Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 9

Ansvarlighed og dokumentation

Jesper Løffler Nielsen & Helene Arensbak Mørk

9.1. Introduktion

Vi har i mange år oplevet en stadigt stigende digitalisering af alle dele af vores private og professionelle liv, og denne udvikling ser ud til at fortsætte. Dette medfører et behov for at stille høje krav til det ansvar, der påhviler dem, der behandler vores personoplysninger. Ikke mindst fordi det kan have store konsekvenser, hvis vores oplysninger ikke behandles sikkert og korrekt.

De grundlæggende principper for behandling af personoplysninger i persondataforordningens artikel 5, stk. 1, er behandlet i bogens kapitel 5. I dette kapitel er fokus først og fremmest på *princippet om ansvarlighed* i artikel 5, stk. 2, der har følgende ordlyd: "Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (ansvarlighed)".

Kapitlet gennemgår, hvordan princippet om ansvarlighed kommer til udtryk i forordningens øvrige bestemmelser, og hvilke krav det stiller til den dataansvarliges udarbejdelse af dokumentation.

9.2. Princippet om ansvarlighed

Princippet om ansvarlighed er en af de mest fundamentale forpligtelser i forordningen, men også en af de vanskeligste at beskrive det præcise indhold af.

Selvom det er første gang, forordningen direkte anvender begrebet "Ansvarlighed", er begrebet ikke som sådan nyt. Begrebet har tidligere været anvendt i internationale regler og standarder, og allerede i 2010 udarbejdede Artikel 29-Gruppen en anbefaling om at introducere begrebet til de EU-retlige regler om databeskyttelse.[1] Denne opfordring blev som bekendt fulgt, og i de følgende afsnit ser vi nærmere på princippets indhold.

9.2.1. Det handler om at tage sine forpligtelser seriøst

Overordnet indebærer princippet om ansvarlighed, at man som dataansvarlig ikke blot kan anskue forordningens krav som noget, juristerne sætter sig ned og får styr på én gang for alle. Arbejdet med databeskyttelse skal være *proaktivt*, *reelt* og *kontinuerligt*. I det følgende uddybes konkrete eksempler på, hvad der nærmere ligger heri.

9.2.1.1. Overblik over behandlingen af personoplysninger

Det første og væsentligste skridt er at få overblik over, *hvilke* personoplysninger man som dataansvarlig behandler, og ikke mindst *hvorfor* og *hvordan* man behandler dem.

En del af dette overblik får man ved at udarbejde de lovpligtige fortegnelser over behandlingsaktiviteter (se afsnit 9.3.1.1. nedenfor), men det vil ofte være nødvendigt at supplere fortegnelserne med yderligere kortlægning eller oversigter over datastrømme.

9.2.1.2. Implementering af passende foranstaltninger

At databeskyttelse ikke er en skrivebordsøvelse, indebærer bl.a., at det ofte vil være relevant at sikre overholdelse af reglerne ved at implementere politikker og procedurer på flere niveauer i den dataansvarliges organisation, jf. nærmere nedenfor i afsnit 9.3.

Også andre foranstaltninger kan være relevante, herunder tekniske og fysiske. Afgørelsen af, hvilke foranstaltninger der er nødvendige, må foretages af den enkelte dataansvarlige og skal tage udgangspunkt i en vurdering af *risikoen* forbundet med de enkelte behandlingsaktiviteter.

1. Artikel 29-Gruppen WP 173.

9.2.1.3. Ansvar, awareness og uddannelse

Ansvarlighed forudsætter dernæst, at der internt i en organisation er en klar fordeling af, hvem der har ansvaret for hvad. Denne ansvarsfordeling bør afspejle sig i de politikker og procedurer, som bliver udarbejdet, jf. forrige afsnit.

