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 5

De overordnede principper for databehandling

Ayo Næsborg-Andersen

5.1. Indledning

Persondataretten kan for en uindviet se voldsomt kompliceret ud med en mængde detailregler, der kan være svære at holde styr på. Der er dog en håndfuld røde tråde i form af grundlæggende principper, som går igennem hele forordningen. Hvis man har styr på disse principper, bliver det væsentligt nemmere at forstå logikken i resten af reglerne, og man vil i meget høj grad kunne ræsonnere sig frem til en rimelig fortolkning, også på de punkter, hvor der måske (endnu) ikke er detaljeret vejledning.

Formålet med dette kapitel er derfor at gennemgå de overordnede principper for databehandling, som de fremgår af databeskyttelsesforordningens (GDPRs) artikel 5. Men først forklares sammenhængen imellem de forskellige typer af regler i forordningen, så læseren får en grundlæggende forståelse for forordningens opbygning. Kapitlet fungerer derfor både som en læseguide til forordningens regler og som en indføring i tankegangen bag forordningen.

5.2. De forskellige typer af regler i forordningen

Når man beskæftiger sig med personoplysninger, er den første handling, man – rent juridisk – skal foretage sig at undersøge, om man er omfattet af reglerne i forordningen. Det kan man læse om i kapitel I (artikel 1-4) i GDPR, som f.eks. indeholder regler om anvendelsesområde, og en hel række definitioner (artikel 4) (se kapitel 3).

Hvis man så falder inden for forordningens regler, er der, groft sagt, fire typer af regler, man skal overholde:

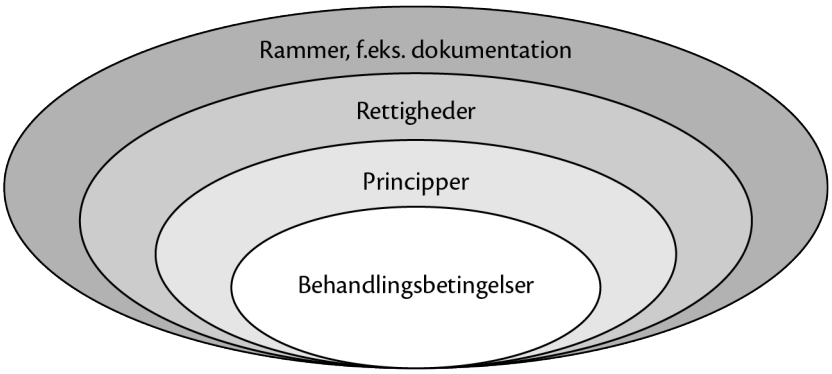
Behandlingsbetingelserne står beskrevet i artikel 6, 9 og 10 i forordningen (se kapitel 6 om behandlingsbetingelser). De skal defineres specifikt for hver eneste behandling, man foretager sig, altså hver gang man gør noget med personoplysninger: fra de først bliver indsamlet, og til de i sidste ende bliver slettet.

Principperne fremgår af artikel 5 og skal overholdes for alle behandlinger, man foretager sig. De er mindre specifikke end behandlingsbetingelserne og skal ikke defineres på ny, hver gang man foretager en ny behandling. Til gengæld skal de altid tænkes med i alt, hvad man gør med personoplysningerne. Principperne beskrives som sagt i dette kapitel.

De registreredes rettigheder står i kapitel III, dvs. artikel 12-23. Det er rettigheder, som de registrerede (dem, som personoplysningerne handler om) har, uanset hvilken behandling der bliver foretaget. For at sikre rettighederne kræver det, at den, som behandler personoplysninger, indretter sig på at kunne overholde dem. Dette skal f.eks. ske ved at fastlægge procedurer for, hvordan indsigtsretten overholdes, og hvordan man korrigerer forkerte oplysninger (se i øvrigt kapitel 13).

Endelig indeholder forordningen en længere række af bestemmelser om *rammerne* for behandlingen af personoplysninger. Det er f.eks. bestemmelserne om databeskyttelsesrådgivere (se kapitel 11), kravene til dokumentation (kapitel 9), databehandleraftaler (kapitel 10), konsekvensanalyser (kapitel 12) og kravene til overførsler til 3. lande (kapitel 15).

Sammenhængen imellem disse fire kategorier kan illustreres af denne figur:[1]



Figur 5.1: De forskellige typer af regler i forordningen.

Når man bevæger sig fra den inderste cirkel til den yderste cirkel i figuren, bliver reglerne mere og mere specifikke for organisationen (hvad enten det er den dataansvarlige eller en databehandler). Organisationen skal således have styr på rammerne, som f.eks. databehandleraftaler og sikkerhedsforanstaltninger, uanset hvilken behandlingsbetingelse der er tale om. Rammerne er specifikke for den enkelte organisation, da denne i hvert fald i nogen grad selv kan vælge, hvilke foranstaltninger der skal iværksættes. Der stilles også forskellige krav til organisationerne afhængig af mængden og typen af oplysninger, der opbevares (se kapitel 14).

