremlægge noget som helst – og er blevet mødt med bøder, bl.a. 34.700 kr. for 347 e-mails til 74 forbrugere. Forbrugerombudsmandens spamvejledning kræver, at man kan dokumentere ikke blot at samtykket blev givet, men også under hvilke omstændigheder og med hvilken tekst; registrering af en IP-adresse er ikke nok.

Købte samtykker og leads – du hæfter selv. Køber du leads fra konkurrencesider eller lader et affiliatenetværk stå for udsendelsen, er det stadig dig, der skal kunne dokumentere et gyldigt samtykke. Forbrugerombudsmanden har politianmeldt leadvirksomheder for at sælge "falske samtykker" fra konkurrencer uden reel præmieudtrækning og har i samme sagskompleks pålagt både elselskab, callcenter og leadmægler bøder på 135.000 kr. hver. Ansaret kan ikke lægges ud til underleverandøren.

Genbrug ved formålsskift, ny afsender eller virksomhedsoverdragelse. Et samtykke dækker kun det formål og den juridiske enhed, det blev givet til. Forbrugerombudsmanden afviste, at en bank kunne overtage

markedsføringssamtykker afgivet til koncernens realkreditinstitut, fordi banken ikke havde overtaget både forretningsaktiviteter og aktiver og passiver – og fandt, at et nyt elektronisk nyhedsbrev ikke kunne sendes på grundlag af gamle tilmeldinger, der ikke var afgivet ved en aktiv handling. Skifter formålet, skal der indhentes nyt samtykke.

Samtykke fra medarbejdere og andre i afhængighedsforhold. [Databeskyttelsesloven § 12, stk. 3](#) fastslår udtrykkeligt, at samtykke kan bruges før, under og efter ansættelsen – men frivillighedskravet gælder uændret. Magtbalancen mellem arbejdsgiver og ansat gør, at et samtykke sjældent er reelt frit, hvis et nej kan opleves som karrieremæssigt risikabelt. Bygger man fx billeder på intranet, GPS-sporing eller helbredsoplysninger på medarbejdersamtykke, risikerer man, at grundlaget falder – og at man ikke har en reservehjemmel.

Tilbagetrækning gjort besværlig. Kan samtykket gives med ét klik, men kun trækkes tilbage ved brev, telefonopkald eller login bag flere niveauer, er kravet i artikel 7, stk. 3, ikke opfyldt – og markedsføringslovens krav om let og gebyrfri tilbagekaldelse heller ikke. Fortsætter udsendelsen efter en afmelding, er hver enkelt henvendelse en selvstændig overtrædelse af spamforbuddet, hvilket har udløst både indskærper og bøder.

§ 10 Relaterede dokumenter

- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn
- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Konsekvensanalyse \(DPIA\)](#) – Databeskyttelseskonsekvensanalyse efter art. 35 – hvornår den udløses, metoden og forhåndshøring af Datatilsynet
- [Handelsbetingelser \(webshop/B2C\)](#) – Vilkårene bag købsknappen – forbrugeraftalelovens oplysningskrav, fortrydelsesret og de vilkår der ikke binder
- [Ansættelseskontrakt](#) – Ansættelsesbeviset efter den nye ansættelsesbevislov – obligatoriske oplysninger, frister og godtgørelse ved mangler

REFERENCE Lovgrundlag

8 paragraffer

Cookiebekendtgørelsen § 3		Databeskyttelsesforordningen § 4	
Databeskyttelsesforordningen § 6	stk. 1	Databeskyttelsesforordningen § 7	
Databeskyttelsesforordningen § 9	stk. 2	Databeskyttelsesloven § 6	stk. 2
Databeskyttelsesloven § 41		Markedsføringsloven § 10	stk. 1

MATERIALE Citerede afgørelser

21 afgørelser

FORBRUGEROMBUDSMANDEN · NÆVN / KLAGEINSTANS

21

24.11.2025	Online tøjvirksomheds udsendelse af spam og brug af ugyldigt samtykke ved forhåndsafkrydsning
17.12.2024	Virksomheds samtykkeindhentning til betalingsoplysninger levede ikke op til krav i Betalingsloven
30.10.2024	Energiselskab idømt bøde for uanmodet telefonsalg og vildledning
12.04.2024	Elselskab idømt bøde for uanmodet telefonsalg og vildledning
19.02.2024	Vildledende samtykkeflow: Forsikringsselskab indskærpes for aggressiv markedsføringspraksis
09.01.2023	Ugyldigt forhåndsafkrydset samtykke til alarmselskab ved ejendomshandel
18.01.2022	Elhandelsvirksomhed krævede accept af unødvendige cookies for adgang til kundekonto: Tilsidesættelse af god skik
13.12.2021	Forbrugerombudsmanden undersøger leadvirksomheders brug af konkurrencer til at indhente samtykke til markedsføring
19.08.2021	Elselskab vedtager bøde for uanmodede telefoniske henvendelser trods påstået samtykke
19.08.2020	Virksomhed straffes for uanmodet elektronisk markedsføring uden samtykke
10.08.2020	Bøde for uanmodet telefonsalg trods manglende samtykke
24.07.2020	Samtykke til markedsføring som betingelse for adgang til nyheder er ikke frivilligt
21.06.2019	Betinget samtykke til markedsføring ved indmeldelse i fordelsprogram
04.06.2019	Virksomhed idømmes bøde for spamming uden gyldigt samtykke
20.05.2019	Bøde for overtrædelse af markedsføringsloven ved udsendelse af e-mails uden samtykke
08.06.2018	Overtagelse af markedsføringssamtykker ved delvis virksomhedsoverdragelse i den finansielle sektor
21.07.2017	Udsendelse af elektronisk nyhedsbrev kræver aktivt samtykke i henhold til markedsføringsloven
26.10.2015	Forhåndsafkrydset samtykkeboks til markedsføring ved online booking er ulovlig
13.07.2015	Ulovlig indhentning af samtykke til markedsføring via forhåndsafkrydset felt og manglende konkretisering
17.07.2014	Forbrugerombudsmandens krav til tydelighed ved indhentning af samtykke til markedsføring fra tredjeparter
24.05.2004	Tøjforretnings brug af børns oplysninger til direkte markedsføring: Overtrædelse af god markedsføringsskik