Selvom der i en organisation er udpeget en eller flere personer, som har ansvaret for at sikre overholdelse af reglerne, kan dette ikke stå alene. I langt de fleste organisationer kan reglerne alene overholdes, såfremt budskabet bredes ud til de øvrige medarbejdere også.

Der er selvsagt stor forskel på, hvor meget den enkelte person behøver at kende til reglerne og de interne politikker og procedurer; jo mere den enkelte person arbejder med personoplysninger, jo mere har personen behov for at vide om de konsekvenser, som databeskyttelsesreglerne har for dette arbejde.

9.2.1.4. Databeskyttelse skal tænkes ind i den daglige drift

Forordningen indeholder også i artikel 25 en udtrykkelig forpligtelse til at sikre databeskyttelse gennem design og standardindstillinger. Princippet uddybes nedenfor i kapitel 14, men til dette skal blot fremhæves, at man som dataansvarlig er forpligtet til at tænke databeskyttelse ind i alle sine arbejdsgange og it-systemer.

9.2.1.5. Opfølgning og kontroller

Sidst, men ikke mindst indebærer ansvarlighedsprincippet også, at arbejdet med databeskyttelse er en løbende forpligtelse.

Når alle ovenstående skridt er foretaget, er man således forpligtet til at følge op med rimelige intervaller, og efter omstændighederne bør man også udføre stikprøvekontroller med henblik på at sikre, at de interne retningslinjer rent faktisk bliver efterlevet. Dette kan den dataansvarlige bl.a. sikre ved at udarbejde et årshjul eller lignende oversigt, der fastlægger (og dokumenterer), hvornår de forskellige politikker og procedurer kontrolleres både i indhold og overholdelse.

9.3. Kravet om dokumentation

Selvom mange af de materielle krav i persondataforordningen er en videreførelse af regler, vi kender, er der sket et grundlæggende paradig-

meskifte i relation til måden, hvorpå vi skal overholde kravene. Det er således ikke længere tilstrækkeligt for den dataansvarlige at overholde reglerne, idet man med forordningen også skal være i stand til at *påvise* denne overholdelse.

I persondataloven eksisterede der en såkaldt anmeldelsespligt, hvorefter såvel offentlige som private dataansvarlige for visse behandlingsaktiviteter var forpligtede til at foretage anmeldelse af behandlingen til Datatilsynet forud for iværksættelsen. Denne pligt er nu afskaffet til fordel for et skærpet krav til den dokumentation, som den dataansvarlige (og i visse tilfælde databehandlere) skal kunne fremvise, hvis f.eks. Datatilsynet anmoder om det. Dette vil blive gennemgået nærmere nedenfor under pkt. 9.3.1.

Ændringen skal ses i sammenhæng med tilsynsmyndighedernes nye rolle på databeskyttelsesområdet, herunder udvidede beføjelser, der i langt højere grad end tidligere vil komme til udtryk i form af både fysiske og skriftlige tilsyn. Se mere herom i kapitel 16.

Modsat anmeldelsespligten, der skulle opfyldes én gang for alle forud for den pågældende databehandling, er der nu tale om en forpligtelse til til enhver tid at være i stand til at fremvise den nødvendige dokumentation, hvilket stiller betydeligt højere krav til den dataansvarlige end tidligere.

Persondataforordningens artikel 5, stk. 2, indeholder imidlertid ingen krav til, *hvordan* den dataansvarlige skal påvise sin overholdelse af stk. 1. Dette kan derimod udledes andre steder i forordningen, særligt i artikel 24, stk. 2, om den dataansvarliges ansvar. Det fremgår af denne bestemmelse, at "hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker".

Der kan i forlængelse heraf henvises til præambel 78, som ligeledes fremhæver interne politikker som en måde, hvorpå den dataansvarlige kan påvise sin overholdelse af forordningen; "For at kunne påvise overholdelse af denne forordning bør den dataansvarlige vedtage interne politikker og gennemføre foranstaltninger, som især lever op til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger".