Går man derimod den modsatte vej i figuren, fra den yderste cirkel til den inderste, bliver reglerne mere og mere specifikke for den enkelte behandling og mere og mere uafhængige af organisationen. Behandler man oplysningerne på baggrund af f.eks. et samtykke, er der således ikke forskel på behandlingsbetingelsen,[2] uanset hvilken organisation

1. Figuren er en videreudvikling af en figur oprindeligt foreslået af lektor, ph.d., Hanne Marie Motzfeldt, Københavns Universitet.
2. Om behandlingsbetingelser, se kapitel 6.

der er tale om. Man vil stadig skulle kunne dokumentere, at der er tale om et gyldigt samtykke, og kravene til et sådant samtykke er det samme for alle dataansvarlige lige fra de store multinationale virksomheder til kommunen og til den lille tømrervirksomhed.

Det er vigtigt at understrege, at alle reglerne skal overholdes for hver eneste behandling. Derfor skal man altid have styr på alle fire typer af regler, og man skal i øvrigt også kunne dokumentere, at man har overvejet dem alle. Dokumentationskravet følger af de grundlæggende principper for databehandling, som beskrives i næste afsnit.

5.3. Principper for databehandling

Principperne for databehandling er som sagt beskrevet i artikel 5. For alle principperne gælder, at man skal kunne påvise (dokumentere), at man har overvejet, hvordan man overholder dem. Dette følger af artikel 5, stk. 2, og det er derfor naturligt at starte med at beskrive denne.

5.3.1. Ansvarlighed (artikel 5, stk. 2)

I artikel 5, stk. 2, under overskriften "ansvarlighed" står, at "den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 [dvs. principperne] overholdes". Den dataansvarlige (se kapitel 10) er altså den, der har ansvaret, og samtidig også den, der skal kunne bevise, at forordningen faktisk overholdes. Ansvarlighedsprincippet vil blive yderligere uddybet i kapitel 9 og vil derfor ikke blive behandlet grundigt her. Det kan dog kort nævnes, at der er to dimensioner i det lovmæssige krav om ansvarlighed:

For det første er der en *intern dimension*, idet den dataansvarlige skal indføre politikker og mekanismer i organisationen, som vil sikre, at forordningen bliver overholdt. Det kan f.eks. være procedurer for sletning af forældet materiale, fulgt af en løbende undervisning af medarbejderne i de vedtagne procedurer.

Derudover indeholder ansvarlighedsprincippet også en *ekstern dimension*, idet den dataansvarlige over for omverdenen – især Datatilsynet – skal kunne bevise, at reglerne er overholdt. Deraf følger de mange dokumentationskrav, som altså er nærmere beskrevet i et senere kapitel.

5.3.2. God databehandlingsskik (artikel 5, stk. 1, litra a)

Litra a i artikel 5, stk. 1, siger, at personoplysninger skal behandles "lovligt, rimeligt og på en gennemsigtig måde". Dette kaldes også populært for god databehandlingsskik. Det er nemmest at dele bestemmelsen op i dens tre bestanddele, når man skal forklare, hvad den indeholder.

5.3.2.1. Lovlighed

Når der i bestemmelsen står, at personoplysninger skal behandles lovligt, betyder det selvfølgelig, at forordningen skal overholdes. Det betyder imidlertid også, at anden lovgivning også skal overholdes. Her tænkes bl.a. på straffeloven, men også f.eks. forvaltningsloven og reglerne om hvidvask.

Der er mange, der har svært ved at forstå forholdet imellem databeskyttelsesreglerne og andre regler, men måske kan denne tommelfingerregel hjælpe: Hvis der står i anden lovgivning, at man skal, så skal man. Hvis man f.eks. skal give aktindsigt i dokumenter efter forvaltningsloven, så skal man selvfølgelig gøre det. Hverken forordningen eller databeskyttelsesloven forhindrer nogen i at leve op til andre love. Der, hvor det bliver lidt sværere at håndtere, er, når andre love siger, at der er noget, man *må* gøre. F.eks. når man i kraft af meroffentlighedsprincippet *må* udlevere flere oplysninger, end den rene aktindsigt egentlig tilskriver. Så skal man undersøge, om man også *må* udlevere oplysningerne ifølge databeskyttelsesreglerne – for ellers må man ikke.

Kort sagt: Hvis man *skal* ifølge anden lov, så behøver man (sandsynligvis) ikke at overveje, om der er behandlingshjemmel i databeskyttelsesreglerne. Hvis man *må* ifølge anden lov, så skal man overveje, om databeskyttelsesreglerne overholdes, hvis man gør det.[3]

5.3.2.2. Rimelighed

I ordet rimelighed ligger, at man som dataansvarlig (og databehandler) – med et nudansk udtryk – skal opføre sig fair og loyalt. Udgangspunktet i forordningen er, at oplysningerne tilhører de registrerede, og

3. Se også forordningens præambel nr. 40 og 41.

alle andre har dem kun til låns.[4] Derfor skal man passe godt på de oplysninger, man har fået betroet. Det betyder bl.a., at man skal rydde op efter et sikkerhedsbrud, begrænse mulige skader og også kunne dokumentere, at man har ryddet op.[5] Man skal også sørge for, at de registrerede faktisk føler, at der bliver passet godt på deres oplysninger, f.eks. ved at etablere en log-ud funktion på hjemmesider, hvor der skal logges ind, så brugerne nemt kan styre processen.

