Databeskyttelsesforordningens princip om dataminimering herunder sletning set i forhold til forvaltningslovens regler

AALBORG UNIVERSITY
DENMARK

Vejleder: Niels Vase

Udarbejdet af:

Studie nr.: 20164177 Jeppe Svansø Laursen

Studie nr.: 20164110 Lars Henrik Fly Steensen

Statistik:

Sider	67
Ord	22.210
Tegn (uden mellemrum)	132.446
Tegn (med mellemrum)	154.619
Afsnit	408
Linjer	1.816

☐ Medtag tekstfelter, fodnoter og slutnoter

1. Abstract

The General Data Protection Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, also known “GDPR”. GDPR is currently in focus for many companies around the world, as they are now in risk of heavy fines, if they do not comply with the regulation, whereas earlier it would have been a slap on the wrist. Private companies or public administrations are forced to focus on complying with data protection of the public.

This thesis explores how the data processor should comply with the Principles relating to processing of personal data, data minimization within the Danish Public Administrations Act, and Rights of the data subject.

The thesis will explore the concepts regarding the principle of inquiry, the duty to note and the obligation to keep records, because of the relevancy to the principle of access to documents in The Danish Administrations Act and the Public Access to Information Act. Furthermore, are the concept of party explained because it is important for the application of access to documents.

The main focus of the thesis is GDPR and its rules regarding a Right of Access and Data minimization. The thesis has focused on specific articles such as 5, 13-18 and 21 (Principles relating to processing of personal data and the Rights of the data subject).

The thesis has used rulings from “Datatilsynet” an independent danish supervisory authority, because the lack of cases from the danish courts. There has only been one ruling from the danish court regarding GDPR. The thesis has therefor chosen to explore data minimization in the Danish Public administration rather than sanctions.

The thesis has studied data minimization by exploring principles such as the deadline for erasure, anonymization of data and the possibility to archive. The conclusion of the study is that The Danish Public Administration cannot erase information about the data subject because they are forced to keep records and notes. They can only archive or anonymize data regarding the data subject.

2. Indholdsfortegnelse

Indhold

3. Indledning

Informationsteknologi har gjort det nemt at gøre alt digital, og vi er gået fra papirfyldte procedurer til digital sagsbehandling. De sociale medier er en fast del af dagligdagen for mange, og folk er så småt begyndt at glemme fundamentale rettigheder som privatlivets fred. Mark Zuckerberg, stifteren af Facebook har tidligere udtalt "*just get over it – no one cares about privacy anymore*".[1] Dette udsagn kunne sagtens have været sandheden, men med forordningen 2016/679 (Generel forordning om databeskyttelse), som erstatter direktiv 95/46 og hovedparten af persondataloven er udsagnet mere et levn fra fortiden.

I takt med at den offentlige sektor har været nødt til at forholde sig til databeskyttelsesforordning, er der kommet mere fokus på behandlingen af personoplysninger. I den forbindelse er det vigtigt for borgerne at kende sine rettigheder i forhold til beskyttelse af personoplysninger. Myndighederne er med forordningens indtog blevet påtvunget en endnu større gennemsigtighed i deres behandling af personoplysninger.

Forordningen trådte i kraft d. 25. maj 2018 og har betydet, at myndigheder og virksomheder har været nødt til at tage stilling til databeskyttelsesreglerne. Den tidligere praksis gav virksomhederne et rap over fingrene med en lille bøde for brud på datasikkerheden, hvorimod den nye praksis efter forordningen tvinger selv store virksomheder til at efterleve reglerne, da der nu er udsigt til bøder på op mod 2-4% af den totale omsætning for virksomheden.[2]

Forordningen er blevet udstedt med henvisning til TEUF-artikel 16, som siger, at "*enhver har ret til beskyttelse af personoplysninger om vedkommende selv*".[3] Dette passer godt overens med retten til privatliv, som er en fundamental grundrettighed, jf. Den Europæiske Menneskerettighedskonvention artikel 8, EU-charterets artikel 7-8, straffelovens kapitel 27 og Grundlovens § 72.[4] [5]

Privatlivet har mange facetter og en opdeling mellem fysisk, informationelt, kommunikationelt og territorialt privatliv kan med fordel antages at eksistere, da den retlige behandling af informationerne kan være forskellig. Det vigtige er, om nogle informationer kan misbruges til at krænke en person, da formålet er at beskytte individets personoplysninger.[6]

[1] Peter Blume: Databeskyttelsesret (2018) s. 25
[2] https://gdpr.dk/databeskyttelsesforordningen/kapitel-8-retsmidler-ansvar-og-sanktioner/artikel-83-generelle-betingelser-for-paalaeggelse-af-administrative-boeder/
[3] Peter Blume: Den nye persondataret (2016) s. 43
[4] Peter Blume: Databeskyttelsesret (2018) s. 14
[5] Peter Blume: Databeskyttelsesret (2018) s. 53
[6] Peter Blume: Databeskyttelsesret (2018) s. 14-15

Forordningen regulerer mange regler, og denne introduktion er derfor meget generel. Der kan derfor opstå et behov for at inddrage flere begreber, da disse er relevante for at opnå en besvarelse af vores problemformulering.

Formålet med denne korte introduktion har derfor været en grundlæggende forståelse af behovet for reglerne, da de tidligere regler ikke kunne følge med internettets fremgang. Dette projekt har til formål at belyse problemstillingen vedrørende behandling og overførsel af personoplysninger i forbindelse med forvaltningsrettens regler om aktindsigt, herunder med særligt fokus på dataminimeringspligten. Denne problemstilling kommer til udtryk i nedenstående problemformulering.

4. Emnevalg

Databeskyttelsesforordningens princip om dataminimering herunder sletning set i forhold til forvaltningslovens regler om aktindsigt

4.1 Problemformulering

På baggrund af udviklingen indenfor informationsteknologi og de mange forskellige regelsæt i andre lovgivninger, vil denne afhandling forsøge at undersøge, hvilke problematikker der opstår som følge af det retlige sammenspil mellem forskellige lovgivninger. Vores overordnede problemstilling lyder derfor som følgende:

Hvordan skal en dataansvarlig overholde Databeskyttelsesforordningsprincipper om dataminimering herunder sletning i henhold til forvaltningsrettens regler om aktindsigt, journaliseringspligt og notatpligt?

4.2 Afgrænsning

Det forventes at læseren har en grundlæggende viden omkring databeskyttelsesforordningen og forvaltningsretten, hvorfor kun relevante begreber i databeskyttelsesforordningen og forvaltningsloven vil blive defineret.

Afhandlingen har valgt at forklare undersøgelsesprincippet, notatpligten og journaliseringspligten, da de er særlig vigtige for behandlingen af aktindsigt. Endvidere er partsbegrebet forklaret, da det er vigtigt i forhold til, om der kan søges aktindsigt efter forvaltningsloven eller offentlighedsloven.

Afhandlingens hovedfokus er databeskyttelsesforordningen, herunder den registreredes rettigheder, særligt reglerne om indsigt og dataminimering. Afhandlingen har primært anvendt databeskyttelsesforordningens artikel 5, 13-18 og 21. Derudover vil en række bestemmelser blive behandlet overfladisk, hvis de anses som relevante for besvarelsen af problemformuleringen.

I analyseafsnittet har afhandlingen fokus på Datatilsynets afgørelser, da disse danner rammen for praksis, grundet manglende domme fra domstolene. Der findes pt. én ny dom, som har været i byretten, men afhandlingen har valgt at fokusere på Datatilsynets afgørelser i stedet, da retstilstanden stadig vurderes at være uklar.

Afhandlingen afgrænses fra behandlingen af følgende oplysninger, da disse vil være for omfattende. Afhandlingen beskriver ikke retten til dataportabilitet, automatiske individuelle afgørelser herunder profilering, reglerne om sanktionsmuligheder og overførsel til tredjelande, da fokus har været på indsigt og dataminimering.

Afhandlingen behandler ikke aktindsigt, som er omfattet af miljøoplysningsloven og sundhedslovgivningen. Udvalgte paragraffer af arkivloven vil dog kort blive nævnt i forbindelse med princippet om dataminimering.

Yderligere kan nævnes at der ikke vil blive behandlet stillingsbesættelser/ansættelsesforhold, administrative straffesager, retsplejeloven, kriminalregisterbekendtgørelsen og andre særlovgivninger.

5. Metode

For at besvare afhandlingens problemstilling er det nødvendigt at redegøre for relevante bestemmelser i databeskyttelsesforordningen. Afhandlingen vil blive udarbejdet ved anvendelse af den retsdogmatiske metode. Ved brug af denne metode beskrives og analyseres den gældende retstilstand.[7] Opgavens formål er at finde og fastlægge forskellige regler og principper, som er relevant i forbindelse med sagsbehandling indenfor databeskyttelsesretlige problemstillinger, der kan opstå med tilknytningen til forvaltningslovens regler om aktindsigt. Reglerne og principperne vil blive analyseret, og en eventuel retlig tvivl vil blive diskuteret. Formålet med den retsdogmatiske metode er ikke at finde en løsning på konkrete problemer, men derimod beskrive retstilstanden.[8] Afhandlingen kommer derfor ikke med en endegyldig konklusion på problemformuleringen, da hensigten er en retlig argumentation af synspunkter.[9]

Det at skrive dogmatisk betyder, at udgangspunktet ligger i gældende ret, de lege lata.[10] Formålet er at analysere, beskrive og systematisere gældende retsregler. Ved anvendelsen ses ofte en opdeling i kasser såsom stat - borger, myndighed - borger og borger - borger. Opstår der en retlig tvist mellem disse parter bruges loven til at finde en rimelig løsning.

Som nævnt vil projektet blive udarbejdet ved at anvende den retsdogmatisk metode. For at kunne gøre dette, er det nødvendigt at benytte den juridiske metode. Den juridiske metode er med til at sikre retssikkerhed for borgerne. Dommerne skal være objektive i henhold til, hvordan en given sag afgøres. Loven og de retlige principper har til formål at skabe en sikker retstilstand for alle borgere. Dansk ret tager udgangspunkt i den nordiske trinfølge; loven, retspraksis, sædvanen og forholdets natur, hvorfor tvister løses herefter.[11]

Projektet vil derfor benytte retskilder og andet retligt relevant empiri til at komme med en vurdering af opstillede retlige tvister. Særligt er det relevant at nævne retsforskriften i databeskyttelsesforordningens artikel 5 stk. 1 og 2, som giver et godt grundlag for behandlingsprincipperne i databeskyttelsesforordningen samt forvaltningslovens § 19 om aktindsigt. Andre relevante artikler, præambler eller paragraffer vil blive nævnt efter behov.

[7] Carsten Munk Hansen: Retsvidenskabsteori (2014), s. 204
[8] Carsten Munk Hansen: Retsvidenskabsteori (2014), s. 205
[9] Peter Blume: Retssystemet og juridisk metode (2020), s. 32f. og s. 183-185
[10] Peter Blume: Retssystemet og juridisk metode (2020), s. 32f.
[11] Carsten Munk Hansen: Retsvidenskabsteori (2014), s. 85ff.

5.1 Retskilder og tilsyn

Den primære retskilde, der benyttes i denne afhandling, er en forordning, som er vedtaget i EU. En forordning er ifølge EU's regler almengyldig, ligesom den er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat. En forordning virker således som en lov i medlemsstaterne, og den gælder i den form, som den er vedtaget, og den må som udgangspunkt ikke gennemføres i national ret. Der må som udgangspunkt ikke være anden dansk lovgivning, der regulerer behandling af personoplysninger, i det omfang det er reguleret i forordningen. Danmark er således forpligtet til at indrette dansk lovgivning i overensstemmelse med forordningens bestemmelser med virkning fra den 25. maj 2018.[12] [13] I databeskyttelsesforordningen er der et råderum, som kan udfyldes af national lovgivning. Derfor er der i Danmark blevet vedtaget Databeskyttelsesloven, som supplerer Databeskyttelsesforordningen.[14]

Databeskyttelsesforordningen og Databeskyttelsesloven erstatter det tidligere gældende Persondatadirektiv[15] som blev implementeret i dansk ret med Persondataloven.[16] Hvor det anses relevant, vil Persondatadirektivet blive inddraget i afhandlingen, af hensyn til fortolkningsspørgsmål.