Som det ses flere steder i forordningen, er der også her tale om en risikobaseret tilgang. Der skal foretages en konkret vurdering af den dataansvarliges behandlingsaktiviteter og på den baggrund tages stilling til, hvad der for den pågældende må anses for *passende* databeskyttelsespolitikker.

9.3.1. Eksempler på dokumentation

Da databeskyttelsespolitikker flere steder i forordningen fremhæves som værende en måde for den dataansvarlige at sikre dokumentation for sin overholdelse af forordningen på, gennemgås nedenfor en række eksempler på, hvordan dette kan gribes an i praksis.

9.3.1.1. Kortlægning og fortegnelse

En kortlægning er ikke et udtrykkeligt krav efter forordningen, men som nævnt ovenfor kan det være en god øvelse for den dataansvarlige med henblik på bl.a. at få overblik over, hvilke oplysninger organisationen behandler og hvorfor, hvor længe oplysningerne behandles, hvor de kommer fra, hvem de deles med osv.

Kortlægningen kan udarbejdes i det format, der passer bedst til den dataansvarliges behov og temperament. Der kan således anvendes alt fra et simpelt Word-dokument til større softwareløsninger udviklet til formålet. Det vigtigste er, at kortlægningen giver den dataansvarlige det nødvendige overblik over, hvilke forpligtelser organisationens behandling af personoplysninger bliver omfattet af.

Hvad der derimod er et udtrykkeligt krav efter forordningen, er såvel den dataansvarliges som databehandlerens pligt til at udarbejde en *fortegnelse* i overensstemmelse med artikel 30. Det er i denne bestemmelse oplistet præcis, hvilke oplysninger en fortegnelse for henholdsvis den dataansvarlige (stk. 1) og databehandleren (stk. 2) skal indeholde.

Ifølge artikel 30, stk. 3, skal fortegnelsen "[...] foreligge skriftligt, herunder elektronisk". Fortegnelsen er et internt dokument, der dog efter anmodning stilles til rådighed for tilsynsmyndigheden, jf. artikel 30, stk. 4.

Der er enkelte tilfælde, der er undtaget kravet om fortegnelse. Der er dog tale om en snæver undtagelse. Ifølge artikel 30, stk. 5, skal "et foretagende eller en organisation" med under 250 ansatte ikke føre fortegnelser over behandlingsaktiviteter, medmindre (1) behandlingen af

personoplysninger sandsynligvis vil medføre en risiko for registreredes rettigheder, (2) behandlingen ikke er lejlighedsvis eller (3) behandlingen omfatter følsomme personoplysninger efter artikel 9 eller personoplysninger vedrørende straffedomme og lovovertrædelser efter artikel 10.

Kan der svares bekræftende på blot én af ovenstående tre indskrænkninger i undtagelsen til at føre fortegnelse, skal der føres fortegnelse.

At der skal være tale om "et foretagende eller en organisation", udelukker offentlige myndigheder, der således altid vil være omfattet af kravet om at føre en fortegnelse.

I artikel 4, nr. 18, defineres et *foretagende* som "en fysisk eller juridisk person, som udøver økonomisk aktivitet, uanset dens retlige status, herunder partnerskaber eller sammenslutninger, der regelmæssigt udøver økonomisk aktivitet". Ifølge Datatilsynet er der her tale om virksomheder.[2]

9.3.1.2. Interne politikker og procedurer

Som nævnt ovenfor fremgår det i hvert fald af artikel 24, stk. 2, at den dataansvarlige bør overveje relevante politikker og procedurer for sin behandling af personoplysninger under hensyntagen til, hvad der for den pågældende behandling kan anses for passende.

På et overordnet plan vil det ofte være relevant at udarbejde en *generel intern persondatapolitik*, der fastlægger, hvordan den dataansvarlige har indrettet sig med henblik på at overholde de forpligtelser, den pågældende er underlagt i forordningen. Det vil med fordel også fremgå heraf, hvilke forventninger den dataansvarlige har til sine ansattes behandling af organisationens data, herunder relevante procedurer for bl.a. håndtering af databrud eller henvendelser fra registrerede.