06

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Whistleblowerpolitik og -ordning

Den lovpligtige interne indberetningsordning for arbejdsgivere med 50+ ansatte – etablering, whistleblowerenhed, procedurer, frister og fortrolighed

Version 1 · Opdateret 21. jul. 2026 · 6 afgørelser · 2011-2024

[Læs online](#)

INTRODUKTION

En **whistleblowerpolitik** er det skriftlige styringsdokument, der beskriver arbejdspladsens interne whistleblowerordning: hvem der kan indberette, hvad der kan indberettes om, hvem der modtager og behandler indberetningen, hvilke frister der gælder, hvordan fortroligheden sikres, og hvilke rettigheder whistlebloweren og den berørte person har. Loven bruger ikke ordet "whistleblowerpolitik", men den kræver to ting, som i praksis kun kan opfyldes med ét sådant dokument: **skriftlig dokumentation** for ordningens etablering og procedurer efter § 16, og **information i klar og lettilgængelig form** til arbejdstagerne efter § 13. Justitsministeriets egne vejledninger fra 2022 anviser da også udtrykkeligt en whistleblowerpolitik som måden at opfylde dokumentationspligten på.

Parterne er fire: **arbejdsgiveren** (den juridiske enhed med eget CVR-nr., der har etableringspligten), **whistleblowerenheden** (den upartiske person eller afdeling – eventuelt en ekstern tredjepart – der modtager, følger op og giver feedback), **whistlebloweren** (som minimum arbejdstagerne, men arbejdsgiveren kan udvide kredsen til leverandører, praktikanter, tidligere ansatte m.fl.) og **den berørte person** samt enhver tredjemand nævnt i indberetningen, som har krav på præcis samme fortrolighed som whistlebloweren selv.

Oversigten er bygget op efter dokumentets naturlige rækkefølge: først hvornår pligten udløses, dernæst checklisten over hvad politikken skal indeholde med hjemmel for hvert punkt, så de typiske fejl med deres konsekvenser, og til sidst fire uddybende afsnit om parterne, anvendelsesområdet, whistleblowerenhedens uafhængighed og fortrolighedens grænser samt håndhævelsen.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Etableringspligten følger den **juridiske enhed** (eget CVR-nr.) med 50+ ansatte – ikke koncernen. Et holdingselskab med 4 ansatte og et driftsselskab med 120 er to forskellige svar.
- 02** Whistleblowerpolitikken er ikke et frivilligt HR-dokument: manglende **skriftlig dokumentation** for ordningen er selvstændigt bødelagt efter § 30, stk. 2, jf. § 16 – og juridiske personer kan straffes efter straffelovens 5. kapitel.

- 03** Whistleblowerenheden skal være **upartisk** og må ikke modtage instruks om håndteringen af den konkrete indberetning; ordningen kan outsources til en ekstern tredjepart, men ansvaret for lovopfyldelsen kan ikke.
- 04** To frister er ufravigelige og strafbelagte: **bekræftelse inden 7 dage** og **feedback senest 3 måneder** efter bekræftelsen. Den interne ordning har ikke den 6-måneders-forlængelse, som eksterne ordninger har.
- 05** Fortroligheden dækker **tre** persongrupper – whistlebloweren, den berørte person og enhver tredjemand nævnt i indberetningen – og skal være teknisk understøttet, så uautoriserede ikke kan få adgang.
- 06** § 26, stk. 5 fraviger forvaltningslovens kapitel 4-6 for identitetsoplysninger – men kun for dem. Den berørte person skal stadig partshøres over og have indsigt i sagens øvrige oplysninger.
- 07** Anonym indberetning er **valgfri** efter whistleblowerloven, men **obligatorisk** i de finansielle sektorordninger, fx [hvidvaskloven § 35, stk. 1](#).
- 08** Loven kan efter § 4 ikke fraviges ved aftale til skade for whistlebloweren eller den berørte person – en politik, en tavsheds klausul eller en fratrædelsesaftale, der lover mindre end loven, er uvirksom på det punkt.

§ 1 Hvornår er dokumentet påkrævet?