Besvarelsen af persondataretlige problemstillinger skal ikke altid beskrives ud fra en dominerende retskilde. Der findes derfor polycentri, da der kan opstå tilfælde, hvor kun enkelte retskildetyper spiller en rolle. Afhandlingens behandling tager udgangspunkt i en dominerende retskilde og behandler derved ikke undtagelserne i eventuelle speciallovgivninger, jf. afgræsningsafsnit 4.2.[17]

Den danske grundlov blev til i 1849 og blev senest revideret i 1953. Den tager derfor ikke højde for persondataretten. Grundlovens § 72 nævner boligens ukrænkelighed og beskyttelse af kommunikationshemmeligheden, der efter praksis også omfatter elektronisk kommunikation. Nogle lande har derfor tilføjet reguleringen sidenhen, men ændringsprocedurerne for den danske grundlov gør, at man muligvis ikke får en sådan tilføjelse i dansk kontekst. Teoretisk er Grundloven den højeste retskilde i dansk ret, og andre regler må derfor ikke gå imod denne. På grund af magtfordelingsprincippet i Grundlovens § 3, har Danmark derfor fået tilføjet deres egen ordning i databeskyttelsesforordningen, jf. artikel 83 nr. 9. Retskildediskussionen, om EU-retten har forrang, tillægger denne afhandling ikke relevans og bliver behandlet med det udgangspunkt, at EU-retten er på samme retskilde niveau som

[12] TEUF artikel 288, stk. 1
[13] https://www.datatilsynet.dk/databeskyttelse/lovgivning
[14] Lov nr. 502 af 23/05/2018
[15] Direktiv 95/46 EF
[16] Lov nr. 429 af 31/05/2000
[17] Peter Blume: Databeskyttelsesret (2018) s. 52

Grundloven. Dette gøres for at undgå en debat om EU ret imod dansk ret og diskuteres derfor ikke yderligere i denne afhandling.[18]

5.2 Administrative retsforskrifter

Tidligere udstedte Justitsministeriet bekendtgørelser med hjemmel i Persondataloven. Dette kan Justitsministeriet ikke længere, eftersom forordningen har supranational karakter (almengyldig, gælder alle medlemsstater).[19] Der kan derfor nu kun udstedes vejledninger, da egentlige retsforskrifter ville gå imod EU-retten. Denne afhandling benytter derfor vejledninger fra Det Europæiske Databeskyttelsesråd, som er et uafhængigt EU-organ, der har til opgave at sikre en ensartet anvendelse af Databeskyttelsesforordningen i EU. [20] Databeskyttelsesrådet kan træffe bindende afgørelser om fortolkning af databeskyttelsesreglerne, hvis der er uenigheder mellem de enkelte landes nationale datatilsyn. Rådet tog over for artikel 29-gruppen, som ikke længere eksisterer. Selvom artikel 29-gruppen ikke eksisterer, anses deres vejledninger stadig som gældende. Det Europæiske Databeskyttelsesråd har tiltrådt vejledningerne fra artikel 29-gruppen og anses som såkaldt soft law, da dokumenterne ikke er juridisk bindende for medlemslandene, men i praksis har de stor retskilde værdi.[21]

Der vil i afhandlingen blive inddraget vejledninger samt afgørelser fra det danske Datatilsyn. Datatilsynet fungerer som et uafhængigt tilsynsorgan. Tilsynets primære funktion er at vurdere alle persondataretlige spørgsmål og træffe afgørelser om, hvorvidt en bestemt adfærd sker i overensstemmelse med Databeskyttelsesforordningen samt Databeskyttelsesloven. Datatilsynet er struktureret i et sekretariat og et råd. Datarådet er nok dem, som er mest afgørende, men retskildemæssigt er de ikke anderledes stillet end sekretariatets afgørelser, de må derfor anses som en helhed. Vejledninger er beskrivende, gældende ret, da de giver en god indikation for dataansvarlige, hvad tilsynet lægger vægt på. Tilsynsafgørelserne offentliggøres ikke, da de har en retsanvendende karakter og dermed ingen egentlig retskildemæssig betydning. Afgørelser, der indebærer ny fortolkning og udfyldning af regler, som er i offentlighedens interesse, bliver gjort tilgængelige på tilsynets hjemmeside. Disse offentliggørelser er derfor hovedkilden til praksis og den gældende ret.[22]

Der findes ikke mange databeskyttelsesretlige domme, men med forordningens indførelse af væsentligt højere bøder vil dette nok blive ændret, da der er en formodning om, at virksomhederne

[18] Peter Blume: Databeskyttelsesret (2018) s. 52f
[19] Peter Blume: Databeskyttelsesret (2018) s. 55
[20] https://www.datatilsynet.dk/internationalt/databeskyttelsesraadet-edpb/
[21] Peter Blume: Persondatarettens kilder og metode (2020) s. 65f.
[22] Peter Blume: Databeskyttelsesret (2018) s. 57

vil afprøve Datatilsynets bødestørrelser i henhold til Grundlovens § 63, eftersom de ikke har mulighed for at påklage bøderne administrativt ved tilsynet.[23]

[23] Peter Blume: Databeskyttelsesret (2018) s. 57

6. Grundlæggende forvaltningsret

Forvaltningsret kunne være et selvstændigt specialeemne i flere kategorier, hvorfor denne gennemgang af forvaltningsretten vil være i hovedtræk for at danne grundlag for projektets problemformulering. Eftersom afhandlingen behandler indsigtsretten i databeskyttelsesforordningen, har afhandlingen valgt at fokusere på dataminimeringen sammenholdt med reglerne om aktindsigt efter forvaltningsloven og offentlighedsloven.

Forvaltningsret dækker mange emner. Den dækker retsreglerne for den offentlige forvaltning og dens handlinger. I den almindelige forvaltningsret behandles en række problemer, som er fælles for al forvaltningsvirksomhed eller store dele heraf. Forvaltningsretlige specialefag, som f.eks. byggeret, kommunalret, miljøret, skatteret og socialret har derimod til opgave at belyse retsregler inden for enkelte sektorer eller dele af forvaltningen.[24]

Forvaltningen har hjemmel i Grundlovens § 3, og er derfor central for dansk myndighedsudøvelse. Grundloven beskriver seks retlige forhold. Der er tre magtorganer i Danmark og tre magtfunktioner. Grundloven bestemmer så denne sammenkædning. Den dømmende magt ved domstolene, den lovgivende magt skal ligge hos Folketinget og regeringen i forening, og at den udøvende magt skal ligge hos forvaltningen (kongen).

Forvaltningen har den ”udøvende” magt i Danmark, hvilket betyder, at forvaltningen administrerer lovgivningen. Forvaltningen udsteder detailregler til udmøntning af love, som lovgiver vedtager. Forvaltningen kan træffe konkrete afgørelser i henhold til lovgivningen samt i øvrigt udføre handlinger, som er nødvendige til udmøntningen af lovgivningen, f.eks. udbetale ydelser og behandle syge. Det er desuden forvaltningens job at kontrollere, borgerne overholder lovgivningen. Forvaltning kan have forskellige betydninger både juridisk og i daglig tale. En sproglig definition vil ikke blive diskuteret i denne afhandling, da det er udenfor afhandlingens formål. Offentlig forvaltning vil derfor være i bred forstand, når der nævnes forskellige myndigheder eller erhverv, der yder forvaltningsvirksomhed.[25]

Forvaltningsmyndigheder kan træffe mange typer ”beslutninger”. Dette kan f.eks. være beslutninger, som er en del af sagsbehandlingen, f.eks. kompetencespørgsmål, sagsoplysning eller inhabilitet. Det

[24] Sten Bønsing: Almindelig forvaltningsret (2018) s. 20
[25] Sten Bønsing: Almindelig forvaltningsret (2018) s. 17-22

kan også være beslutninger af privatretlig karakter, såsom kontraktindgåelse og anerkendelse af erstatningsansvar. Det kan være beslutninger om udstedelse af interne tjenestebefalinger, generel regeludstedelse f.eks. af bekendtgørelser eller vedtægter, og enkeltafgørelser rettet mod konkrete parter.

Begrebet forvaltningsafgørelser dækker først og fremmest over konkrete enkeltafgørelser rettet mod enkeltpersoner, grupper af personer og generelle afgørelser, der gælder for en større ubestemt kreds af personer. Enkeltafgørelserne kaldes i forvaltningsretten for "forvaltningsakter", dvs. afgørelser, hvor der er udpeget personer, som er "parter".[26] Der er forskel på, om der er tale om en beslutning eller afgørelse, idet forvaltningsloven kun finder anvendelse på afgørelser.[27] En afgørelse, både generelle og konkrete, kan defineres således: "*Der er tale om udtalelser fra en forvaltningsmyndighed, der tilsigter ensidigt at fastsætte, hvad der er eller skal være ret*.".[28] Forvaltningsvirksomheden er derfor anderledes end privatretten, hvor der i aftaler gælder et gensidighedsprincip, hvor forvaltningen tager udgangspunkt i ensidighed. Beslutninger, som afslutter en sagsbehandling, har særlig betydning, idet det kan have betydning for, om der er tale om en afgørelse. Et eksempel er, hvis en beslutning tager stilling til et væsentligt retsspørgsmål som f.eks. en borgers indsigelse jf. databeskyttelsesforordningens artikel 21 mod behandlingen af personoplysninger i en afgørelse, der er omfattet af forvaltningsloven, mens dette ikke er tilfældet for f.eks. stillingtagen til meddelelse efter artikel 13 og 14 i databeskyttelsesforordningen. Der er dog tale om en afgørelse, hvis der skal tages stilling til en klage fra den registrerede over manglende meddelelse, samt ved indsigelser mod databehandling.[29]

6.1 Sagens oplysning

6.1.1 Undersøgelsesprincippet

Enhver afgørelse drejer sig om, at de konkrete omstændigheder i en sag skal sammenholdes med et regelgrundlags beskrivelse af de faktiske omstændigheder, der skal være opfyldt, for at afgørelsen kan træffes. Myndigheden har ansvaret for at indhente alle relevante oplysninger. Det gælder både oplysninger af retlig karakter og af faktisk karakter. Hvad angår retsgrundlaget skal myndigheden fremskaffe de retskilder, som er relevante, og i den forbindelse undersøge, hvilke regler der er relevante for sagen. Der gælder desuden en pligt til at fortolke, hvor reglerne ikke er tilstrækkeligt klare, og ved at skønne, hvor der er overladt et skøn til forvaltningen.[30]

[26] Sten Bønsing: Almindelig forvaltningsret (2018) s. 84f.
[27] Sten Bønsing: Almindelig forvaltningsret (2018) s. 85
[28] Sten Bønsing: Almindelig forvaltningsret (2018) s. 85
[29] Sten Bønsing: Almindelig forvaltningsret (2018) s. 89-90
[30] Sten Bønsing: Almindelig forvaltningsret (2018) s. 147f.

Når en sag starter, har myndigheden en stor opgave med at få indhentet de faktiske forhold, som har betydning for sagen. Det vil sige, de oplysninger som er nødvendige for at kunne afgøre, om retsfaktum i sagen er opfyldt. De forhold kan variere alt efter sagen og kan indebære forhold som bopæl, sygdomsforhold, et barns trivsel, forholdene i et fremmed land, der truer en udlænding i en grad, der berettiger til asyl og mange andre forhold.