Derudover betyder kravet om rimelighed også, at man skal tage hensyn til de registrerede og ikke bruge deres oplysninger på en måde, som de ikke kunne have forudset. Derfor er der f.eks. også i forordningen krav om, at registrerede skal have at vide, hvad deres oplysninger skal bruges til, når de indsamles (artikel 13 og 14), og om, at registrerede skal underrettes, hvis deres oplysninger er i fare for at blive misbrugt (artikel 34 og præambel 86). De registrerede skal være fuldt informerede, før de giver samtykke til behandling af deres oplysninger (artikel 7). Endelig er der også et krav om, at den dataansvarlige skal notere, hvis de registrerede gør indsigelser, f.eks. hvis de ikke er enige i en oplysning, som står i deres journal (artikel 16). Dette hører alt sammen med til kravet om, at man skal opføre sig fair og loyalt over for de registrerede.

5.3.2.3. Gennemsigtighed

Princippet om gennemsigtighed er beskrevet i præambel 39, hvor der står, at:

> "Det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet."

Det er et helt centralt element i princippet, at de registrerede skal kunne forudse konsekvenserne af en behandling. Hvis der f.eks. indgår ny teknologi, eller det i øvrigt er svært at gennemskue, hvad en

4. Forordningens præambel nr. 7 udtrykker det, som at "fysiske personer bør have kontrol over deres oplysninger".
5. Se f.eks. Datatilsynets journalnumre 2015-631-0140 og 2011-631-0136.

behandling indebærer, har den dataansvarlige en særlig opgave i at fortælle de registrerede, hvad konsekvenserne vil være.[6]

Derfor skal der også gives forhåndsinformation i en række situationer. Det handler f.eks. om ansatte, hvis lønoplysninger videregives til en bredere kreds, eller hvis internetforbrug bliver overvåget. Her har de registrerede ikke nødvendigvis mulighed for at forhindre behandlingen (videregivelsen af lønoplysninger er f.eks. reguleret af aktindsigten i offentlighedsloven), men de skal have den nødvendige viden, så de kan indrette sig efter forholdene (ved f.eks. at undlade at besøge "problematiske" hjemmesider i arbejdstiden). Det samme gælder, hvis fortrolige oplysninger f.eks. er blevet offentliggjort ved en fejl – her skal de registrerede have at vide, at det er sket, så de kan tage de nødvendige forholdsregler.[7]

I forordningen er princippet om gennemsigtighed især tydeligt i kapitel III om de registreredes rettigheder. Der er det en helt klar og gennemgående regel, at de registrerede skal have de relevante informationer om, hvordan deres oplysninger bliver behandlet, og at de skal have det i et klart, enkelt og (for dem) forståeligt sprog, jf. også artikel 12, stk. 1. Det betyder bl.a., at tjenester, der er målrettet børn, skal kommunikere på en måde, som børn forstår.[8] Er tjenesten rettet mod en anden målgruppe, skal der også kommunikeres på en måde, som et gennemsnitligt medlem af målgruppen vil kunne forstå.[9]

5.3.3. Formålsbegrænsning (artikel 5, stk. 1, litra b)

Princippet om formålsbegrænsning kaldes også formålsbestemthedsprincippet og indeholder to aspekter: *For det første* må oplysninger kun indsamles (og bruges) til "legitime" (dvs. saglige) formål. *For det andet* må oplysningerne kun bruges til enten det formål, de oprindeligt er indsamlet til, eller til formål, som ikke er "uforenelige" med de oprinde-

6. Artikel 29-Gruppen WP 260 rev.01, pkt. 10.
7. Se f.eks. Datatilsynets afgørelse vedrørende Uberettiget adgang til personnumre på studerende hos Det Sundhedsvidenskabelige Fakultet på Københavns Universitet, j.nr. 2017-311-0667.
8. Artikel 29-Gruppen WP 260 rev.01, pkt. 14.
9. Ibid., pkt. 9.

lige formål. Se nedenfor under beskrivelsen af fastlæggelse af forenelighed (artikel 6, stk. 4), hvordan man vurderer dette.

Derfor er første trin i behandling af personoplysninger altid at definere, hvilket formål behandling har. Hvad skal man bruge oplysningerne til? Dette skal skrives ned, så man kan dokumentere, at man har overvejet og fastlagt formålet. Derudover skal det også bruges til at fastlægge behandlingsbetingelserne i artikel 6 og/eller 9 (se kapitel 13).

Formålet skal beskrives så præcist, som det er muligt. Man må ikke gøre formålet så vagt, at det reelt er tomt, eller den registrerede ikke kan gennemskue, hvad oplysningerne vil blive brugt til.[10] F.eks. er det ikke nok at skrive, at oplysningerne skal bruges til "administrative" eller "kommercielle" formål. Man behøver dog heller ikke at specificere formålet så meget, at samtlige detaljer er beskrevet. Lovforslaget til den oprindelige persondatalov fastslår f.eks. at "til brug for udbud af finansielle ydelser" er præcist nok formuleret. Derimod er "til brug for kommercielle formål" ikke præcist nok.[11] Det vigtigste er, at den registrerede kan gennemskue, hvad oplysningerne bliver brugt til.

5.3.3.1. Saglighed

Kravet om legitime formål hænger sammen med kravet om god databehandlingsskik, hvor man jo skal behandle oplysninger "lovligt". Det samme gælder også for formålet – det skal også opfylde kravene til lovlighed. Derfor skal formålet være lovligt, både i forhold til forordningen og i forhold til anden lovgivning.