Lovpligtigt – 50 eller flere ansatte. Etableringspligten følger af [whistleblowerlovens § 9, stk. 1](#): "Arbejdsgivere med 50 eller flere ansatte skal etablere en intern whistleblowerordning". Pligten gælder både privat og offentlig sektor og påhviler den enkelte **juridiske enhed** – efter forarbejderne forstået i overensstemmelse med CVR-lovens enhedsbegreb, dvs. enhver arbejdsgiver med eget CVR-nr. Ved opgørelsen medregnes **alle** ansatte uanset beskæftigelsesgrad, som modtager vederlag for personligt arbejde i tjenesteforhold. Den offentlige sektor omfatter alt, der er omfattet af forvaltningslovens § 1, stk. 1 og 2, samt domstolene og Folketinget. Danmark har ikke udnyttet direktivets adgang til at undtage små kommuner ([whistleblowerdirektivet artikel 8, stk. 9](#)), og da samtlige danske kommuner har langt over 50 ansatte, er de alle omfattet.

Ikrafttrædelse – pligten er fuldt indfaset. Efter [§ 31](#) trådte loven i kraft 17. december 2021, mens kapitel 3 først fik virkning for private arbejdsgivere med 50-249 ansatte fra **17. december 2023**. Den overgangsperiode er udløbet: alle omfattede arbejdsgivere skal have ordningen på plads i dag.

Betinget – sektorspecifikke ordninger med langt lavere tærskel. Efter [§ 2](#) går sektorspecifikke indberetningsregler forud, og whistleblowerloven supplerer dem. En række love kræver en whistleblowerordning allerede ved **flere end fem ansatte** og med **obligatorisk anonymitet** – bl.a. [hvidvaskloven § 35](#), [lov om forsikringsformidling § 17](#), [betalingsloven § 26](#), [lov om ejendomskreditselskaber § 5 a](#) og [lov om forbrugslåns virksomheder § 13](#). Ordningen skal her være etableret senest tre måneder efter ansættelsen af den sjette ansatte. Er forpligtelsen EU-retligt begrundet, skulle også mellemstore virksomheder opfylde whistleblowerlovens krav allerede fra 17. december 2021 – uanset at de har under 250 ansatte. Justitsministeren kan desuden efter [§ 9, stk. 2](#) og en konkret risikovurdering udstrække pligten til arbejdsgivere med under 50 ansatte; bemyndigelsen forudsættes kun udnyttet i særlige tilfælde.

Frivilligt – men med en vigtig hage. Arbejdsgivere under tærsklen kan etablere en ordning frivilligt, og deres ansatte kan under alle omstændigheder indberette til den eksterne, nationale whistleblowerordning i Datatilsynet efter [§ 17, stk. 1](#). Men behandlingshjemlen i [§ 22](#) forudsætter, at ordningen er oprettet i medfør af loven. En **frivillig** ordning må derfor finde sit behandlingsgrundlag i databeskyttelseslovgivningen – og der er efter Justitsministeriets vejledning ikke hjemmel til at behandle følsomme oplysninger omfattet af [GDPR artikel 9](#) i en frivillig ordning. Den frivillige politik skal derfor afgrænses langt snævrere end den lovpligtige.

§ 2 Det skal dokumentet indeholde

1. Politikken skal angive, hvilken arbejdsgiver (juridisk enhed) ordningen dækker, og hvem der kan indberette. Som minimum skal ordningen stilles til rådighed for arbejdsgiverens arbejdstagere; arbejdsgiveren kan frivilligt udvide kredsen til fx leverandører, praktikanter, frivillige, bestyrelsesmedlemmer og tidligere ansatte. (*Lov om beskyttelse af whistleblowere § 9, stk. 1*)
2. Anvendelsesområdet skal afgrænses: overtrædelser af EU-retten omfattet af whistleblowerdirektivet samt alvorlige lovovertrædelser og øvrige alvorlige forhold – og det bør fremgå, hvad der falder udenfor (bagatelagtige forhold, almindelige samarbejdskonflikter, klassificerede oplysninger, advokaters og sundhedspersoners tavshedsbelagte oplysninger). (*Lov om beskyttelse af whistleblowere § 1*)
3. Indberetningskanalen skal beskrives konkret. Ordningen skal muliggøre skriftlig eller mundtlig indberetning eller begge dele, og gives der adgang til mundtlig indberetning, skal whistlebloweren på anmodning kunne få et fysisk møde inden for rimelig frist. (*Lov om beskyttelse af whistleblowere § 10*)
4. Whistleblowerenheden skal udpeges og fremgå af politikken – hvilken person eller afdeling, der er upartisk modtager, følger op og giver feedback. Er opgaven outsourcet til en ekstern tredjepart eller lagt hos et koncernforbundet selskab, skal også dette fremgå. (*Lov om beskyttelse af whistleblowere § 11*)
5. Politikken skal beskrive, hvordan fortroligheden om identiteten på whistlebloweren, den berørte person og enhver tredjemand nævnt i indberetningen sikres, og hvordan uautoriseret adgang forhindres – indberetninger må ikke ligge på fælles drev eller i almindeligt tilgængelige arkiver. (*Lov om beskyttelse af whistleblowere § 12, stk. 1*)
6. Sagsbehandlingsprocedurerne og de to frister skal stå eksplicit: bekræftelse på modtagelse inden 7 dage, omhyggelig opfølgning, og feedback hurtigst muligt og senest 3 måneder fra bekræftelsen. Adgangen til at afvise indberetninger uden for lovens anvendelsesområde bør også beskrives. (*Lov om beskyttelse af whistleblowere § 12, stk. 2*)
7. Registrerings- og dokumentationsreglerne skal fremgå: modtagne indberetninger skal registreres under iagttagelse af tavshedspligten, og mundtlige indberetninger skal dokumenteres ved optagelse efter samtykke eller ved nøjagtigt referat/afskrift, som whistlebloweren kan kontrollere, berigtige og acceptere. (*Lov om beskyttelse af whistleblowere § 24*)
8. Politikken skal fastlægge opbevarings- og sletteregler. Indberetninger må kun opbevares, så længe det er nødvendigt og forholdsmæssigt; der gælder ingen fast frist, men grundløse indberetninger og indberetninger uden for ordningen behøver ikke gemmes, og efter en politianmeldelse bør oplysningerne som udgangspunkt slettes, når sagen er afsluttet hos myndigheden. (*Lov om beskyttelse af whistleblowere § 23, stk. 2*)
- 9.