Det er som udgangspunkt forvaltningens opgave at indhente de faktiske oplysninger. Forvaltningen er underlagt en undersøgelsespligt, jf. Officialprincippet.[31] Det gælder både positive og negative forhold for borgeren. Myndigheden har pligt til at være neutral, når de indhenter oplysninger og skal arbejde for at opnå en materielt korrekt afgørelse i en given sag. Dette princip er generelt ulovbestemt, men der findes en række særområder, hvor der findes regler for indhentelse af oplysninger, såsom miljø, konkurrence og det sociale område. De ulovbestemte regler finder samtidig anvendelse med de lovbestemte love, medmindre andet er angivet i specialloven.[32]

Når forvaltningen har ansvaret for sagens oplysning, betyder det ikke, at forvaltningen har pligt til selv at fremskaffe oplysninger i sagen. Forvaltningen har pligt til at tage initiativ til at tilvejebringe alle oplysninger i sagen.[33] Myndigheden har altså muligheden for at pålægge den, som har lettest og nemmest ved at fremskaffe oplysninger (borgeren eller myndigheden) jf. FOB 2015-28. Dette er en generel tolkning af pligten og kan modificeres. Hvis det står i lov, så kan man lægge forpligtelsen til at fremskaffelse af oplysning over på parten. Dette kan både være direkte indskrevet i lovgivningen (byggelovens §16 om byggetilladelser) eller indirekte ved at lægge bevisbyrden over på parten såsom at indskrive, at ”*medmindre ansøgeren godtgør, at…*”.[34]

Myndigheden bestemmer selv, hvilke oplysninger der skal indhentes og inddrages. Parten må godt opfordre til oplysninger, men det er forvaltningen, der bestemmer, hvilke de vil anvende. Forvaltningen har dog pligt til at vurdere de oplysninger, parten foreslår. Er de relevante, vil de derfor få betydning for sagens oplysning. De relevante oplysninger skal indhentes fra forvaltningen, da de er nødvendige for at nå en korrekt materiel afgørelse.

Hvis loven giver myndigheden en skønsmulighed, bliver vurderingen af spørgsmålet sværere. Forvaltningen skal herved opklare, hvad der er relevant. Hvor mange oplysninger skal der indhentes? Til det er svaret; ”*der skal indhentes så mange og så detaljerede oplysninger, at der forsvarligt kan træffes en korrekt afgørelse*.”.[35] Det vil sige, der skal ikke indhentes flere oplysninger, end der er

[31] https://www.ombudsmanden.dk/myndighedsguiden/generel_forvaltningsret/officialprincippet/
[32] Sten Bønsing: Almindelig forvaltningsret (2018) s. 148
[33] Sten Bønsing: Almindelig forvaltningsret (2018) s. 148f
[34] Sten Bønsing: Almindelig forvaltningsret (2018) s. 149
[35] Sten Bønsing: Almindelig forvaltningsret (2018) s. 150

nødvendigt, hvilket stemmer overens med databeskyttelsesforordningen artikel 5, stk. 1, litra c. og delvist forvaltningslovens § 32 eller dennes princip.[36] Der kan derfor udledes et saglighedsprincip, hvis det ikke er sagligt nødvendigt for sagen, så skal det ikke indhentes.

Der gælder desuden et princip om fri bevisbedømmelse. Dette betyder, at det er forvaltning, der afgør, hvornår en sag er tilstrækkeligt oplyst, og hvilke oplysninger der skal indhentes. Den er derfor ikke bundet af faste skrevne regler. Afhængigt af sagens karakter skal der lægges vægt på betydningen for borgeren. Hvis det har stor betydning for borgeren, så vil indhentning af oplysninger nok være større, men hvis den har mindre betydning, så kan det være man ikke behøver helt så mange oplysninger for at kunne nå frem til det korrekt resultat.[37]

6.1.2 Notatpligt

Det følger af offentlighedslovens § 13, at forvaltningen har notatpligt, når den kommer i besiddelse af oplysninger, der har betydning for en sag. Det er ikke afgørende, hvordan forvaltningen får kendskab til oplysningerne, f.eks. ved en samtale, et møde, en orientering fra en kollega i forvaltningen, egne iagttagelser, oplysninger fra andre sager, søgeresultater fra internettet, oplysninger fra sociale medier mv. Notatpligten gælder også, hvis myndigheden modtager oplysninger i et format, som er dårligt egnet til arkivering f.eks. en sms. Her skal oplysningen noteres på en anden måde. Notatet skal laves "snarest mulig". Det vil sige indenfor kort tid, hvor oplysningerne er friske i erindringen.[38]

Notatpligten gælder for oplysninger om en sags "faktiske" grundlag. Ifølge forarbejderne skal dette afgrænses lidt bredere end blot "faktiske oplysninger". Notatpligten beror i højere grad på, hvilken funktion oplysningen har i myndighedens sagsbehandling, end om det er faktisk eller ej. Det centrale er, at det er en oplysning om en sags faktiske grundlag. Det afgørende for, om en oplysning skal noteres, er, om oplysningen er af en sådan karakter, at den bidrager til at supplere sagens bevismæssige grundlag eller i øvrigt tilvejebringes for at skabe klarhed med hensyn til sagens faktiske omstændigheder. Notatpligten omfatter således oplysninger, der indeholder en subjektiv præget stillingtagen til et forhold, for så vidt vurderingen er af betydning for den administrative bevisoptagelse. Desuden omfatter notatpligten "eksterne faglige vurderinger", f.eks. en videnskabelig eller teknisk vurdering af forhold, som skal indgå i myndighedens afgørelse.[39]

[36] Sten Bønsing: Almindelig forvaltningsret (2018) s. 149-151
[37] Sten Bønsing: Almindelig forvaltningsret (2018) s. 151-152
[38] Sten Bønsing: Almindelig forvaltningsret (2018) s. 153
[39] Sten Bønsing: Almindelig forvaltningsret (2018) s. 153

Forvaltningen har pligt til at notere alle væsentlige sagsekspeditionskridt i sager, hvor der vil blive truffet en afgørelse, jf. § 13, stk. 2. i offentlighedsloven. Dette gælder, f.eks. hvis der som led i sagens behandling indhentes godkendelse eller samtykke hos andre myndigheder, hvis sagen sendes til videre ekspedition hos en anden myndighed, hvis der gives aktindsigt, hvis aktindsigt ikke kan gives inden udløbet af 7-dagesfristen, hvis der iværksættes høring, hvis spørgsmål i sagen eller om sagens behandling kræver materiale fra parten, og i særdeleshed hvis en afgørelse meddeles mundtligt.[40]

Notatpligten gælder ikke, hvis oplysninger i øvrigt fremgår af sagens dokumenter, jf. offentlighedslovens § 13, stk. 1, 2. pkt., og § 13, stk. 2. Notatpligten gælder endvidere ikke jf. offentlighedslovens § 13, stk. 3 i forbindelse med strafferetsplejen.

Forskellige regler i speciallogivning kan gøre det nødvendigt for forvaltningen at tage noter. Den registrerede skal f.eks. gives indsigt efter databeskyttelsesforordningens artikel 15, stk. 1, litra c og g. Den registrerede har ret til at få oplyst, hvor de indsamlede oplysninger stammer fra. Hvis forvaltningen ikke notere disse oplysninger løbende, kan det være svært at opfylde. Formålet med notatpligten er, at forvaltningen skal kunne fungere og sagsbehandle, også selv om en sag skifter sagsbehandler undervejs. Det forventes, at myndigheden kan dokumentere/bevise, hvad der findes af oplysninger i en sag. En forsvarlig partshøring forudsætter, at sagens oplysninger foreligger i skriftlig form, da større og komplekse sager skal kunne behandles af flere medarbejdere. Øvrige medarbejdere skal kunne se, hvad der er foretaget i sagen. Derfor skal medarbejderne dokumentere, hvad der er foretaget i en sag, af hensyn til en eventuel ansvarsplacering (eller fritagelse for ansvar), revision, kontrol mv. Notater er forvaltningens hukommelse og er vigtige for den bevismæssige betydning under en prøvelse ved domstolene.[41]

6.1.3 Journaliseringspligt

Forvaltningsmyndigheder har pligt til at journalisere centrale dokumenter i sager, jf. offentlighedslovens § 15. Bestemmelsen er begrundet i, at den skal understøtte offentlighedsprincippet, hvilket er grunden til, at den er placeret i offentlighedsloven og ikke forvaltningsloven. Princippet skal nok ses som et bredere sagsbehandlingsprincip, som er begrundet i andre formål end blot offentlighed.[42] Jour-

[40] Sten Bønsing: Almindelig forvaltningsret (2018) s. 154
[41] Sten Bønsing: Almindelig forvaltningsret (2018) s. 155
[42] Sten Bønsing: Almindelig forvaltningsret (2018) s. 156

nalisering giver generelt en større sikkerhed for, at sager behandles korrekt, og at der træffes de materielt rigtige afgørelser, idet det overordnet sikrer, at den enkelte medarbejder har det fulde overblik over en sag og at forskellige medarbejdere kan håndtere den samme sag. Journaliseringspligten sikrer, at forvaltningen har lettere ved at identificere dokumenterne i en sag, at forvaltningen har det fulde overblik over en sags dokumenter, og at sager behandles ens.[43]

Journaliseringspligten gælder kun for dokumenter, der modtages og afsendes af myndigheden, samt interne dokumenter i endelig form, herunder i særdeleshed § 13-notater. Herudover er journaliseringspligten kun krævet for dokumenter, der er led i "administrativ sagsbehandling". Der er et krav om, at dokumenterne har betydning for en sag eller sagsbehandling i øvrigt.[44] Mange dokumenter vil derfor ikke have betydning for et sagsforløb og behøver derfor ikke journaliseres, medmindre de har haft en "faktisk" betydning for sagen eller sagsbehandlingen.

Journaliseringspligtens indhold betyder, at der skal indrettes et system, hvor forvaltningen noterer kerneoplysninger om de journaliseringspligtige dokumenter, jf. offentlighedslovens § 15, stk. 3. Disse kerneoplysninger er, dato for dokumentets modtagelse eller afsendelse og en kort tematisk angivelse af dokumentets indhold (f.eks. partshøring af xx). Journaliseringssystemet er derfor et selvstændigt system, hvor der er en oversigt over de centrale (eller alle) dokumenter i en sag. Dokumenterne skal journaliseres "snarest muligt", jf. § 15, stk. 2, praksis siger dette er ca. indenfor 7 arbejdsdage, men kan variere afhængigt af følsomme dokumenter.

Der er en særskilt ret til aktindsigt i journaloversigten vedr. en konkret sag, jf. offentlighedslovens § 7, stk. 2, nr. 2. Journaliseringspligten gælder statslige forvaltningsmyndigheder omfattet af offentlighedslovens § 2 samt centrale kommunale og regionale forvaltninger.[45]

6.2 Partsbegrebet

For at kunne anvende forvaltningslovens regler om partsindsigt er det vigtigt først at fastlægge, hvad der menes med en part. I forvaltningsloven findes der ikke en definition af partbegrebet, men igennem forvaltningsrettens udvikling er partsbegrebet defineret som "*Den umildbare adressat for en konkret afgørelse*".[46] Ud over parter, som er direkte adressater i en afgørelses sag, kan partsbegrebet også omfatte andre. Dette kaldes det udvidede partsbegreb. Formålet med det udvidede partsbegreb er at andre, som ikke direkte er medvirkende i en afgørelse, stadig kan blive påvirket af afgørelsen. Derfor

[43] Sten Bønsing: Almindelig forvaltningsret (2018) s. 155f
[44] Sten Bønsing: Almindelig forvaltningsret (2018) s. 156
[45] Sten Bønsing: Almindelig forvaltningsret (2018) s. 157
[46] Sten Bønsing: Almindelig forvaltningsret (2018) s. 93

gives disse personer partsrettigheder. For at kunne blive anset som part, når man ikke er direkte adressat, skal personen opfylde tre kriterier: Direkte-, væsentlig- og individuel interesse. Hvis et af disse kriterier er særligt fremtrædende i sagen, kan der slækkes lidt på et andet. Det er derfor vigtigt, at der er tale om en samlet vurdering.[47] Partsbegrebet er derfor ikke kun omfattet af fysiske personer, men juridiske personer kan også være parter i en sag.[48]

6.2.1 Partsindsigt

I forvaltningen er der flere forskellige måder, en borger kan søge aktindsigt. Der er reglerne i Databeskyttelsesforordningens artikel 15, Forvaltningslovens §§ 9-10, Offentlighedslovens §§ 7-8 og særlovgivning, som ikke bliver belyst i denne afhandling. I følgende afsnit vil afhandlingen beskrive, hvordan og hvornår man kan søge aktindsigt efter forvaltningslovens regler, samt i hvilket omfang der gives aktindsigt.