Formålet skal også *aktuelt* ligge inden for den dataansvarliges virksomhed. Man må således ikke fastsætte et "måske i fremtiden"-formål. På samme måde må man heller ikke fastlægge et "nice to have"-formål, fordi man måske vil kunne bruge oplysningerne, hvis de bliver indsamlet.

Derudover kræves det, at formålet med behandlingen lever op til det større krav om rimelighed – formålet må ikke ligge uden for det,

10. Artikel 29-Gruppen WP 203, s. 39.
11. Forslaget til lov nr. 429 af 31. maj 2000, lovforslag nr. 147, FT 1999/00, de specielle bemærkninger til § 5.

som de registrerede med rimelighed kan forvente, at oplysningerne bliver brugt til.[12]

Endelig skal den dataansvarlige, som bestemmer formålet, også være den, der har ret til at tage den beslutning. Fra gammel praksis har der f.eks. været en sag, hvor beboerne på et kollegie besluttede, at deres køkken skulle tv-overvåges for at forhindre tyveri. Imidlertid var det kun bestyrelsen, der havde kompetence til at træffe sådan en beslutning, og allerede derfor var overvågningen ulovlig.[13]

5.3.3.2. Formålsbegrænsning

Udover at beskrivelsen af formålet tjener til, at man kan kontrollere, om der er tale om et sagligt formål, forhindrer beskrivelsen også, at den dataansvarlige senere kan bruge oplysningerne til andre formål. Beskrivelsen virker altså også som en begrænsning og en garanti til de registrerede for, at de ikke pludselig ser deres oplysninger brugt til noget, de ikke kunne have vidst, at de ville blive brugt til.

I den forbindelse er der to aspekter, der er væsentlige at have med, da de alligevel udvider anvendelsesmulighederne udover lige det, der står sort på hvidt i de oprindelige formål. Det handler *for det første* om formål, som ligger i så naturlig forlængelse af det oprindelige formål, at de må betragtes som en del af dette – og dermed ikke et nyt formål. *For det andet* er der en helt generel undtagelse i forordningen for oplysninger, der bruges til forskning og statistik. *Endelig* er der mulighed for, at den registrerede kan give samtykke, eller at lovgivningen kan diktere et nyt formål.

I det følgende beskrives først de generelle undtagelser og bagefter betingelserne for at fastlægge forenelighed – altså hvornår man kan sige, at et nyt formål kan rummes inden for det oprindelige formål.

5.3.3.2.1. Forskning og statistik

Princippet om formålsbegrænsning indeholder en helt generel undtagelse, når det handler om forskning og statistik. Kapitel 17 og 18

12. Artikel 29-Gruppen WP 203, s. 12.
13. Datatilsynets afgørelse vedrørende Klage over tv-overvågning af kollegiekøkken j.nr. 2007-219-0043 (der var i øvrigt også andre grunde til, at overvågningen var problematisk).

behandler dette langt mere indgående, så her skal kun kort nævnes, at den grundlæggende, ufravigelige betingelse for, at man må bruge oplysninger til forskning eller statistik, er, at oplysningerne så *kun* bruges til disse formål. Man kan bedst illustrere princippet ved at forestille sig en ensrettet vej fra det oprindelige formål til forskning og statistik. Oplysningerne kan godt bevæge sig den ene vej, fra det oprindelige formål til forskning og statistik, men der er adgang forbudt den anden vej. Én gang forskning eller statistik, altid forskning eller statistik.

5.3.3.2.2. Samtykke

Derudover kan den registrerede altid give samtykke til nye formål, jf. artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a – men det kræver, at den dataansvarlige indhenter et nyt samtykke til disse nye formål. Det er i øvrigt værd at bemærke, at dette er det eneste princip, som kan fraviges på baggrund af et samtykke. Man kan altså ikke samtykke til, at f.eks. princippet om dataminimering ikke skal overholdes.

5.3.3.2.3. Lovgivning

Generelt gælder, som også tidligere beskrevet, at hvis anden lovgivning siger, at man *skal*, så forhindrer forordningen ikke, at man følger lovgivningen. Derfor kan lovgiver bestemme, at oplysninger indsamlet til ét formål også skal kunne bruges til andre formål.[14] Dette er bl.a. sket i databeskyttelseslovens § 5, stk. 3, som giver mulighed for, at myndigheder kan sammenkøre oplysninger på baggrund af en bekendtgørelse, men ses også i f.eks. forvaltningsloven, når oplysninger gives videre fra en myndighed til en anden. Den slags lovgivning har eksisteret i mange år – f.eks. bliver lønoplysninger videregivet til SKAT, selvom de jo egentlig kun har som oprindeligt formål at sikre, at ansatte får udbetalt den korrekte løn.

5.3.3.2.4. Fastlæggelse af forenelighed (artikel 6, stk. 4)

I nogle tilfælde har den dataansvarlige måske ikke kunnet forudse alle de forskellige formål, oplysningerne skal bruges til (eller har bare ikke

14. Dette følger naturligt af forordningens artikel 6, stk. 1, litra c, og artikel 9, stk. 2, litra b, f, g, h, i og j, samt artikel 10.

fået tænkt sig om, inden formålet blev defineret). Derfor kan det blive nødvendigt på et senere tidspunkt at overveje, om et nyt formål reelt er et nyt formål, eller om det kan rummes inden for det oprindelige formål.