Behandlingen af personoplysninger skal beskrives – behandlingsgrundlaget for indberetninger samt hvordan oplysningspligt, indsigt og berigtigelse efter databeskyttelsesreglerne håndteres over for de registrerede, herunder den berørte person. (*Lov om beskyttelse af whistleblowere § 22*)

10. Den særlige, strafbelagte tavshedspligt for whistleblowerenheden og for enhver, der ved lovlig videregivelse får kendskab til oplysningerne, skal fremgå – sammen med de snævre rammer for videregivelse af identitetsoplysninger og pligten til forudgående underretning af whistlebloweren. (*Lov om beskyttelse af whistleblowere § 25*)
11. Repressalieforbuddet skal indarbejdes som en klausul: whistlebloweren, formidlere og tilknyttede tredjeparter må ikke udsættes for eller trues med repressalier, og whistlebloweren ifalder ikke ansvar for at tilsidesætte en lovbestemt tavshedspligt, når indberetningen var nødvendig for at afsløre forholdet. (*Lov om beskyttelse af whistleblowere § 8, stk. 1*)
12. Informationen skal stilles til rådighed i klar og lettilgængelig form (fx intranet eller hjemmeside) og skal både beskrive proceduren for intern indberetning med opfordring til at bruge den interne kanal først OG proceduren for ekstern indberetning til Datatilsynets nationale ordning og eventuelle sektortilsyn. (*Lov om beskyttelse af whistleblowere § 13*)

LOV

Lov om beskyttelse af whistleblowere § 1

Lov om beskyttelse af whistleblowere § 8, stk. 1

Lov om beskyttelse af whistleblowere § 9, stk. 1

Lov om beskyttelse af whistleblowere § 10

Lov om beskyttelse af whistleblowere § 11

Lov om beskyttelse af whistleblowere § 12, stk. 1, 2

Lov om beskyttelse af whistleblowere § 13

Lov om beskyttelse af whistleblowere § 22

Lov om beskyttelse af whistleblowere § 23, stk. 2

Lov om beskyttelse af whistleblowere § 24

Lov om beskyttelse af whistleblowere § 25

§ 3 Arbejdsgiver, whistleblowerenhed, whistleblower og berørt person

Arbejdsgiveren er den juridiske enhed. Forarbejderne til § 9 knytter begrebet direkte til CVR-lovens definition af en juridisk enhed – en fysisk person som arbejdsgiver, en juridisk person eller en filial af en udenlandsk juridisk person, en trust, en statslig administrativ enhed, en region, en kommune eller et kommunalt fællesskab. Konsekvensen er skarp: enhver arbejdsgiver med eget CVR-nr. og 50 eller flere ansatte har sin egen etableringspligt, og en koncerns samlede medarbejdertal er irrelevant for det enkelte selskab. Ved opgørelsen tælles alle ansatte, der modtager vederlag for personligt arbejde i tjenesteforhold, uanset om de er på fuld tid, deltid, tidsbegrænset kontrakt eller vikariat.

Whistleblowerenheden er den upartiske person eller afdeling, der efter § 11, stk. 1 modtager indberetninger, holder kontakten med whistlebloweren, følger op og giver feedback. Enheden må gerne varetage andre opgaver på arbejdspladsen, og Justitsministeriets vejledninger nævner udtrykkeligt compliance- eller HR-medarbejdere, juridiske medarbejdere, finanschefen, en ledende revisor, et bestyrelsesmedlem eller databeskyttelsesrådgiveren som mulige valg. Kravet er upartiskhed og fravær af interessekonflikter, ikke organisatorisk eller økonomisk uafhængighed. Opgaverne kan efter § 11, stk. 2 varetages af en ekstern tredjepart eller af en arbejdsgiver i et koncernforbundet selskab, og kommuner kan efter § 15 løse opgaven for hinanden eller etablere ordningen i et § 60-fællesskab.

Whistlebloweren er defineret i § 3, nr. 7 og omfatter langt mere end de nuværende ansatte: selvstændigt erhvervsdrivende, aktionærer og ledelsesmedlemmer, frivillige, praktikanter, personer der arbejder under kontrahenters og leverandørers tilsyn, tidligere ansatte og jobansøgere. Arbejdsgiveren *skal* kun stille ordningen til rådighed for sine arbejdstagere, men kan vælge at åbne den for hele kredsen – og politikken bør sige klart, hvem der er inde og hvem der er ude, for de øvrige grupper er under alle omstændigheder beskyttet, når de går til den eksterne ordning. Endelig har **den berørte person** – den, indberetningen retter sig mod – og enhver tredjemand nævnt i indberetningen krav på nøjagtig samme fortrolighed som whistlebloweren, jf. § 12, stk. 1.