I forvaltningen gælder der et princip om gennemsigtighed. En af måderne, forvaltningen har skabt gennemsigtighed, er ved hjælp af aktindsigt. For at kunne anvende forvaltningslovens regler om aktindsigt skal pågældende, som søger aktindsigt, være part i en afgørelsessag. Ovenfor i afsnit 6.2 er partsbegrebet beskrevet.

Det fremgår af forvaltningslovens § 9, stk. 1. at en part i en afgørelsessag kan forlange at blive gjort bekendt med sagens dokumenter. Der er ingen krav til begrundelsen for aktindsigt, da der kan være flere årsager hertil. Der kan være tale om ren nysgerrighed, eller at en borger vil klage over en afgørelse, som forvaltningen har foretaget. Derfor skal der være mulighed for at se, hvordan sagen er blevet behandlet.[49] Borgeren skal dog opfylde identifikationskravet i forvaltningslovens § 9a. Det vil sige, at borgeren skal angive, hvilken sag der er tale om. Når borgeren angiver, hvilken sag der er tale om, er det nok, at borgeren angiver sit navn samt en kort beskrivelse af sagstypen.[50] Hvis borgeren har meget sparsomme oplysninger, skal forvaltningen stadig hjælpe, da der påhviler dem en vejledningspligt efter forvaltningslovens § 7.[51] Som beskrevet ovenfor har borgeren ret til at blive gjort bekendt med sagens dokumenter. Begrebet dokumenter skal anses i bred forstand, da dokumenter omfatter mange typer af oplysninger, f.eks. mails, foto, papir, sms osv. Det må derfor antages, at dokumentbegrebet er teknologineutralt, hvilket vil sige, at det er lige meget, om der er tale om fysiske

[47] Sten Bønsing: Almindelig forvaltningsret (2018) s. 93-94
[48] Sten Bønsing: Almindelig forvaltningsret (2018) s. 92
[49] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 201-202
[50] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 202
[51] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 202

eller elektroniske dokumenter.[52] Visse dokumenter kan være undladt, hvis de ikke vurderes som betydningsfulde for sagen. Eksempler på undladte dokumenter kunne være post-its og sms.

Ligeledes fremgår det af forvaltningslovens § 9, stk. 2. at der er adgang til aktlister. Det kan være en fordel at få indsigt i aktlister, hvis en sag spænder sig over utroligt mange sider, da det kan bidrage til et overblik af sagen. Hvis listen kun omfatter journaliseringspligten efter offentlighedslovens § 15, vil aktlisten ikke være komplet.[53]

I forbindelse med retten til at søge aktindsigt gælder der en række undtagelser. Undtagelserne fremgår af forvaltningslovens §§ 11-15 og omfatter visse sager, dokumenter og oplysninger, som man ikke kan få aktindsigt i.

Den første undtagelse er, at en borger ikke kan søge om en almindelig aktindsigt efter forvaltningslovens § 9, stk. 1., hvis der behandles en administrativ straffesag på borgeren, jf. Forvaltningslovens § 12. Borgeren vil her skulle benytte reglen om aktindsigt efter forvaltningslovens § 18. Denne afhandling vil ikke komme nærmere ind på reglerne om aktindsigt i administrative straffesager, da dette ikke er omfattet af problemformuleringen.[54]

Den anden undtagelse er, at en borger ikke har adgang til alle dokumenter, som er benyttet i en sag. Det fremgår af forvaltningslovens § 12, at aktindsigten ikke omfatter interne arbejdsdokumenter. Begrebet interne dokumenter skal forstås som dokumenter, der bliver brugt til f.eks. udkast om afgørelser, planer, brevveksling mellem kommunalbestyrelse og dennes udvalg, mv. samt udarbejdelse af referater fra interne møder. Grunden til denne undtagelse er, at man ikke vil offentliggøre de interne beslutningsprocesser, hvorved medarbejdere kan føle sig overvåget i deres daglige sagsbehandling. Frygten er da, at de interne dokumenter ikke vil blive udarbejdet.[55] Bestemmelsen strider på den ene side imod offentlighedsprincippet, men frygten for, at dokumenterne ikke vil blive udarbejdet, vægter højere. Det skal nævnes, at forvaltningen har pligt til at overveje meroffentlighed efter § 14 i offentlighedsloven.

Hvis et internt dokument skulle blive udleveret til en borger ved en fejl, mister dokumentet automatisk sin karakter som et internt dokument, jf. Forvaltningslovens § 12, stk. 2. Hvis afgivelsen sker på et retligt grundlag, altså at en anden myndighed rekvirerer det i forbindelse med en høring, vil det ikke miste sit grundlag som et internt arbejdsdokument, jf. Forvaltningslovens § 12, stk. 2.[56]

[52] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 202-203
[53] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 203-204
[54] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 205-206
[55] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 206
[56] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 207-208

Det fremgår af forvaltningslovens § 13, at visse interne dokumenter er omfattet af aktindsigten. Af § 13, stk. 1, nr. 1. fremgår det tydeligt af ordlyden, at der er tale om gengivelser af myndighedens beslutning vedrørende en sags afgørelse. Det fremgår af § 13, stk. 1, nr. 2, at dokumenter som alene indeholder gengivelser af oplysninger, som en myndighed har haft pligt til at notere sig, ikke er undtaget for aktindsigt. Der er her tale om § 13-notater jf. offentlighedsloven. Det fremgår af § 13, stk. 1, nr. 3, at *"dokumenterne er selvstændige dokumenter, der er udarbejdet af en myndighed for at tilvejebringe bevismæssig eller anden tilsvarende klarhed med hensyn til en sags faktiske omstændigheder."*[57] Dette vil sige dokumenter som besigtigelsesrapporter og afhøringsrapporter.

Det fremgår af forvaltningslovens § 14, at man ikke kan fortage aktindsigt i dokumenter af særlig karakter. Ordlyden beskriver, hvilke dokumenter der ikke kan foretages aktindsigt i, jf. forvaltningslovens § 14, nr. 1-3, statsrådsprotokoller, dokumenter der udvikles mellem en myndighed, som udfører sekretariatsopgaver for en anden myndighed, og myndigheders brevveksling mellem sagkyndige til brug i retssager.

Dokumenter, som er undtaget af forvaltningslovens § 14 kan dog, hvis de vedrører sagens faktiske grundlag, begæres aktindsigt i, jf. forvaltningslovens § 14 a. Denne pligt kaldes ekstraheringspligten. Dokumenter som kunne være omfattet af denne paragraf, kunne være metoder og forudsætninger, som forvaltningen har anvendt ved fastlæggelsen af de faktuelle oplysninger.[58]

Den tredje kategori af undtagelser er oplysninger, som er undtaget fra aktindsigten, jf. Forvaltningslovens §§ 15-15b. Denne form for undtagelser medvirker, at borgeren stadig kan få aktindsigt i sin sag, da undtagelserne kun dækker visse oplysninger i en sag og ikke hele sager.[59]

Det fremgår af forvaltningslovens § 15, at aktindsigten kan begrænses, hvis det er vigtigt for statens sikkerhed eller rigets forsvar, medmindre partens interesse i at benytte kendskabet til sagens dokumenter for at varetage sine egne interesser taler imod. Denne bestemmelse bruges sjældent, da sådanne oplysninger normalt ikke benyttes i en sag for en almindelig borger. Det fremgår af forvaltningslovens § 15 a, stk. 1. at aktindsigt kan begrænses i henhold til udenrigspolitiske hensyn. Her kan der være tale om informationer, der ikke må videregives, såfremt de kommer fra specielle organisationer eller lande.[60] Retten til aktindsigt kan endvidere begrænses i det omfang partens interesse i at kunne benytte kendskabet til sagens dokumenter til varetagelse af sit tarv efter en konkret vurdering, jf. forvaltningslovens § 15 a, stk. 2.[61]

[57] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 209
[58] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 209-210
[59] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 213
[60] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 214
[61] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 214

Det fremgår af forvaltningslovens § 15 b, at retten til aktindsigt kan begrænses i det omfang partens interesse i at kunne benytte kendskab til sagens dokumenter til varetagelse af sit tarv findes at burde vige for afgørende hensyn til forebyggelse og opklaring af lovovertrædelser. Forvaltningslovens § 15 b, nr. 1-5. opstiller i hvilke situationer undtagelsen finder anvendelse.[62]

6.3 Offentlighedsloven

Som anført i afsnit 6.2.1 kan der anmodes om aktindsigt efter flere regelsæt. I dette afsnit vil afhandlingen behandle reglerne om almindelig aktindsigt også kaldt ”dokumentoffentlighed”. Den grundlæggende forskel mellem aktindsigtsreglerne efter offentlighedsloven og forvaltningsloven er navnlig, at forvaltningslovens regler om aktindsigt kun omhandler parters aktindsigt, hvorimod reglerne om aktindsigt efter Offentlighedsloven omhandler åbenhed i forvaltningen, som kommer til udtryk i offentlighedslovens § 1.[63]

Offentlighedsloven er et meget bredt regelsæt, som giver alle ret til aktindsigt i dokumenter fra forvaltningen, jf. offentlighedslovens § 7. Ligesom ved partsindsigt gælder der heller ikke nogen begrundelse for, hvorfor man søger aktindsigt. Som udgangspunkt gælder aktindsigt alle dokumenter i forvaltningen.[64] Dokumenterne skal indgå som led i en administrativ sagsbehandling. Det betyder, at dokumenter, der kun modtages til arkivering, ikke er omfattet af aktindsigten. Dokumenter er først omfattet af aktindsigten dagen efter, jf. offentlighedslovens § 7, stk. 3. Samtidig er der ikke ret til løbende aktindsigt, hvilket betyder, at forvaltningen ikke sender dokumenter løbende.[65]

Når borgere beder om aktindsigt skal de kunne identificere sagen, jf. offentlighedslovens § 9. Borgeren skal ikke kunne angive selve journalnummeret, men skal være i stand til at beskrive, hvad der indgår i sagen, og hvad den handler om. Det kunne f.eks. være et navn på en part, tidspunktet for sagen eller lignende. Dernæst skal borgeren angive det tema, som sagen drejer sig om, f.eks. ”ansøgning om ret til hjælpemidler”.[66] Som beskrevet i det tidligere afsnit 6.2.1 har forvaltningen en vejledningspligt, som skal opfyldes i de tilfælde, hvor borgeren har sparsomme oplysninger om en sag, jf. forvaltningslovens § 7.