I 2008 behandlede Datatilsynet en sag, hvor Forsvarets Personeltjeneste havde videregivet adresser, navne og stillingsbetegnelser på 15.000 ansatte til et forsikringsselskab.[15] Formålet var at gøre de ansatte opmærksomme på, at der var indgået en aftale om fordelagtige tilbud på forsikringer som en del af Forsvarets indsats for at fastholde medarbejdere. Dette kritiserede Datatilsynet, fordi oplysningerne var indsamlet og behandlet for at administrere ansættelsesforholdene og ikke for, at de skulle gives videre til en privat virksomhed med henblik på markedsføring.

Når man skal vurdere, om der er tale om et nyt formål eller om et formål, der kan rummes inden for det oprindelige formål, er der en række momenter, man skal inddrage. De fremgår bl.a. af forordningens artikel 6, stk. 4, og gælder både for ordinære og følsomme oplysninger. Momenterne omfatter:

a. Forbindelse til det oprindelige formål

Er der en naturlig sammenhæng imellem det oprindelige formål og det nye formål? I eksemplet ovenfor var der ikke en naturlig sammenhæng imellem ansættelsesforhold og markedsføring, men der er sandsynligvis en naturlig sammenhæng imellem et ansættelsesforhold og arbejdsgiverens behov for at lave statistik, der inddrager oplysninger om medarbejderne.

b. Indsamlingens karakter, især forhold mellem registrerede og dataansvarlige

Blev oplysningerne afgivet frivilligt, eller er der tale om et magtforhold? En offentlig instans bliver som regel anset for at være den stærke part i forholdet til borgerne, derfor bør man være ekstra kritisk i sådanne situationer. Det gælder især, når der er tale om oplysninger, hvor de registrerede ikke har haft noget valg

15. Datatilsynets afgørelse af 19. august 2008 vedrørende Forsvarets Personeltjeneste, J.nr. 2008-632-0034.

i forhold til at aflevere dem, som f.eks. oplysningerne i CPR-registeret. Men det gælder også, når konsekvenserne ved ikke at afgive oplysningerne har været for store til, at der var tale om et reelt valg, f.eks. hvis borgeren har ansøgt om sociale ydelser.[16] På samme måde bør man være kritisk i situationer, hvor den ene part er arbejdsgiver, og den anden arbejder for denne – her vil konsekvenserne ofte også være for store ved ikke at afgive de ønskede oplysninger, og der har derfor reelt ikke været tale om en frivillig indsamling.[17]

Hvis der har været en magtubalance som netop beskrevet, bør man være forsigtig med at tolke nye formål ind i de oprindelige formål. Har der derimod reelt været tale om frivillig afgivelse af oplysninger, er der et større spillerum.

c. Typer af oplysninger

Forordningen kategoriserer oplysninger alt efter, om de er følsomme (artikel 9), handler om straf eller lovovertrædelser (artikel 10), eller om de er ordinære (alle andre oplysninger, artikel 6) (se også kapitel 6 om personoplysninger). Hvis der er tale om oplysninger, der enten er omfattet af artikel 9 eller 10, skal man være forsigtig med at tolke nye formål ind i de oprindelige. Er der derimod tale om ordinære oplysninger, er spillerummet større.

d. Konsekvenser for de registrerede

Det er især vigtigt at overveje, hvilke konsekvenser det vil have for de registrerede, hvis det nye formål bliver tolket ind i det oprindelige. Dette moment afspejler forordningens fokus på den registreredes oplevelse og beder endnu en gang den dataansvarlige om at sætte sig i den registreredes sted. Hvis man f.eks. bruger oplysninger, der blev indsamlet for at udbetale socialhjælp, til at vurdere, om en ansøger skal tilbydes et job, vil konsekvensen for den registrerede potentielt være voldsom.

16. Artikel 29-Gruppen WP 83, s. 9.
17. Artikel 29-Gruppen WP 259 rev.01, s. 7.

e. Garantier

Endelig skal man også ifølge bestemmelsen overveje, om man har iværksat passende garantier. Det kan f.eks. være kryptering og pseudonymisering, men også andre sikkerhedsforanstaltninger som f.eks. at begrænse mængden af personer, der har adgang til oplysningerne. Derudover kan man også overveje, om man skal orientere de registrerede om det nye formål og eventuelt give dem mulighed for at gøre indsigelse.

f. Andre momenter, som ikke fremgår direkte af artikel 6, stk. 4

Der står i artikel 6, stk. 4, at man "bl.a." skal tage hensyn til de momenter, der står i bestemmelsen (som netop beskrevet). Der kan godt være andre momenter, der er relevante. Derfor er der en række tommelfingerregler, som måske kan hjælpe til at vurdere formålsforeneligheden.[18]

Hvis man *skifter behandlingsbetingelse* – f.eks. går fra artikel 6, stk. 1, litra b (kontrakt) til artikel 6, stk. 1, litra f (interesseafvejning) – er der stor sandsynlighed for, at der er tale om et nyt formål.

Hvis det nye formål er *kommercielt*, og det oprindelige ikke var, er der sandsynligvis tale om et nyt formål.

Er der *andre rettigheder* i spil? Er der f.eks. tale om, at man videregiver oplysningerne som led i aktindsigt eller på baggrund af ytrings- og informationsfrihed? Så vil der sandsynligvis være tale om et nyt formål.