LOV

Lov om beskyttelse af whistleblowere § 3

Lov om beskyttelse af whistleblowere § 9

Lov om beskyttelse af whistleblowere § 11

Lov om beskyttelse af whistleblowere § 15

§ 4 Hvad må der indberettes om – og hvad falder udenfor

Anvendelsesområdet i § 1, stk. 1 har to ben. Det første er overtrædelser af **EU-retten** inden for whistleblowerdirektivets område – offentlige udbud, finansielle tjenesteydelser, hvidvask, produktsikkerhed, transportsikkerhed, miljø, fødevarerikkerhed, folkesundhed, forbrugerbeskyttelse, databeskyttelse og konkurrence m.v. Det andet ben er nationalt og bredere: **alvorlige lovovertrædelser eller øvrige alvorlige forhold**. Justitsministeriets vejledning for whistleblowere giver en lang eksempelliste – bl.a. mandatsvig, afpresning, databedrageri, overtrædelser af skattelovgivningen og bogføringsloven, tilsidesættelse af tavshedspligter og lovbestemte handlepligter, grove eller gentagne brud på forvaltningsretlige principper, bevidst vildledning af borgere, seksuel og grov chikane, omsorgssvigt og alvorlige it-uregelmæssigheder.

Det, der falder **udenfor**, er lige så vigtigt at skrive ind i politikken. Vejledningen nævner oplysninger af bagatelagtig karakter og overtrædelser af interne retningslinjer om sygefravær, rygning, alkohol, påklædning eller privat brug af kontorartikler – samt oplysninger om whistleblowerens eget ansættelsesforhold, herunder konflikter mellem medarbejdere, samarbejdsvanskeligheder og forhold, der hører under det fagretlige system. Undtagelsen fra undtagelsen er, at seksuel chikane og anden grov chikane **er** omfattet, at systematiske overtrædelser af interne retningslinjer kan miste deres bagatelkarakter, og at samarbejdsvanskeligheder mellem medarbejdere i kritiske funktioner kan udgøre et alvorligt forhold, hvis de skaber reel risiko for menneskers liv og helbred.

§ 1, stk. 3 undtager desuden fem kategorier helt: klassificerede oplysninger omfattet af sikkerhedscirkulæret, som samtidig er fortrolige efter [straffelovens § 152, stk. 3](#), oplysninger omfattet af advokaters tavshedspligt efter [retsplejelovens § 129](#), oplysninger omfattet af sundhedspersoners tavshedspligt efter [sundhedslovens § 40](#), oplysninger om rettens rådslagning og afstemning samt sager inden for strafferetsplejen. Falder en indberetning uden for anvendelsesområdet, kan enheden afvise den efter § 12, stk. 3 uden pligt til at videresende – men whistlebloweren bør oplyses om afvisningen og vejledes om, hvor vedkommende i stedet kan gå hen. Er der tale om en offentlig arbejdsplads, kan der efter omstændighederne bestå en almindelig forvaltningsretlig undersøgelsespligt, uanset hvordan myndigheden er blevet opmærksom på forholdet.

LOV

Lov om beskyttelse af whistleblowere § 1

Lov om beskyttelse af whistleblowere § 12, stk. 3

Retsplejeloven § 129

Straffeloven § 152, stk. 3

§ 5

Upartiskhed, frister og outsourcing af ordningen

Kravet om **upartiskhed** i § 11 betyder efter Justitsministeriets vejledninger, at de udpegede personer skal forholde sig objektivt og sagligt, uanset hvem indberetningen handler om, og at arbejdspladsen ved udpegningen skal tage højde for, at der ikke opstår interessekonflikter. Vejledningen skærper det ét sted: arbejdspladsen skal sikre, at enheden **i forhold til den konkrete sagsbehandling er uafhængig af den daglige ledelse** – ledelsen må ikke instruere eller beordre enheden til at håndtere en indberetning på en bestemt måde. Til gengæld skal arbejdspladsen fastsætte *generelle* retningslinjer og procedurer for sagsbehandlingen. På offentlige arbejdspladser skal procedurerne desuden sikre, at forvaltningslovens regler og de ulovbestemte principper om habilitet overholdes i den enkelte sag.

Fristerne i § 12, stk. 2 er de mest håndfaste krav i hele ordningen. Bekræftelse på modtagelsen skal ske **inden for 7 dage**, der skal følges omhyggeligt op, og feedback skal gives hurtigst muligt og **senest 3 måneder** fra bekræftelsen. Feedback betyder efter vejledningen, at enheden i videst muligt omfang oplyser, hvilke tiltag der er iværksat eller påtænkes, og hvorfor – inden for rammerne af tavshedspligter og databeskyttelsesreglerne. Er der åbnet for anonyme indberetninger, skal modtagelsen også bekræftes, hvis det teknisk kan lade sig gøre.

Outsourcing er udtrykkeligt tilladt efter § 11, stk. 2, og både indberetningsplatformsudbydere, advokater og revisorer kan bruges. Men arbejdsgiveren kan ikke fraskrive sig sine forpligtelser: det forudsættes, at tredjeparten afgiver en **skriftlig garanti** for at overholde lovens krav om uafhængighed, fortrolighed, databehandling og tavshedspligt, og vejledningen anbefaler, at der alligevel udpeges en intern kontaktperson, som kan indhente oplysninger og forberede beslutninger om reaktioner. Datatilsynet har i en udtalelse af 13. oktober 2021 (j.nr. 2021-211-6947) behandlet netop spørgsmålet om, hvem der er dataansvarlig ved outsourcing af en intern whistleblowerordning – og svaret afgør, om der skal indgås en databehandlaftale efter [GDPR artikel 28](#). Se også oversigten over [Datatilsynets afgørelser](#) og [databeskyttelse i ansættelsesforhold](#).