En ansøgning om aktindsigt kan afslås, hvis den udgør et uforholdsmæssigt ressourceforbrug, jf. offentlighedslovens § 9, stk. 2, nr. 1. Det kan skyldes sagens omfang, fordi det vil tage for lang tid

[62] Sten Bønsing: Forvaltningsret - Lærebog for statskundskab (2018) s. 214-215
[63] Sten Bønsing: Almindelig forvaltningsret (2018) s. 258
[64] Sten Bønsing: Almindelig forvaltningsret (2018) s. 259
[65] Sten Bønsing: Almindelig forvaltningsret (2018) s. 260-261
[66] Sten Bønsing: Almindelig forvaltningsret (2018) s. 262

for forvaltningen at gå alle papirer igennem og sikre, at alle oplysninger, som er omfattet af aktindsigten, bliver udleveret, og at andet bliver slettet eller aggregeret. Umildbart skal der ikke bruges mere end 25 timer på en sag om aktindsigt.[67]

I henhold til offentlighedsloven gælder der en række undtagelser til aktindsigten. Afhandlingen vil ikke uddybe alle undtagelserne, men forklare nogle og ellers orientere om, hvor de andre undtagelser kan findes. Ligesom ved partsindsigt gælder der undtagelser for sager. Undtagelserne findes i §§ 19-22 og omhandler sager omkring strafferetsplejen, lovgivning, personalesager og kalender.[68] Undtagelser om dokumenter findes i §§ 23-29 og omhandler dokumenter, der vedrører Ministerbetjening, sager mellem KL, Danske Regioner mv., interne dokumenter, skuffecirkulærer, særlige dokumenter, folketingspolitikerreglen mv.[69]

Den tredje kategori af undtagelser er oplysninger som fremgår af offentlighedslovens §§ 30-34. En af de store forskelle på partindsigt og almindelig aktindsigt er, at du for sidstnævnte ikke kan få oplysninger om enkeltpersoners private, herunder økonomiske forhold, jf. offentlighedslovens § 30, nr. 1. Dette betyder, at man ikke har ret til, at få informationer om en privat persons personlige forhold. Det kan være race, religion, cpr-nummer, helbred, privat økonomi mv. De samme regler gælder for virksomheder. Der kan derfor ikke udleveres informationer om drift eller forretningsforhold, jf. offentlighedslovens § 30, nr. 2.[70]

I vidt omfang minder §§ 31-33 om §§ 15-15 b i forvaltningsloven og omhandler hensyn til statens sikkerhed, hensyn til udenrigspolitiske interesser og opklaring af forbrydelser. Den sidste undtagelse af oplysninger er § 34. Det fremgår af paragraffen, at hvis en del af dokumentet indeholder oplysninger, som er undtaget efter §§ 30-33 skal der gives delvis aktindsigt. De undtagende oplysninger skal derfor fjernes før udleveringen.[71]

Den sidste undtagelse er § 35 som omhandler tavshedspligt.

6.3.1 Meroffentlighed

Det er klart, at der findes undtagelser til aktindsigten, men i nogle tilfælde skal der gives aktindsigt efter offentlighedslovens § 14, stk. 1., også kaldet ”meroffentlighedsprincippet”. Denne paragraf medvirker, at der kan gives aktindsigt i et videre omfang, end hvad det følger af offentlighedsloven

[67] Sten Bønsing: Almindelig forvaltningsret (2018) s. 263
[68] Sten Bønsing: Almindelig forvaltningsret (2018) s. 269-272
[69] Sten Bønsing: Almindelig forvaltningsret (2018) s. 272-278
[70] Sten Bønsing: Almindelig forvaltningsret (2018) s. 278-279
[71] Sten Bønsing: Almindelig forvaltningsret (2018) s. 279-282

§§ 23-35.[72] Når en borger efter undtagelserne i §§ 23-35 ikke har ret til aktindsigt, har forvaltningen som udgangspunkt en pligt til at overveje meroffentlighed. Forvaltningen skal her tage hensyn til ansøgere, som har en særlig interesse. Eksempler på folk med en særlig interesse er forskere og journalister.[73] Meroffentlighed kan ikke anvendes, hvis det bryder reglerne om tavshedspligt, særligt undtagelserne i §§ 30-33 vil man oftest ikke kunne anvende meroffentlighed på, da der her hviler en tavshedspligt hos forvaltningen. Det vil oftest være muligt at anvende meroffentlighed på interne dokumenter som er omfattet af §§ 23-24 (arbejdsdokumenter), hvis disse ikke konkret har behov for beskyttelse. Dokumenter og oplysninger vil der være mulighed for at anvende meroffentlighed efter offentlighedslovens §§ 19-21, jf. § 14, stk. 2.[74] Hvis der gives afslag om meroffentlighed skal det begrundes efter forvaltningslovens §§ 22-24. Begrundelsen behøves ikke at være specielt detaljeret, men den skal alligevel angives og forklares, da der er tale om en afgørelse fra forvaltningen.[75]

[72] Sten Bønsing: Almindelig forvaltningsret (2018) s. 264
[73] Sten Bønsing: Almindelig forvaltningsret (2018) s. 264-265
[74] Sten Bønsing: Almindelig forvaltningsret (2018) s. 265
[75] Sten Bønsing: Almindelig forvaltningsret (2018) s. 266

7. Databeskyttelsesforordningen

7.1 Legal definitioner

7.1.1 Personoplysninger

Som det fremgår af Databeskyttelsesforordningen, er denne blevet til med et formål om at beskytte enhvers persondata i Den Europæiske Union. En helt central bestemmelse i databeskyttelsesforordningen må derfor være personoplysninger. I databeskyttelsesforordningens artikel 4, nr. 1. fremgår det, at en personoplysning er: *"enhver form for information om en identificeret eller identificerbar fysisk person"*, også kaldet "den registrerede". For at kunne forstå, hvordan en fysisk person direkte eller indirekte kan identificeres må vi kigge længere nede i artikel 4, nr. 1. hvor det fremgår at: *"... ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet".*

Det fremgår af databeskyttelsesforordningens præambelbetragtning nr. 26, at alle midler må tages i brug, som med rimelighed vil kunne anvendes af den dataansvarlige til direkte eller indirekte, at kunne identificere den udpegede person. For at bestemme, hvilke midler der falder inden for rimelighedens grænser, fremgår det af betragtningen, at flere objektive forhold skal vurderes. Det kan være omkostninger samt den tid, der anvendes til identifikation.[76]

Når der nævnes personoplysninger, sondres der mellem 3 forskellige typer.

1) Almindelige personoplysninger.

2) Straffedomme og lovovertrædelser.

3) Følsomme personoplysninger.

De almindelige personoplysninger er oplysninger, som ikke er omfattet af begrebet "følsomme personoplysninger". De følsomme personoplysninger fremgår af databeskyttelsesforordningens artikel 9, hvor der er tale om en udtømmende liste. Almindelige personoplysninger kan således være: "*identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre rent private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato og -stilling, arbejdsområde og arbejdstelefon".*[77]

[76] Betænkning nr. 1565 side. 58

[77] https://www.datatilsynet.dk/databeskyttelse/hvad-er-personoplysninger

Herunder skal man være opmærksom på, at et CPR-nummer, hverken er klassificeret en almindeeller følsom personoplysning, men derimod som en fortrolig oplysning, og bliver behandlet i databeskyttelsesforordningens artikel 11.

Straffedomme og lovovertrædelser må umiddelbart antages for at være almindelige personoplysninger, hvilket fremgår af databeskyttelsesforordningens artikel 10. Nationalt er dette reguleret i databeskyttelsesloven § 8 og bliver her anset som fortrolige oplysninger. Straffedomme og lovovertrædelser, vil ikke blive behandlet nærmere i denne afhandling, da det ikke har relevans for afhandlingens problemformulering.

Den sidste form for personoplysninger er følsomme personoplysninger. Det fremgår af databeskyttelsesforordningens artikel 9, stk. 1. at følsomme personoplysninger er*:*
"race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering".[78]
Som forklaret ovenfor er denne liste udtømmende. Oplysningerne, som ikke fremgår af denne artikel, må derfor anses for at være almindelige personoplysninger. Det er som udgangspunkt ikke tilladt at behandle følsomme personoplysninger. Der findes dog en række undtagelser, som fremgår af artikel 9, stk. 2, litra a-j. Disse er ikke nærmere forklaret, da dette afsnit er for en basisviden om personoplysninger.

Modsat følsomme personoplysninger, behøves der ikke samme snævre hjemmel til at behandle almindelige personoplysninger. Her vil man fortage en konkret vurdering af, hvorvidt der "behandles" data. I visse tilfælde vil der skulle indhentes samtykke for at kunne behandle data. Et sådant samtykke gives ofte i form af en kontrakt eller e-kontrakt. Denne form for samtykke anvendes f.eks. ved jobansøgninger, hvor man giver en juridisk person lov til at opbevare og behandle sine data. Derfor er det vigtig, at databehandleren ikke skal indhente samtykke, hver gang persondata skal behandles. Et eksempel kan være en bankrådgiver, der skal finde en kunde i deres database eller indstille til et lån. Her vil der typisk gives et samtykke til behandling af ens data ved oprettelse af kundeforholdet.

[78] Generel informationspjece om databeskyttelsesforordningens fra Datatilsynet side. 7. afsnit 3.1

7.1.2 Pseudonymisering

Et begreb som ligger tæt op ad personoplysninger er pseudonymisering, det fremgår af databeskyttelsesforordningens artikel 4, nr. 5. at pseudonymisering er:

"behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger…".

Når der skal anvendes supplerende oplysninger, er der et krav om, at de opbevares separat og er underlagt tekniske samt organisatoriske foranstaltninger som gør, at man ikke kan henføre dem til en identificerbar- eller identificeret person.[79] Eftersom pseudonymisering gør en personoplysning til en "ikke-identificerbar personoplysning" vil der stadig være tale om en personoplysning, jf. punkt 1 under kommentaren til artikel 4, nr. 1.[80] Pseudonymisering er derfor bare en foranstaltning som kan benyttes for at overholde behandlingssikkerheden i artikel 32, stk. 1, litra a.

7.1.3 Dataansvarlig og databehandler

Det fremgår af databeskyttelsesforordningens artikel 4, nr. 7, at en dataansvarlig er:

"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret".

Den dataansvarlige er enten en fysisk eller juridisk person. Det er vigtigt at kunne udpege den dataansvarlige, da det er den dataansvarliges job at sikre, det offentlige eller den private virksomhed lever op til reglerne i databeskyttelsesforordningen.

Det er den dataansvarliges job at sikre, den offentlige myndighed og dens databehandler har lov til at behandle oplysninger, som de er i besiddelse af (også kaldt behandlingshjemmel). Den dataansvarlige skal sikre, at den offentlige forvaltning er i stand til at imødekomme den registrerede persons rettigheder, herunder oplysninger om udlevering af materiale til tredjemand, oplysningspligten eller give den registrerede indsigt i sine data. Til sidst skal den dataansvarlige sikre sig at indberette eventuelle brud på persondatasikkerheden til Datatilsynet inden for 72 timer. Ved behandling af

[79] Databeskyttelsesforordningens artikel 4(7)
[80] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 265

data er det normalt, at den dataansvarlige betaler de omkostninger, der er i forbindelse med behandling af personoplysningerne.[81]

Fælles dataansvar betyder, at to eller flere dataansvarlige i fællesskab fastlægger formålene med behandlingen og hjælpemidlerne hertil. For at skabe gennemsigtighed skal der foreligge en aftale, der beskriver hver af de dataansvarliges ansvarsområder, for at den registrerede kan gennemskue, hvem de skal henvende sig til. Den registrerede har dog frit valg til at vælge, hvem de henvender sig til, hvorefter de dataansvarlige internt må afklare forholdet.[82]

Under den dataansvarlige er databehandleren. Det fremgår af databeskyttelsesforordningens artikel 4, nr. 8. at en databehandler er *"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne".* Det vil sige, at databehandleren ikke selv må bestemme, hvilke data, der skal behandles, samt med hvilket formål behandlingen skal ske. Dette er nemlig den dataansvarliges job. Grunden til denne opdeling er af hensyn til den registreredes sikkerhed. Det skal være muligt for den registrerede at henvende sig til den rigtige person, "den dataansvarlige", hvis den registrerede person ønsker at anvende sin ret til bl.a. at få indsigt, at blive glemt mv.