Skifter man *sektor*? Går oplysningerne fra en forvaltning til en anden – som f.eks. fra miljøforvaltning til socialforvaltning – så vil der typisk være tale om et nyt formål, som så kræver sin egen behandlingsbetingelse. Det samme er tilfældet, hvis oplysningerne går fra den private sektor til det offentlige eller omvendt.

Kommer oplysningerne fra et *register* eller bare et bredt informationssystem og skal bruges til et snævert formål? Så er der sandsynligvis også tale om et nyt formål.

Det er vigtigt at understrege, at selv om det viser sig, at der er tale om et nyt formål, er det ikke på forhånd udelukket, at behandlingen

18. Artikel 29-Gruppen WP 203, s. 23-27.

kan foretages. Det kræver blot, at man så at sige "starter forfra" og overvejer, om man overholder forordningen ved at iværksætte behandling med det nye formål. Har man f.eks. hjemmel (gyldig behandlingsbetingelse) til den nye behandling? Har man overholdt oplysningspligten? Har man foretaget den nødvendige dokumentation af sikkerhed mv.? Hvis man vurderer (og dokumenterer), at man overholder forordningen, må man gerne bruge oplysningerne til det nye formål.

5.3.4. Dataminimering (artikel 5, stk. 1, litra c)

Princippet om dataminimering fastslår, at personoplysninger skal være *tilstrækkelige*, *relevante* og *begrænset til, hvad der er nødvendigt*. For alle tre parametre gælder det, at de skal måles med det formål, som oplysningerne er indsamlet til.

5.3.4.1. Tilstrækkelige

Allerførst skal det understreges, at princippet om dataminimering ikke handler om, at man ikke må indsamle oplysninger. Tværtimod skal man indsamle (og behandle) nok oplysninger, til at man kan opnå det formål, som man fastsatte fra starten. Man skal altså først overveje, om man har alle de oplysninger, man faktisk har brug for, når man skal opfylde dataminimeringsprincippet. Dette skyldes, at hvis man ikke har alle de nødvendige oplysninger, er der stor risiko for, at de data, man bruger, giver et forkert resultat. Og da et af hovedformålene med databeskyttelsesforordningen er, at de registrerede skal have tillid til, at brugen af personoplysninger sker på en forsvarlig måde, nytter det ikke noget, at man har misvisende resultater.[19] Det fremmer nemlig på ingen måde tilliden.

5.3.4.2. Relevante

Man skal altid overveje, om de oplysninger, man behandler, nu også reelt er relevante for behandlingsformålet. Indeholder oplysningerne informationer, som kan bidrage til, at man opnår formålet, eller har man dem kun med, fordi det f.eks. var nemmere ikke at sortere i dem? Hvis det er tilfældet, overholder man ikke princippet om dataminimering.

19. GDPR præambelbetragtning nr. 7.

5.3.4.3. Nødvendige

Oplysninger kan både være tilstrækkelige og relevante, men hvis de blot f.eks. duplikerer andre informationer eller i virkeligheden er overflødige, er de ikke nødvendige for, at formålet kan opnås.

Det klassiske eksempel på denne overvejelse er en situation, hvor man har brug for at kunne skelne imellem forskellige personer. Så længe personerne har forskellige navne, har man faktisk ikke brug for andre oplysninger end deres navne. Hvis personerne har enslydende navne, har man til gengæld brug for lidt flere oplysninger som f.eks. deres adresser. Man vil kun i meget sjældne tilfælde have brug for flere oplysninger, da det er yderst sjældent, at flere personer med samme navn bor på samme adresse. Skulle det alligevel ske, ville en fødselsdato eller et fødselsår sandsynligvis være nok til at kunne adskille dem. Man har således i princippet ikke brug for et CPR nr. for at kunne skelne personer fra hinanden. Når man alligevel i så høj grad gør brug af netop CPR nr. i Danmark, er det, fordi lovgivningen giver os mulighed for det – og i mange tilfælde faktisk også dikterer, at det skal bruges, især i kontakten med de offentlige myndigheder.[20]

5.3.5. Rigtighed (artikel 5, stk. 1, litra d)

Personoplysninger skal være rigtige. Dette krav bygger på den tanke, at oplysninger af dårlig kvalitet ikke kan anvendes i digitale tjenester. Så hellere have lidt færre oplysninger, der til gengæld er korrekte, end mange oplysninger, hvor man ikke ved, om de er rigtige eller ej.

Dette betyder for det første, at den dataansvarlige skal være omhyggelig, når oplysningerne indsamles, så man kun får korrekte og fyldestgørende oplysninger. Det betyder dog også og ikke mindst, at den dataansvarlige skal slette eller rette (berigtige) "urigtige" oplysninger med det samme. Dette skal også ses i sammenhæng med forordningens artikel 16 og 17 om den registreredes ret til berigtigelse og sletning (se kapitel 13).

---

20. Se CPR-loven. Se i øvrigt også, fra det svenske datatilsyn (Datainspektionen), d.nr. 1603-2006 af 27. februar 2007, hvor tilsynet udtalte kritik af det svenske Posica kasseapparat-system, hvor alle, der købte alkohol i en supermarkedskæde, skulle have deres identifikationspapirer skannet, også selv om der ikke var tvivl om, at de var ældre end den fastsatte minimumsalder.