LOV

Lov om beskyttelse af whistleblowere § 11, stk. 2

Lov om beskyttelse af whistleblowere § 12, stk. 2

Lov om beskyttelse af whistleblowere § 14

PRAKSIS Datatilsynet · Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning?

13.10.2021

§ 6 Fortrolighed, tavshedspligt og forholdet til forvaltningsloven og GDPR

Whistleblowerloven opstiller et **særligt tavshedspligtsregime**. Efter § 25 har den, der er udpeget til at modtage og følge op på indberetninger, tavshedspligt om de oplysninger, der indgår heri – og tavshedspligten smitter af på enhver, der ved lovlig videregivelse efter § 26 får kendskab til oplysningerne, samt på uautoriserede medarbejdere ved eksterne ordninger, der utilsigtet får kendskab til dem. Brud straffes med bøde ved forsæt eller grov uagtsomhed, jf. § 30, stk. 1, nr. 1. At tavshedspligtbrud i det hele taget tages alvorligt i praksis, illustreres af Østre Landsrets dom af 25. marts 2021 om videregivelse af fortrolige oplysninger og misbrug af stilling efter straffelovens §§ 152 og 155. Se nærmere oversigten om [tavshedspligt](#).

§ 26 beskytter identiteten særskilt. Oplysninger, hvoraf whistleblowerens identitet direkte eller indirekte kan udledes, må uden udtrykkeligt samtykke kun videregives til autoriserede medarbejdere i whistleblowerenheden – og til anden offentlig myndighed, når det sker for at imødegå overtrædelser eller for at sikre berørte personers ret til et forsvar. Whistlebloweren skal underrettes forud for en sådan videregivelse, medmindre

underretningen vil bringe undersøgelser eller retssager i fare. Og efter **stk. 5** finder [forvaltningslovens kapitel 4-6](#) om partsaktindsigt, partshøring og begrundelse **ikke** anvendelse på identitetsoplysningerne. Fravigelsen er snæver: den berørte person skal fortsat partshøres over og have indsigt i sagens **øvrige** oplysninger, og begrundelsen skal redegøre for de faktiske omstændigheder – blot uden det, der kan afsløre whistlebloweren. I den praktiske afvejning af, hvornår identitetsoplysninger kan holdes tilbage på grund af repressalierisiko, er Folketingets Ombudsmands udtalelse FOB 2024-29 illustrativ: ombudsmanden tilsidesatte ikke en styrelses vurdering af, at der forelå afgørende hensyn efter forvaltningslovens § 15 b, nr. 5, til at undlade partshøring over oplysninger, der kunne identificere den, der havde indberettet til en whistleblowerordning. Omvendt viser FOB 2020-44 om aktindsigt i Forsvarsministeriets whistleblowerordning, at generelle betragtninger om ordningens karakter ikke i sig selv rækker som begrundelse for at undtage oplysninger. Se videre i oversigterne om [partshøring](#) og [aktindsigt](#).

Databeskyttelsesretligt giver [§ 22](#) hjemmel til at behandle personoplysninger – også følsomme oplysninger og oplysninger om strafbare forhold – når det er nødvendigt for at behandle indberetninger i en ordning oprettet i medfør af loven, og bestemmelsen går forud for behandlingsreglerne i databeskyttelseslovgivningen. Alle øvrige regler gælder dog fortsat: behandlingsprincipperne, behandlingssikkerheden efter [GDPR artikel 32](#) og de registreredes rettigheder. Oplysningspligten over for den berørte person kan som følge af den særlige tavshedspligt undlades efter [GDPR artikel 14, stk. 5, litra d](#), og indsichtsretten kan efter en konkret vurdering begrænses efter [databeskyttelseslovens § 22](#). Endelig gælder efter [§ 23](#), at indberetninger skal registreres og kun må opbevares, så længe det er nødvendigt og forholdsmæssigt – der er ingen fast frist, men heller ingen adgang til at gemme grundløse indberetninger i det uendelige.

LOV

[Databeskyttelsesloven § 22](#)[Lov om beskyttelse af whistleblowere § 22](#)[Lov om beskyttelse af whistleblowere § 23](#)[Lov om beskyttelse af whistleblowere § 25](#)[Lov om beskyttelse af whistleblowere § 26, stk. 5](#)

PRAKSIS

Landsretten · Stadfæstelse af dom for videregivelse af fortrolige oplysninger og misbrug af stilling

25.03.2021

Håndhævelse: bøder for arbejdsgiveren og godtgørelse til whistlebloweren

§ 7

Whistleblowerloven har **to** håndhævelsesspor, og en whistleblowerpolitik skal tage højde for begge.

Det første er **strafansvaret for arbejdsgiveren**. Efter [§ 30, stk. 2](#) straffes med bøde en arbejdsgiver omfattet af § 9, der ikke lever op til forpligtelserne efter [§ 10](#) (indberetningskanalen), § 11 (whistleblowerenheden), § 12, stk. 1 eller 2 (fortrolighed og procedurer), § 13 (informationspligten) eller § 16 (dokumentationspligten). Juridiske personer kan straffes efter straffelovens 5. kapitel, jf. [§ 30, stk. 3](#). Bemærk hvad der **ikke** er med i bødebestemmelsen: ressourcodeling efter § 14, kommunale fællesordninger efter § 15 og registrerings- og dokumentationsreglerne i §§ 23-24. Til gengæld er dokumentationspligten i § 16 selvstændigt strafsanktioneret – efter forarbejderne netop for at lette en eventuel efterforskning af anmeldelser om manglende ordning. Det er dette forhold, der gør den skriftlige whistleblowerpolitik til et retligt nødvendigt dokument og ikke blot god skik.