7.1.4 Begrebet behandling

Det fremgår af databeskyttelsesforordnings artikel 4, nr. 2. at begrebet behandling skal forstås som "*enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for"*. Det er vigtigt, at bestemmelsen ikke nævner en udtømmende liste af eksempler.[83] Eksemplerne kan være almindelig sagsbehandling og sletning. Sletning vil dog medføre, at personoplysningerne ikke længere vil være identificerbare, hvorved oplysningerne ikke længere er omfattet af databeskyttelsesforordningen.[84]
I midlertidig er det vigtig at have for øje, at ikke alt anvendelse af data skal anses for at være en behandling. Er der f.eks. tale om en dataansvarlig overlader personoplysninger til en databehandler kan det ikke anses for være en behandling.[85]

[81] Datatilsynet vejledning til dataansvarlige og databehandlere, s. 6.
[82] https://gdprguide.arkivo.dk/vaelg-emne/ansvar-roller/faelles-ansvar
[83] Peter Blume: Den nye persondataret (2016), s. 59
[84] Peter Blume: Den nye persondataret (2016), s. 59
[85] Betænkning nr. 1565/2017, s. 59

7.1.5 Register

Det fremgår af databeskyttelsesforordningens artikel 4, nr. 6, at et register er:

"... enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag"

Det fremgår af bestemmelsen, at manuelle registre er omfattet af dette begreb. Manuelle registre er f.eks. fortegnelser og kartotekskasser. Der skal være tale om let tilgængelige data, hvor samme sikkerhedsregler skal anvendes ligesom ved digital behandling. Det er derfor vigtigt, at disse data bevares struktureret og vedrører bestemte personer, således at der er en let søgbarhed i materialet. Det der klassificerer et register er, at der er etableret en søgbarhed, som skaber en tilgængelighed.[86]

7.1.6 Tredjemand

Det fremgår af databeskyttelsesforordningens artikel 4, nr. 10. at begrebet tredjemand skal forstås således:

"en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger"

Begrebet tredjemand er vigtigt at definere, da det kan have stor betydning for, hvorvidt den dataansvarlige har ret til at behandle den pågældendes data. Samtidig kan definitionen have betydning for, om den dataansvarlige videregiver personoplysninger, jf. Databeskyttelsesforordningens artikel 6, stk. 1, litra f.[87]

7.1.7 Samtykke

En af de vigtige begreber i databeskyttelsesforordningen er samtykke. Grunden til at dette begreb er vigtig er, at den dataansvarlige skal have samtykke for at den registreredes persondata kan behandles, jf. databeskyttelsesforordningens artikel 6 og 9.

Det fremgår af artikel 4, stk. 11 at samtykke fra den registrerede er:

"enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling".

[86] Peter Blume: Den nye persondataret (2016), s. 60

[87] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020) s. 284

Som nævnt ovenfor er samtykke vigtigt for lovligt at kunne behandle persondata. For at komme nærmere ind på, hvornår der foreligger samtykke, henvises der til databeskyttelsesforordningens præambelbetragtning nr. 32. Det fremgår heraf, at samtykke gives i form af en utvetydig bekræftelse, som både er informeret, specifik og frivillig, hvorved der accepteres at ens personoplysninger må blive behandlet.[88] Samtykket skal være specifikt, da det skal angive, hvilke formål behandlingen har. Det vil derfor betyde, at kravet om et informeret samtykke kan være vanskeligt at opfylde, da den dataansvarlige skal sikre sig, at den registrerede har kendskab til, hvad behandlingen tilsigter at realisere.[89]

Som det fremgår ovenfor, skal samtykket være utvetydigt, det vil sige, der ikke skal være tvivl om, at der er givet samtykke til behandlingen. Det fremgår således af databeskyttelsesforordningens artikel 7. nr. 1, at den dataansvarlige har bevisbyrden for, at der er givet et utvetydigt samtykke.[90]

Et samtykke skal være frivilligt før det er gældende. Det vil sige, at et samtykke som er fremskaffet under tvang samt magtudøvelse ikke kan klassificeres som et gyldigt samtykke. Et samtykke vil derimod stadig være frivilligt selv om det skyldes en modydelse. Det fremgår af databeskyttelsesforordningens præambelbetragtning nr. 42 at et samtykke ikke bør anses som frivilligt hvis "*... den registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende".*

Måder, hvorpå man kan opnå samtykke, kan være både mundtlige, skriftlige eller elektroniske erklæringer. Et eksempel herpå kan være hjemmesider, hvor man sætter kryds i cookies og giver samtykke til anvendelse af ens persondata, såsom ip-adresse. Et andet eksempel kunne være behandling af oplysninger ved en jobansøgning, hvor man giver pågældende virksomhed lov til behandling af sine persondata.

Det fremgår af databeskyttelsesforordningens artikel 7, stk. 3, at man altid har muligheden for at tilbagekalde et samtykke. Et samtykke skal ikke anses for at være en bindende aftale. Ved tilbagekaldelse af et samtykke gælder der ikke et formkrav. Det betyder, at et samtykke ikke behøver at blive tilbagekaldt på samme måde som det er fremskaffet.[91] Det eneste krav for en tilbagekaldelse er, at det gives til den dataansvarlige. Den dataansvarlige har derfor bevisbyrden for, om et samtykke er kaldt tilbage eller ej.[92] Såfremt et samtykke er tilbagekaldt, må alt fremtidig behandling af den registreredes data ikke foretages. Den registrerede skal informeres i forbindelse med sit samtykke om, hvorvidt det

[88] Betænkning nr. 1565 bind. 1. s. 63
[89] Peter Blume: Den nye persondataret (2016), s. 64
[90] Peter Blume: Den nye persondataret (2016), s. 64
[91] Peter Blume: Den nye persondataret (2016), s. 66
[92] Peter Blume: Den nye persondataret (2016), s. 66

er muligt, at det kan tilbagekaldes, da det skal være en let proces for den registrerede at tilbagekalde et samtykke.[93]

7.2 De grundlæggende principper

I Databeskyttelsesforordningens kapitel II, artikel 5-11, er der fastsat bestemmelser om, i hvilket omfang behandling af personoplysninger må finde sted. Bestemmelserne skal sammenholdes med databeskyttelseslovens kapitel 3, §§ 5-8.[94] I denne afhandling, tages der udgangspunkt i artikel 5, hvor de mest grundlæggende principper for den dataansvarliges behandling af personoplysninger findes. Artikel 6-11 beskriver behandlingsreglerne, da artikel 5 ikke giver den dataansvarlige en selvstændig retlig hjemmel til behandling af oplysninger.[95] Der er valgt et fokus på artikel 5, da disse regler altid skal iagttages, selvom hjemlen til behandling kan fremkomme af et andet artikelnummer. Retstilstanden vil derfor være iagttaget, da forordningens artikel 5 er det samme som den tidligere persondatalovs § 5 og databeskyttelsesdirektivets artikel 6 med mindre justeringer, så der blot er tale om en videreførelse af gældende ret.[96]

Når afhandlingen vælger at uddybe artikel 5, skal grunden findes i denne overførsel af tidligere regler. God databehandlingsskik er ikke blot en juridisk disciplin, men en genstand for en etisk filosofi. Formålet for databeskyttelsesforordningen har været at gøre reglerne mere konkrete og relevante.

Når private virksomheder og offentlige myndigheder behandler personoplysninger, skal de overholde de generelle regler i databeskyttelsesforordningen. Hvis de ikke gør dette, så har de etisk fejlet, men kan samtidig blive juridisk ansvarlige og derved sanktioneres med kæmpe bøder for eventuelle brud på forordningen.

7.2.1 Lovlighed, rimelighed og gennemsigtighed

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 1, litra a:

”*Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.”*

[93] Peter Blume: Den nye persondataret (2016), s. 66
[94] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 309-311
[95] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 313
[96] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 313

Hvad angår kravet om lovligt og rimeligt efter litra a, har det samme ordlyd som det tidligere databeskyttelsesdirektiv og persondatalov. Bestemmelsen fastsætter en form for god databehandlingskik efter de tidligere regler, som tilsynsmyndighederne er forpligtet til at følge.

Gennemsigtighedsprincippet er nyt i forhold til databeskyttelsesdirektivet og persondataloven. Det fremgår dog af Databeskyttelsesforordningens præambelbetragtning nr. 39 at princippet om gennemsigtighed betyder, "*at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klar og enkelt sprog*".[97] Dette kan findes i den dataansvarliges oplysningspligt efter artikel 13 og 14. Kravet om, at personoplysninger skal behandles på en gennemsigtig måde, kan således ikke antages at medføre en ændring i den gældende retstilstand.

Den tidligere tilsynspraksis vedrørende god databehandlingsskik gælder derfor stadig. Der er flere eksempler, hvor dette har været relevant. Her kan nævnes restriktionerne i anvendelsen af kreditoplysninger ved stillingsbesættelse, jf. pkt. 3, under kommentaren til databeskyttelseslovens § 20, stk. 1, og en pligt til at efter indsigelsens karakter, at notere den registrerede persons indsigelse mod oplysningers rigtighed mv., jf. kommentaren til forordningens artikel 16.[98]

Datatilsynet har under persondataloven med henvisning til § 5, stk. 1, i visse tilfælde stillet krav om underretning af berørte personer i tilfælde af brud på persondatasikkerheden. Dette forhold bliver nu reguleret i artikel 33. jf. betragtning 39. Fysiske personer skal gøres bekendt med risici, regler og garantier og rettigheder i forbindelse med behandling af personoplysninger. Hidtidig praksis har derfor stadig betydning i den nuværende forordning. Datatilsynet har i Dt.s j.nr. 2011-632-0103, fundet det beklageligt, at oplysninger om to borgere var blevet udleveret til en uvedkommende person i forbindelse med aktindsigt i akter fra et elektronisk dokumenthåndteringssystem. Datatilsynet fandt, at den pågældende myndighed ikke havde levet op til kravet om nødvendige sikkerhedsforanstaltninger, men noterede sig, at der var iværksat en række foranstaltninger, som skulle sikre, at det ikke ville ske igen. Tilsynet bemærkede desuden, at myndigheden burde have taget initiativ til at få slettet denne udleverede information for at begrænse skaden. Dette var imod princippet om god databehandlingsskik. Denne pligt stemmer overens med artikel 34 i databeskyttelsesforordningen.

I Google Street View Wifi-sagen, Dt.s j.nr. 2010-215-0469 var der indsamlet personoplysninger uden at opfylde kravene i persondataloven, da Google ikke havde grundlag for opbevaring af oplysningerne. Datatilsynet sagde, at Google straks skulle slette disse, men andre datatilsynslande gjorde

[97] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 314
[98] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 315

indsigelse. Sletning måtte derfor vente til de andres landes behandling var færdig. God databehandlingsskik skal vurderes i forhold til den person, som oplysningerne angår, uanset hvilken sammenhæng oplysningerne indgår i, og uanset om vedkommende er part i en sag eller ej, jf. John Vogter, Forvaltningsloven s. 55.[99]

7.2.2 Formålsbegrænsning

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 1, litra b:

"*Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål".*

Litra b første led er stort set identisk med ordlyden af det tidligere databeskyttelsesdirektivs artikel 6, stk. 1, litra b. Der kan derfor ikke anses at være en ændring i forhold til hidtil gældende ret. Det er vigtigt at bemærke at 1. led suppleres af artikel 6, stk. 1, litra b. 2.[100]

2. led følger ligeledes det tidligere databeskyttelsesdirektiv, men på en måde, hvor det er tydeliggjort, at reglen om formålsbegrænsning ikke forhindrer viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, hvis det sker i overensstemmelse med forordningens artikel 89, stk. 1.[101]

Princippet om formålsbestemthed kaldes "finalité-princippet". Det betyder, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål. Dette princip er fundamentalt og vigtigt i databeskyttelse og gælder uanset om indsamling sker ved den registrerede eller 3. mand. Der påhviler den dataansvarlige en ubetinget pligt til at kunne bevise, hvad formålet med indsamlingen har været jf. artikel 5, stk. 2.[102]

Pligten til at oplyse den registrerede om indsamlingen af data sker ikke ud fra princippet i artikel 5, men derimod artikel 13 og 14 om oplysningspligt. Generelt set må det antages, at artikel 5, stk. 1, litra b sammenholdt med artikel 5, stk. 2 ikke indebærer en pligt for den dataansvarlige til skriftligt at formulere formålet med en bestemt indsamling. Den dataansvarlige har alene pligt til at gøre sig

[99] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 314-316
[100] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 317
[101] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 317
[102] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 318

bekendt med, hvad formålet er for enhver indsamling af oplysninger, som er omfattet af databeskyttelsesloven. I praksis vil man formodentligt nok gøre dette skriftligt i forbindelse med salgsarbejdet, da det derved bliver nemmere at løfte en bevisbyrde over for et eventuelt tilsyn.