Det følger af dataminimeringsprincippet (ovenfor), at man ikke må opbevare flere oplysninger end nødvendigt for at opnå formålet. Dette princip gælder også i forbindelse med rigtighedsprincippet: Hvis en oplysning er korrekt og i øvrigt fyldestgørende nok til, at formålet kan opfyldes, er der ikke krav om, at man indsamler flere oplysninger for at gøre oplysningerne "helt rigtige".

Dette kan bl.a. ses i forordningens artikel 11, som handler om de situationer, hvor man har personoplysninger, der ikke er direkte knyttet til identificerede personer. Det kunne f.eks. være oplysninger om brugerne af en hjemmeside, hvor brugerne diskuterer i et forum. Her har man nok brugernavne, og sandsynligvis også e-mailadresser, men ikke nødvendigvis andre oplysninger. I sådan en situation er der ikke krav om, at man finder frem til navne eller fysiske adresser for at gøre oplysningerne fuldstændige.

Rigtighedsprincippet hænger også tæt sammen med den gode databehandlingskik, hvor man jo skal behandle oplysninger fair og loyalt. Det vil ikke være fair eller loyalt over for de registrerede f.eks. at træffe en afgørelse på baggrund af ufuldstændige eller direkte forkerte oplysninger. Derfor ligger der også i princippet en forpligtelse for den dataansvarlige til at sikre sig, at oplysninger er ajourførte. Denne forpligtelse vil sandsynligvis være større, jo vigtigere oplysningerne er for formålet, og desto større konsekvenserne af forkerte eller ufuldstændige oplysninger er. Er der f.eks. tale om en sundhedsjournal, kan det få katastrofale følger, hvis der står den forkerte blodtype eller der ikke står noget om, at en patient er allergisk over for penicillin. Modsat har det sandsynligvis ikke livstruende konsekvenser, hvis medlemmerne af en mailingliste ikke modtager ugens tilbud på dåsetomater.

Den dataansvarlige er også selv ansvarlig for at sikre, at oplysningerne er korrekte ved indsamlingen og ved den senere anvendelse.

Fra Datatilsynets tidligere praksis kan nævnes to eksempler: I det første havde en bank ikke sikret, at tidsregistreringen på deres overvågningsvideo var korrekt, så der blev udleveret det forkerte klip til politiet, da det efterspurgte video fra et bestemt tidsrum.[21] I det andet eksempel havde Kræftens Bekæmpelse i forbindelse med et forsknings-

21. Datatilsynets afgørelse af 8. oktober 2007 vedrørende Spørgsmål om synkronisering af ure ved tv-overvågning, J.nr. 2007-213-0022.

projekt udsendt breve til 247 personer, hvor der stod, at de levede med en kræftsygdom.[22] De 247 personer var fundet igennem Cancerregisteret, som indeholder oplysninger om patienter, der har fået en kræftdiagnose. Imidlertid er der også en lang række andre sygdomme, der registreres i Cancerregisteret, og det var disse sygdomme og ikke kræft, som de 247 personer havde. I begge eksemplerne kritiserede Datatilsynet kraftigt, at de dataansvarlige ikke havde tilrettelagt deres arbejde sådan, at de kontrollerede, om oplysningerne var korrekte, inden de blev brugt.

Det er ikke alle oplysninger, der bliver indsamlet, som er mulige at verificere. Hvis det er tilfældet, skal den dataansvarlige notere dette, så man ved, at oplysningen ikke er verificeret, og at man derfor ikke kan stole ubetinget på, at den er rigtig. På samme måde skal den dataansvarlige også notere, hvis oplysningen ikke kommer fra en troværdig kilde, som f.eks. en anonym henvendelse. Ikke fordi oplysningen nødvendigvis skal kasseres, men fordi man skal vide, hvor troværdig den er.[23] Med andre ord handler det om hele tiden både at gøre sit bedste for at indsamle gode oplysninger og på den anden side hele tiden at være ærlig om, hvor gode og pålidelige oplysningerne faktisk er. Kravene til pålideligheden vil stige, desto vigtigere oplysningerne er for behandlingen.

I de gamle regler, dvs. persondataloven og persondatadirektivet, som ikke gælder længere, var der et krav om, at forkerte oplysninger skulle slettes eller rettes "snarest muligt". I forordningen står der imidlertid "straks", hvilket betyder, at man ikke kan vente, til det er belejligt, men netop skal gøre det, så snart man bliver opmærksom på fejlen.[24]

5.3.6. Opbevaringsbegrænsning (artikel 5, stk. 1, litra e)

I forlængelse af rigtighedsprincippet, som jo gør, at man skal slette forkerte oplysninger, kommer opbevaringsbegrænsningen, også kaldet

22. Datatilsynets afgørelse af 15. december 2016 vedrørende udsendelse af breve med urigtige oplysninger om sygdom, j.nr. 2015-631-0117.
23. Se også Artikel 29-Gruppen WP 117, især s. 11.
24. Betænkning 1565/2017, s. 98.

tidsbegrænsningsprincippet. Det handler kort sagt om, at man ikke må opbevare oplysninger længere, end man reelt har brug for dem.

