

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 fortegnelser 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 ryggrad:** 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 indsigtsret efter artikel 15, men offentlige myndigheds 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 databehandleraftalens 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 modenhetstilsyn 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 Forenklingsstyrelsens 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 indsichtsret	
03.06.2019	Alvorlig kritik og bødeindstilling til IDdesign for overtrædelse af princippet om opbevaringsbegrænsning	2018-41-0015