7.2.2.1 Udtrykkeligt angivne og legitime formål

Den dataansvarlige har i forbindelse med indsamlingen pligt til "udtrykkeligt" at definere formålet for behandlingen. Formålet skal derfor være tilstrækkeligt, veldefineret og velafgrænset for at skabe åbenhed og klarhed omkring, hvad der bliver behandlet. Det er derfor vigtigt for den dataansvarlige at være præcis i sine formuleringer. Den dataansvarlige kan ikke komme med en generel eller vag definition som et eksempel herpå, "til administrative formål" eller "til brug for kommercielle formål", disse formuleringer vil ikke være tilstrækkelige til at opfylde kravet om udtrykkelighed. Derimod kan en præcis angivelse såsom "til brug for udbud af finansielle ydelser" anses for at være tilstrækkelig.[103]

Konsekvensen ved kravet om udtrykkelighed er, at den dataansvarlige ikke må indsamle oplysninger, som der ikke er behov for. Det er ligegyldigt om informationerne er af praktiske grunde, såsom at der indsamles supplerende oplysninger. Dette understøttes desuden af artikel 5, stk. 1, litra c, om dataminimering. Indsamlingen af oplysninger skal altså være saglige og ske med legitime formål. Det kunne f.eks. være administrative formål, som ligger indenfor den dataansvarliges myndighedsområde at varetage. Kravet om saglighed skal vurderes konkret i forhold til den enkelte myndighed, private virksomhed m.v. Afgørende er om indsamlingen af oplysninger sigter mod at løse opgaver, som falder under deres kompetenceområde.[104]

Som et eksempel på praksis kan nævnes afgørelsen:

Dt.s j.nr. 2005-212-0299 – Tivoli sagen

Tivoli ønskede til brug for adgangskontrol at fortage digital lagring af billeder af kortholderne. Lagringen skulle ske i en central database. Ved besøg skulle gæsten køre sit kort, som ikke skulle indeholde et billede, heller ikke i digital form, gennem en kortlæser ved indgangen, hvorefter gæstens billede ville blive synligt for kontrolløren via en skærm. Formålet hermed var udelukkende at sikre, at gæsten var identisk med kortholderen. Hvis gæsterne ikke ønskede at afgive billede, så skulle de kunne fremvise andet billedlegitimation.

Datatilsynet udtalte, at behandling af det digitale billede kunne ske med hjemmel i den tidligere persondatalovs § 6, stk. 1, nr. 1, dvs. på grundlag af kortholderens samtykke, men ikke med hjemmel

[103] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 318
[104] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 318f

i denne lovs § 6, stk. 1, nr. 2 og 7. Kortholderens samtykke skulle opfylde kravene i persondataforordnings artikel 4, nr. 11. Derudover fandt datatilsynet ikke grundlag for at tilsidesætte Tivolis vurdering af, at der var tale om en saglig og proportional behandling af personoplysninger. Tilsynet lagde her vægt på at gæsterne havde mulighed for at vælge andre løsninger. [105]

Når det gælder offentlige myndigheders indhentning af personoplysninger, vil artikel 5, stk. 1, litra b minde meget om forvaltningslovens § 32, hvorefter den, der virker indenfor den offentlige forvaltning, ikke må skaffe sig fortrolige oplysninger, som ikke har betydning for udførslen af en opgave. FOB 2003.699; hvor ombudsmanden udtalte, at en kommunal sagsbehandler havde handlet i strid med forvaltningslovens § 32 samt persondatalovens § 5, stk. 2 (nu persondataforordnings artikel 5, stk. 1, litra b.) ved at have indhentet fortrolige informationer om kommunens arbejdsmarkedschef og dennes familie i et kommunalt register, som indeholdt fortrolige oplysninger til brug for ligningen af skatteborgerne i kommunen.

7.2.2.2 Senere behandling til andre formål

Viderebehandling af oplysninger må ikke være uforenelig med de formål, hvortil oplysningerne er indsamlet. Dette indebærer at oplysninger, som den dataansvarlige har indsamlet, ikke frit kan genbruges, videregives m.v. Dette gælder også indenfor offentlig forvaltning. Det vil sige videregivelse kun må ske, hvis det er indenfor samme samtykke område. Videregivelse til tredjemand skal derfor være lovlig efter de materielle regler for behandling af personoplysninger i forordningen og dansk lovgivning. Der er ikke mulighed for at omgå reglerne ved, at den dataansvarlige videregiver oplysninger til en tredjemand, som ved sin indsamling af oplysninger sætter formål, som er anderledes end de oprindeligt indhentede oplysninger. Der er dog ingen regel, der siger, at den registrerede kan give sit samtykke til, at de indsamlede oplysninger gerne må behandles til andre formål, jf. forordningens artikel 6, stk. 4. Videregivelse skal blot ske med et sagligt grundlag.

Artikel 6, stk. 4 præciserer, hvornår det er muligt/lovligt at videregive oplysninger ud fra artikel 5, stk. 1 litra b. Der er 3 muligheder. 1) Den registrerede kan selv give samtykke til det. 2) Der kan være love efter medlemsstatens nationale regler der giver lov til videregivelsen og 3) Databehandleren kan ud fra "testen" i artikel 6, stk. 4, 2. led, litra a-e samt betragtning 50 fortage en vurdering af, hvornår en viderebehandling er foreneligt med formålet. En videregivelse kan medføre konsekvenser

[105] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 319

såsom kryptering eller pseudonymisering.[106] Skulle den dataansvarlige vurdere at en videregivelse er indenfor formålet, skal den dataansvarlige forsat overholde oplysningspligten og informere den registrerede før en videregivelse finder sted jf. artikel 13 og 14.

Private virksomheder må godt bruge sine kundeoplysninger til egen markedsføring, så længe det sker efter reglerne i markedsføringsloven § 6. Der kunne dog nemt opstå situationer, hvor en virksomhed vil overtræde artikel 5, stk. 1, litra b. Et eksempel, hvor forordningen med stor sandsynlighed ville have fundet anvendelse i dag er:

Rt.s. j.nr. 1997-1413-023 – Telefirma intern videregivelse.

Kunden havde købt mobilabonnement gennem et telefirma, som derefter benyttede data i forbindelse med oprettelsen af kontaktbureau. Dette kontaktbureau var internt og derfor ikke i strid med lov om private registre, da der var tale om intern overgivelse af lovligt registrerede oplysninger. [107]

Indsamlede oplysninger vil uanset det oprindelige formål kunne anvendes til senere behandling i historisk, statistisk eller videnskabeligt øjemed, jf. bestemmelsen 2. led., så længe der er hjemmel i behandlingsreglerne. Hvis behandlingen sker til mere end det oprindelige formål f.eks. kommercielle eller administrative formål finder 2. led derfor ikke anvendelse. [108]

7.2.3 Dataminimering

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 1, litra c:

"*Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles*."

Ordlyden er stort set identisk med ordlyden fra det tidligere databeskyttelsesdirektivs artikel 6, stk. 1, litra c og persondatalovens § 5, stk. 3. Den skal således ikke forstås anderledes end tidligere gældende ret.

Behandling af oplysninger må ikke gå videre end, hvad der kræves til opfyldelse af de formål, som den dataansvarlige er berettiget til at forfølge. Den dataansvarlige skal derfor behandle oplysningerne ud fra et proportionalitetsprincip.

Dt.s j.nr. 2018-31-0070 – TDC A/S sagen:

[106] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 323f.
[107] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 326
[108] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 328

Her tog Datatilsynet stilling til, om TDC A/S behandling af oplysninger om en kunde i forbindelse med selskabets registrering af trafik- og lokaliseringsdata. (hvilke master, kunders telefoner opretter forbindelse til).

TDC havde gjort gældende, at det var nødvendigt at registrere lokaliseringsdata for al mobildatatrafik for at overholde logningsbekendtgørelsens krav set i forhold til MMS-kommunikation, men Datatilsynet mente ikke at opbygningen af TDC's it-systemer kunne begrunde den manglende overholdelse af databeskyttelsesreglerne. TDC havde logget oplysninger, som ikke var nødvendige for deres formål (det var kun 1,6% og 0,09 % der vedrørte MMS kommunikation), samt at TDC selv havde sagt at de ikke havde et formål med at registrere de overskydende oplysninger. Dette var derfor strid på databeskyttelsesforordnings artikel 5, stk. 1 litra c. Det kan dog næppe antages af bestemmelsen, at en dataansvarlig i konkrete sagsbehandlinger har pligt til at gennemgå relevansen og nødvendigheden af hver enkelt oplysning i en sag. Hvis en borger oplyser om personlige forhold, som ikke har direkte betydning for sagen, så påhviler der ikke myndigheden en pligt til at slette disse oplysninger, jf. de forvaltningsretlige krav til dokumentation, aktindsigt mv. Der er en vis margin for, hvornår en sagsoplysning kan ses for relevant og nødvendig. Det er dog klart, at hvis der ikke er et sagligt formål for at efterspørge personoplysninger, så skal myndigheden undlade at efterspørger dem.[109]

7.2.4 Rigtighed

Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra d:

"*Personoplysning skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges".*

Litra d er indholdsmæssigt det samme, som databeskyttelsesdirektivets artikel 6, stk. 1, litra d og persondatalovens § 5, stk. 4. Der er kun få sproglige ændringer, så derfor må den anses for at være som hidtil gældende ret.

Kravet om ajourføring sikrer, at der påhviler den dataansvarlige en forpligtelse til at fortage ajourføring af oplysninger, som viser sig forældede/forkerte. Omfanget af denne kontrol afhænger af oplysningernes karakter, deres anvendelse, indsamlingens pålidelighed og om oplysningerne har betydning for en eller flere myndigheder, virksomheder m.v.[110]

[109] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 329-330
[110] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 331

Forordningens formulering har med stor sandsynlighed ført til en praksis ændring, da der tidligere i persondataloven blev omtalt at oplysninger skulle slettes eller berigtiges hurtigst muligt. I databeskyttelsesdirektivet blev der heller ikke nævnt noget om tid. Ændringen i ordlyden fra snarest muligt til straks gør derfor at forordningen er strengere, men formålet er uændret, formuleringen stiller blot større krav til den dataansvarlige om at berigtige fejl.

Tidligere begreber som vildledende og ufuldstændige er udgået i forordningen, men betydningsmæssigt er det stadig indenfor "urigtige oplysninger", hvorfor der ikke ses en ændring i retstilstanden. Den registrerede vil selv kunne anmode om, at den dataansvarlige berigtiger, sletter eller begrænser oplysninger, som viser sig at være urigtige eller vildledende eller ulovligt behandlet, jf. forordningens artikel 16-18. I praksis vil reglerne i artikel 5 eller 16-18 ikke føre til, at urigtige oplysninger skal slettes. Det begrundes i, at det er nødvendigt for offentlige myndigheder samt private virksomheder at kunne dokumentere det faktuelle grundlag for en beslutning/afgørelse. Det fremgår af afgørelse fra Social- og Indenrigsministeriet F-2-03; hvor en amtskommune i forbindelse med behandlingen af en ansøgning om støtte til køb af bil havde noteret, at ansøgeren havde et mangeårigt massivt alkoholmisbrug. Ansøgeren havde anmodet kommunen og amtskommunen om at slette denne oplysning, da den efter hans vurdering var fejlagtig. Begge myndigheder afslog, og sagen blev indbragt for det sociale nævn, som ikke fandt, at oplysningen skulle slettes fra journalen. Ankestyrelsen stadfæstede nævnets afgørelse, men bestemte, at oplysningen skulle berigtiges.[111]

Den manglende pligt for offentlige myndigheder til at slette oplysninger skal findes i reglerne om notatpligt, jf. offentlighedslovens § 13 og journaliseringspligten i offentlighedslovens § 15. Disse regler understøtter vigtige forvaltningsretlige regler, såsom aktindsigt jf. offentlighedsloven og forvaltningslovens § 19 om partshøring. Derudover bidrager notatpligten og journaliseringspligten til, at der efterfølgende kan klarlægges, hvad der er sket i en sag (dokumentationshensyn), ligesom det giver mulighed for at føre kontrol, om myndighederne har handlet korrekt (kontrolhensyn).