Det andet spor er **whistleblowerens civilretlige krav**. Efter [§ 8](#) må whistlebloweren – og formidlere, tilknyttede tredjeparter samt virksomheder, whistlebloweren ejer eller arbejder for – ikke udsættes for repressalier eller trusler herom. Sker det alligevel, giver [§ 28](#) krav på godtgørelse, og en afskedigelse i strid med § 8, stk. 1,

skal underkendes med krav på genansættelse, medmindre det efter en interesseafvejning er åbenbart urimeligt. Afgørende er bevisbyrdereglen i § 29: beviser whistlebloweren at have indberettet og lidt en ulempe, påhviler det **arbejdsgiveren** at bevise, at ulempen ikke var repressalier. Københavns Byret anvendte i dom af 2. oktober 2024 (BS-33549/2023-KBH) netop §§ 8, 28 og 29 og tilkendte en medarbejder godtgørelse for repressalier efter en whistleblower-indberetning. Allerede før lovens tilblivelse blev der tilkendt godtgørelse i en landsretssag fra 2013 om opsigelse af en kvalitetschef efter en intern indberetning om miljøforhold, og en landsretsdom fra 2011 om erhvervsbedrageri og hvidvask viser, at trusler mod en whistleblower også kan have et strafferetligt efterspil.

Hertil kommer ansvarsfriheden i § 7: whistlebloweren anses ikke for at have tilsidesat en lovbestemt tavshedspligt og ifalder heller ikke ansvar for at have skaffet sig adgang til de indberettede oplysninger – forudsat god tro efter § 6, og at anskaffelsen ikke i sig selv er strafbar. Da loven efter § 4 ikke kan fraviges ved aftale til skade for whistlebloweren, afskærer hverken en tavsheds klausul i ansættelseskontrakten, en NDA eller en fratrædelsesaftale den ansatte fra at indberette. Uddybende praksis om beskyttelsen findes i oversigterne om [whistleblowerbeskyttelse](#), [offentligt ansattes ytringsfrihed](#) og [loyalitetspligt](#) og [forretningshemmeligheder](#).

LOV	Lov om beskyttelse af whistleblowere § 7	Lov om beskyttelse af whistleblowere § 8
	Lov om beskyttelse af whistleblowere § 28	Lov om beskyttelse af whistleblowere § 29
	Lov om beskyttelse af whistleblowere § 30, stk. 2	
PRAKSIS	Landsretten · Ansættelsesretlig godtgørelse til whistleblower: Opsigelse af kvalitetschef fundet ulovlig efter intern indberetning om miljøforhold 14.08.2013	
	Landsretten · Landsretsdom om omfattende erhvervsbedrageri, grov hvidvask og trusler mod whistleblower 03.03.2011	
	Byretten · Medarbejder tilkendt godtgørelse for repressalier efter whistleblower-indberetning 02.10.2024	

§ 8 Typiske faldgruber

Koncernfælles ordning uden hensyn til det enkelte CVR-nummer. Etableringspligten ligger på den enkelte juridiske enhed, og forarbejderne til § 9 knytter arbejdsgiverbegrebet direkte til CVR-lovens enhedsbegreb. Koncernfælles ordninger er tilladt efter § 9, stk. 3, og private virksomheder med 50-249 ansatte må efter § 14 dele ressourcer om modtagelse og undersøgelser – men delingen omfatter hverken feedback til whistlebloweren eller imødegåelse af overtrædelsen. Hvert selskab skal derfor selv kunne dokumentere sin egen enhed og sine egne procedurer, ellers er der tale om en bødebelagt mangel efter § 30, stk. 2.

HR som whistleblowerenhed uden reelt uafhængighedsværn. Justitsministeriets vejledninger tillader udtrykkeligt, at funktionen placeres hos en HR- eller compliance-medarbejder, en juridisk medarbejder, en ledende revisor eller databeskyttelsesrådgiveren. Fejlen opstår, når politikken ikke sikrer, at enheden i den konkrete sagsbehandling er uafhængig af den daglige ledelse – ledelsen må ikke instruere om håndteringen af en enkelt indberetning – og når der ikke er en plan for indberetninger, der handler om HR-chefen, direktionen eller enheden selv. Uden det er upartiskhedskravet i § 11, stk. 1 ikke opfyldt, og medarbejderne bruger reelt ikke kanalen.

Fristerne behandles som ordensforskrifter. 7-dagesbekræftelsen og 3-måneders-feedbacken i § 12, stk. 2 løber uanset ferie, advokatundersøgelser og verserende politisager, og den interne ordning har ikke den forlængelse til 6 måneder i behørigt begrundede tilfælde, som gælder for eksterne ordninger efter § 20, stk. 2. Overskridelse

er både bødebelagt og åbner efter [§ 5, stk. 2, nr. 1](#) for, at whistlebloweren kan gå til offentligheden med fuld beskyttelse.