For så vidt angår databrud, stiller forordningen i øvrigt direkte krav om, at "den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt".

2. Datatilsynet 2018f, s. 14

Den generelle interne persondatapolitik vil fungere som fundament for organisationens øvrige politikker og procedurer relateret til behandling af personoplysninger, herunder også fordeling af ansvar. Afhængig af organisationens størrelse og karakter kan det desuden være passende med supplerende dokumenter, f.eks. it-sikkerhedspolitik samt procedurer for sletning og udarbejdelse af konsekvensanalyser.[3]

9.3.1.3. Eksterne politikker

Dokumentation i form af eksterne politikker har også stor betydning for overholdelse af forordningens krav. Går man f.eks. tilbage til de grundlæggende principper for behandling af personoplysninger, finder man bl.a. princippet om gennemsigtighed i artikel 5, stk. 1, litra a, der forpligter den dataansvarlige til at behandle oplysningerne på en for den registrerede gennemsigtig måde, herunder ved at sikre, at den registrerede er bekendt med, hvem der behandler dennes oplysninger og hvordan[4]. Dette kommer i særdeleshed til udtryk i forordningens kapitel III om den registreredes rettigheder, navnlig artikel 13 og 14 om oplysningspligten.[5]

Også behandlingsgrundlaget *samtykke* i artikel 6 og 9, som er omtalt ovenfor i kapitel 6, stiller krav om dokumentation. Ifølge artikel 7, stk. 1, skal den dataansvarlige således kunne påvise den registreredes samtykke, hvis han har baseret sin behandling på dette grundlag.

9.3.1.4. Databehandlere

Endelig skal kort nævnes kravet i artikel 28, hvorefter der skal indgås en skriftlig databehandleraftale, der lever op til en lang række materielle krav, med alle databehandlere.

Foruden selve aftalen, der i sig selv udgør dokumentation, kan det for mange organisationer desuden være relevant at føre en skematisk oversigt eller lignende til at sikre overblik over sine databehandlere, herunder kommende og gennemførte tilsyn med disse.[6]

---

3. Se mere om konsekvensanalyser i kapitel 12.
4. Se mere om princippet om gennemsigtighed i afsnit 5.3.2.3.
5. Se mere om de registreredes rettigheder i kapitel 13.
6. Se mere om håndtering af databehandlere i kapitel 10.

9.3.2. Andre gode grunde til at sikre løbende dokumentation

Udover at leve op til eksplicitte krav i forordningen kan dokumentation også fungere som et forebyggende værktøj med henblik på at undgå store bøder, ligesom det overordnet set gør hverdagen lettere for den dataansvarlige.[7]

En procedure for de ansattes håndtering af databrud fungerer f.eks. både som retningslinjer, således at processen glider lettere, hvorved det bliver nemmere at overholde de stramme tidsfrister i artikel 12, og i særdeleshed også som dokumentation for den dataansvarliges indsats. Der vil blive set på en eventuel overtrædelse med mildere øjne, hvis den dataansvarlige har gjort en reel indsat, fremfor ikke at have forholdt sig til kravene overhovedet.

Arbejdet lettes i særdeleshed også i forbindelse med et eventuelt tilsyn fra Datatilsynet, hvis den dataansvarlige har sikret løbende dokumentation for sit arbejde med databeskyttelse i organisationen. Der er bl.a. set eksempler på, at der med meget kort frist skal svares på, hvordan den dataansvarlige har sikret at instruere sine medarbejdere tilstrækkeligt om databeskyttelse, herunder hvornår dette sidst er sket, hvor ofte det sker og med hvilke konkrete midler.

7. Jf. særligt artikel 83, stk. 2, litra d.