Når man skal overveje, om man har brug for oplysningerne, skal man holde dem op imod behandlingsformålet. Hvis oplysningerne ikke længere er nødvendige for at opfylde formålet, skal man sørge for, at de bliver slettet. Der er ikke nogen fast regel for, hvor længe man skal opbevare oplysningerne i forordningen eller databeskyttelsesloven. Derimod kan der sagtens være regler i andre love, som gør, at man skal opbevare dem i et bestemt tidsrum. Og som allerede skrevet flere gange, skal man overholde reglerne i andre love.

Bogføringsloven siger f.eks., at erhvervsdrivende virksomheder skal opbevare bogføringsmateriale i 5 år.[25] På samme måde indeholder forældelsesloven forskellige frister for opbevaring i henholdsvis 3 og 5 år.[26]

Det er også værd at huske på, at hvis der skal fastlægges et retskrav, f.eks. ved en erstatningssag ved domstolene, skal den dataansvarlige selvfølgelig opbevare de nødvendige oplysninger, så længe det er nødvendigt for, at retskravet kan fastsættes. Dette følger direkte af forordningens artikel 9, stk. 2, litra f, for så vidt angår de følsomme oplysninger, men gælder også for de ordinære oplysninger, hvor hjemlen enten kan findes i den retlige forpligtelse i artikel 6, stk. 1, litra c (især for de offentlige myndigheder) eller interesseafvejningen i litra f i samme bestemmelse (for private dataansvarlige). Se i øvrigt kapitel 6 om behandlingsbetingelser.

Derudover bør man bruge sin sunde fornuft, når man fastlægger, hvor længe oplysninger skal opbevares, og især lægge vægt på, hvad de registrerede retmæssigt kan forvente.

Et teleselskab opbevarede kundernes slettede e-mails i et år, som en service til kunderne. Imidlertid var det ikke forudsigeligt for kunderne, at dette skete, og derfor var det yderst kritisabelt.[27]

25. Lovbekendtgørelse nr. 648 af 15. juni 2006, § 10.
26. Lovbekendtgørelse nr. 1238 af 9. november 2015, kapitel 3 og 4.
27. Datatilsynets afgørelse af 15. maj 2003 vedrørende Teleudbyders opbevaring af e-post, j.nr. 2002-215-x.

5.3.6.1. Statistik og forskning

En grundlæggende undtagelse fra tidsbegrænsningsprincippet er reglen om, at oplysninger, der udelukkende bruges til forskning eller statistik, ikke skal slettes. Disse oplysninger må altså gerne blive opbevaret i længere tid, men det er under forudsætning af, at den dataansvarlige har implementeret passende tekniske og organisatoriske foranstaltninger, som f.eks. pseudonymisering og kryptering (se kapitel 14). Derudover er det også en vigtig betingelse, at oplysningerne udelukkende bruges til statistik eller forskning og ikke føres tilbage i systemet igen. Der skal så at sige være vandtætte skotter imellem statistik og forskning samt resten af systemet. Se også kapitel 18 om statistik og 17 om forskning.

5.3.7. Integritet og fortrolighed (artikel 5, stk. 1, litra f)

Under overskriften om integritet og fortrolighed gemmer der sig et princip om, at man skal passe godt på oplysningerne, når man har dem. Med andre ord skal man sørge for en tilstrækkeligt høj sikkerhed, så oplysningerne bevarer deres integritet (ikke bliver ødelagt), og også forbliver fortrolige (ikke bliver delt med nogen, der ikke har lov til at se dem).

Dette bliver beskrevet i flere detaljer i kapitel 14, så her skal kun nævnes enkelte pointer.

For det første er det værd at bemærke, at forordningen siger, at man skal have "tilstrækkelig" sikkerhed. Den definerer ikke, hvad der ligger i begrebet "tilstrækkelig" – det er altså op til den dataansvarlige at vurdere dette.

For det andet dikterer forordningen heller ikke, hvilke foranstaltninger man skal sætte i værk – den siger kun, at de skal være "passende". Igen skal den dataansvarlige altså selv vurdere, hvad der vil være "passende".

Foranstaltningerne deles typisk op i tre kategorier:

— De *organisatoriske* foranstaltninger handler om, at man skal sørge for, at hele organisationen er med til at overholde reglerne, f.eks. ved at indføre faste procedurer for, hvem der arbejder med de forskellige personoplysninger, og hvordan det skal gøres – og

ikke mindst, hvordan man sørger for, at disse procedurer altid bliver overholdt.

— *Fysiske* foranstaltninger kan f.eks. være, at man sørger for, at det sted, hvor serverne står placeret, ikke er i risiko for at blive oversvømmet ved en stormflod.
— *Systemtekniske* foranstaltninger retter sig – som navnet siger – imod de systemer, der anvendes. Det er f.eks. detaljer som, at det kun er autoriserede medarbejdere, der har adgang til fortrolige oplysninger, eller at kryptering foregår automatisk.

5.4. Afrunding

Som beskrevet i dette kapitel går principperne i artikel 5 som røde tråde igennem hele forordningen. Mange af de enkelte bestemmelser kan således læses som detailreguleringer af de enkelte principper – som f.eks. bestemmelserne om dokumentation, der følger af ansvarlighedsprincippet. Med dette kapitel er det derfor håbet, at læseren har fået en grundlæggende forståelse af forordningens tankegang, som kan være en hjælp i læsningen af resten af bogen.