Politikken lover mere fortrolighed, end loven kan holde. Efter [§ 26, stk. 2](#) kan identitetsoplysninger videregives uden samtykke til anden offentlig myndighed for at imødegå overtrædelser eller for at sikre berørte personers ret til et forsvar. En politik, der lover ubetinget hemmeligholdelse, giver et falsk løfte – og i personrelaterede konflikter kan sagen ofte slet ikke oplyses forsvarligt, medmindre whistlebloweren samtykker til, at identiteten videregives. Det bør politikken sige ærligt, så whistlebloweren kan træffe et informeret valg.

Anonymitet loves, men systemet understøtter den ikke. Whistleblowerloven kræver ikke, at der kan indberettes anonymt – det er valgfrit for den enkelte arbejdsplads. Men loves anonymitet i politikken, skal kanalen faktisk kunne levere den, herunder uden IP-logning og med mulighed for anonym tovejskommunikation, så enheden kan stille opfølgende spørgsmål. I de finansielle sektorordninger, fx [hvidvaskloven § 35, stk. 1](#), er anonymitet derimod et ufravigeligt krav, og en fælles koncernpolitik skal derfor honorere den strengeste af de to standarder.

Frivillig ordning under 50 ansatte uden behandlingsgrundlag. Behandlingshjemlen i [§ 22](#) forudsætter, at arbejdsgiveren er forpligtet til at have ordningen, og at den er oprettet i medfør af loven. En mindre arbejdsplads, der frivilligt kopierer en standardpolitik, står derfor uden hjemmel til at behandle følsomme oplysninger og oplysninger om strafbare forhold ud over det, databeskyttelseslovgivningen selv giver. Resultatet er en ordning, der i sig selv er en databeskyttelsesretlig overtrædelse.

Outsourcing uden databehandleraftale og skriftlig garanti. Anvendes en ekstern indberetningsplatform, advokat eller revisor efter [§ 11, stk. 2](#), forbliver arbejdsgiveren ansvarlig for, at ordningen lever op til loven, og det forudsættes, at tredjeparten afgiver en skriftlig garanti om uafhængighed, fortrolighed, databehandling og tavshedspligt. Datatilsynet har i sin udtalelse om outsourcing af interne whistleblowerordninger (j.nr. 2021-211-6947) taget stilling til rollefordelingen mellem dataansvarlig og databehandler – mangler databehandleraftalen, er både arbejdsgiver og leverandør eksponeret.

Ordningen bruges som almindelig HR-postkasse – eller afviser for meget. Bagatelagte forhold og almindelige samarbejdsconflikter falder uden for [§ 1, stk. 1](#), og enheden kan afvise dem efter [§ 12, stk. 3](#) uden pligt til at videresende. Men seksuel chikane og anden grov chikane ER omfattet, og systematiske overtrædelser af interne retningslinjer kan miste deres bagatelkarakter. En politik, der pr. automatik afviser alt om "eget ansættelsesforhold", rammer derfor forkert i begge retninger – og den manglende visitering er samtidig et brud på pligten til omhyggelig opfølgning.

§ 9 Relaterede dokumenter

- [Personalehåndbog](#) – Virksomhedens interne regelsæt – hvad der binder, hvad der kræver varsel at ændre, og de lovpligtige politikker indeni
- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn

- [Ansættelseskontrakt](#) – Ansættelsesbeviset efter den nye ansættelsesbevislov – obligatoriske oplysninger, frister og godtgørelse ved mangler
- [Fortrolighedsaftale \(NDA\)](#) – Hemmeligholdelsesaftalen før forhandlinger og samarbejder – og dens samspil med forretningshemmelighedsloven
- [Fratrædelsesaftale](#) – Den forhandlede afslutning af ansættelsen – fritstilling, godtgørelser, fuld og endelig afgørelse og skattefælder

REFERENCE Lovgrundlag

8 paragraffer

Hvidvaskloven § 35 stk. 1	Lov om beskyttelse af whistleblowere § 9 stk. 1
Lov om beskyttelse af whistleblowere § 11	Lov om beskyttelse af whistleblowere § 12 stk. 2
Lov om beskyttelse af whistleblowere § 13	Lov om beskyttelse af whistleblowere § 16
Lov om beskyttelse af whistleblowere § 26 stk. 5	Lov om beskyttelse af whistleblowere § 30 stk. 2

MATERIALE Citerede afgørelser

6 afgørelser

LANDSRET TEN · ANKEINSTANS		3
25.03.2021	Stadfæstelse af dom for videregivelse af fortrolige oplysninger og misbrug af stilling	1412-1716
14.08.2013	Ansættelsesretlig godtgørelse til whistleblower: Opsigelse af kvalitetschef fundet ulovlig efter intern indberetning om miljøforhold	RA-2012-521-2019
03.03.2011	Landsretsdom om omfattende erhvervsbedrageri, grov hvidvask og trusler mod whistleblower	
BYRET TEN · FØRSTE INSTANS		1
02.10.2024	Medarbejder tilkendt godtgørelse for repressalier efter whistleblower-indberetning	10098-11839
DATATILSYNET · NÆVN / KLAGEINSTANS		1
13.10.2021	Hvem er dataansvarlig ved outsourcing af en intern whistleblowerordning?	2021-211-6947
PARKERINGSKLAGENÆVNEN · NÆVN / KLAGEINSTANS		1
05.07.2022	Tvist om manglende p-tilladelse og utilstrækkelig skiltning på Refshaleøen	park-1716