

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 kundeventde 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

§ 3 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.

Lagdelt 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 kundeorienterede 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 politikkens 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 kundeventd 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