Der kan nærmere henvises til Justitsministeriet udtalelse til Dt.s j. nr. 2017-769-0056; hvor det blev anført at offentlige myndigheder kun havde få muligheder for at slette oplysninger, hvis der var lovhjemmel til det eller, hvis et dokument ved en fejl var blevet journaliseret forkert og herefter blev journaliseret på den korrekte sag. Offentlige myndigheder vil derfor skulle berigtige urigtige eller

[111] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 333

vildledende oplysninger ved at lave et notat på sagen, men ikke fjerne de forkerte oplysninger, jf. artikel 16-18, særligt artikel 16 og 17 stk. 3, litra b.[112]

7.2.5 Opbevaringsbegrænsning

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 1, litra e:

"*Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder*".

Artikel 5, stk. 1, litra e, 1. led, svarer indholdsmæssigt til databeskyttelsesdirektivets artikel 6, stk. 1, litra e og persondatalovens § 5, stk. 5. Der er således ikke sket en ændring i hidtil gældende ret. 2. led, henviser til forordningens artikel 89, stk. 1. Det tydeliggøres derfor at reglen om opbevaringsbegrænsning ikke forhindrer, at personoplysninger kan behandles til arkivformål, videnskabelige eller historiske forskningsformål eller til statiske formål, så længe man overholder reglerne i forordningens artikel 89.[113]

Formålet med reglen er at sikre mod en unødvendig ophobning af data. Der opstår altid en risiko ved at gemme data, da uvedkommende over tid måske får adgang til dem. Bestemmelsen gør at man ikke må opbevare identificerbare personoplysninger længere end, hvad der er nødvendigt af hensyn til de formål, hvortil oplysningerne er indsamlet eller senere behandling, jf. artikel 5, stk. 1, litra b.[114]

Der er ikke et fast facit på, hvor lang tid en myndighed eller virksomhed må opbevare data, da det altid skal bedømmes ud fra en konkret vurdering af sagen. Det forudsættes dog, at tilsynsmyndigheden fastsætter nogle generelle kriterier for, hvor længe den dataansvarlige i almindelighed må opbevare identificerbare oplysninger.[115]

Den hidtidige praksis vedrørende persondatalovens § 5, stk. 5, sagde, at hvis virksomheden havde fastsat generelle slettefrister, havde en dataansvarlig ikke pligt til løbende at gennemgå samtlige sager, dokumenter mv. Gennemgangen skulle foretages med henblik på at sikre, at der ikke blev

[112] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 334
[113] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 334f.
[114] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 334f.
[115] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 335

opbevaret konkrete personoplysninger i strid med persondatalovens § 5, stk. 5, så længe der var fastsat procedurer, som sikrede at der skete sletning efter de fastsatte frister.[116] Da ordlyden efter forordningen ikke har ændret sig, må det derfor stadig gælde.

7.2.5.1 Hvornår er der sket sletning? Opbevaringsbegrænsning

Der er sket sletning ifølge Datatilsynet når:

"*Sletning af personoplysninger i et system er en handling, der sikrer at oplysningerne ikke længere er tilgængelige. Hvis personoplysninger efter sletning fx kan tilgås af systemets administrator, er der ikke tale om en reel sletning. Hvis personoplysninger omvendt reelt set er slettet via operativsystemet, og på disken venter på at blive overskrevet med andre data, er der tale om sletning, da oplysningerne ikke længere med rimelige midler er tilgængelige*".[117]

Datatilsynet diskuterer endvidere forskellen på, om der er backup af oplysningerne, hvortil det må konkluderes, at den dataansvarlige har en pligt til at sørge for at slette personhenførbare oplysninger, såfremt det er muligt efter systemet. Der skal samtidig oprettes en log, hvis man ikke kan slette oplysningerne fra backuppen, så skal de blive slettet, når det er muligt. Der skal desuden tages stilling til en slettefrist af disse logs, da der kan være personhenførbare oplysninger i dem.

Praksis efter forordningen om manglende sletning kan nævnes:

Dt.s j.nr 2018-41-0015 – Ilva A/S i dømt bøde for manglende slettefrister

Tre butikker anvendte et ældre it-system, hvor der ikke var fastsat frister for sletning af kundernes oplysninger. Der var tale om overtrædelse af artikel 5, stk. 1, litra e, idet virksomheden havde opbevaret ca. 385.000 kunders navne, adresser, telefonnumre, e-mails og købshistorik i en længere periode end nødvendigt til de formål, hvortil de blev behandlet.

Desuden fandt Datatilsynet, at virksomheden havde overtrådt artikel 5, stk. 2, idet den ikke havde fastlagt og dokumenteret frister for sletning af personoplysninger. Virksomheden havde et nyt IT-system, hvor der var fastsat slettefrister, men hvor virksomheden stadig havde behandlet oplysningerne efter slettefristen var nået. Virksomheden havde desuden ikke dokumenteret sine procedurer for sletning af personlysninger i dens rekrutteringssystem og HR-system. Førstnævnte overtrædelse

[116] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 335
[117] www.datatilsynet.dk/emner/persondatasikkerhed/sletning

gav anledning til politianmeldelse, mens de øvrige overtrædelser udløste alvorlig kritik. Denne afgørelse er der faldet dom ved i byretten 12.02.2021,[118] hvorfor denne er det nyeste praksis indenfor området. Dommen er dog anket til landsretten.[119]

Slettefristen skal være proportional med formålet, dvs. hvis man låner en bog på biblioteket, så har biblioteket behov for at vide, hvem der har lånt bogen og hvor lang tid de har lånt bogen. Når biblioteket har fået returneret bogen efter en måned eller to, har de ikke længere et behov for oplysningerne, hvorfor slettefristen kan sættes til 2 måneder, hvorimod, hvis man har brug for opbevaring pga. lovgivning eller andre formål, kan der være flere års slettefrist. Det skal derfor altid vurderes ud fra en konkret vurdering.[120]

7.2.6 Integritet og fortrolighed

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 1, litra f:

"*Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger*".

Bestemmelsen omhandler behandlingssikkerhed. I databeskyttelsesdirektivet og persondataloven var der ikke en lignende bestemmelse. Der var i databeskyttelsesdirektivets artikel 17 og i persondatalovens kapitel 11 nævnt regler omkring behandlingssikkerhed, men princippet i litra f er en tilføjelse, da det ikke tidligere kunne aflæses direkte. Forordnings artikel 32 præcisere herefter behandlingssikkerheden i forbindelse med personoplysninger. Ved tilføjelsen af dette princip i databeskyttelsesforordningens artikel 5, ved den dataansvarlige, at der bliver lagt større vægt på behandlingssikkerheden fremadrettet.[121]

7.2.7 Ansvarlighed

Det fremgår af databeskyttelsesforordnings artikel 5, stk. 2:

"Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes".

[118] https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/?fbclid=IwAR1r1kyHvx4Q5v_EwCs13Si8mfrO6f35DjSa1h5KXEAtbIz880iXOZfoB5w
[119] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 337
[120] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 335-340
[121] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 340

Efter de tidligere gældende regler fra databeskyttelsesdirektivets artikel 6, stk. 2, skulle den dataansvarlige sikre, at de grundlæggende principper i direktivet blev overholdt. Der er ikke i præamblen til forordningen en uddybning af, hvordan artikel 5, stk. 2, skal forstås, men med bestemmelsen må det antages at være understreget, at den dataansvarlige skal dokumentere overholdelsen af principperne for behandlingen. Den dataansvarlige skal nu kunne "*påvise*" at man overholder principper i artikel 5, hvor det tidligere var nok at "*sikre*" overholdes. Det stemmer godt overens med, at man med forordningen ønskede en større ansvarlighed for de dataansvarlige.[122]

7.3 Oplysningspligt artikel 13-14

Reglerne om oplysningspligt findes i artikel 13-14 og er centrale i forhold til indsigtsretten i artikel 15. De sikrer at behandling af personoplysninger foregår på en rimelig og gennemsigtig måde, jf. betragtning 39. En dataansvarlig har pligt til på eget initiativ at opfylde oplysningspligten overfor den registrerede, hvorimod indsigtsretten kræver en anmodning fra den registrerede. Der findes ingen regler for høringspligt i databeskyttelsesforordningen. Dette er reguleret i forvaltningsloven, særligt § 19. Reglerne om oplysningspligt finder desuden ikke anvendelse ved domstolene, da disse behandles efter retsplejeloven jf. databeskyttelseslovens § 22, stk. 4.[123]

En dataansvarlig har pligt til at "give" oplysninger jf. artikel 13 og 14. Det vil derfor ikke være tilstrækkeligt at have oplysningerne på en hjemmeside eller lignende. Det begrundes i, at den registrerede i så fald selv skal lave en aktiv handling, hvorimod der står i artikel 13, stk. 1 og artikel 14, stk. 1, at man aktivt skal lede den registrerede til oplysningernes placering. Det kan gøres med et direkte link, brug af QR-kode, udlevering af fysiske foldere osv. Måden den dataansvarlige aktivt giver informationen, er ligegyldig, så længe artikel 13, stk. 1 overholdes, hvoraf det fremgår, at oplysninger gives på en tydelig, kortfattet og letforståelig måde. Oplysningerne skal endvidere udleveres gratis for den registrerede, medmindre der er udbedt flere kopier, jf. artikel 15, stk. 3, 2. pkt.

Ønsker den dataansvarlige at viderebehandle personoplysninger til et andet formål, end det er indsamlet, skal den dataansvarlige forud for viderebehandlingen give den registrerede oplysninger om det andet formål, jf. artikel 13, stk. 3 og artikel 14, stk. 4, jf. finalité-princippet i artikel 5, stk. 1, litra b. Tidligere praksis fra Datatilsynet på området var anderledes, da man efter den gamle persondatalov kunne behandle oplysninger til andre efterfølgende saglige formål, uden at den dataansvarlige

[122] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 341
[123] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 462

på ny skulle give den registrerede meddelelse herom. Det var kun, hvis behandlingen ikke var uforenelig med det eller de formål, som oprindeligt var oplyst til den registrerede i forbindelse med oplysningspligten.[124] Der er derfor sket en udvidelse af området, da den gælder når der foretages viderebehandling af personoplysninger til andre formål end det, hvortil personoplysninger er indsamlet, jf. artikel 13, stk. 3, og artikel 14, stk. 4.[125]

Det er vigtigt at sikre sig som dataansvarlig, at man indhenter et konkret, specifikt samtykke, som opfylder alle formålene til ens behandling, da den dataansvarlige ellers skal indhente nye samtykker. Det begrundes i artikel 13, stk. 1, litra c, og artikel 14, stk. 1, litra c, idet den dataansvarlige ellers ikke overholder kravet i artikel 5, stk. 1, litra b, om, at oplysninger skal indsamles til udtrykkeligt angivne og legitime formål.

Oplysningspligten efter artikel 13 skal opfyldes "på det tidspunkt, hvor personoplysningerne indsamles", jf. stk. 1, hvilket i praksis betyder indenfor 10 dage. Oplysningspligten efter artikel 14 skal opfyldes på ét af tre forskellige tidspunkter, jf. artikel 14, stk. 3. Indsigtsretten skal derimod opfyldes uden unødig forsinkelse og senest en måned efter modtagelsen af anmodningen, jf. artikel 12, stk. 3.[126]

Undtagelserne til oplysningspligten efter artikel 13, stk. 1-3, findes i artikel 13, stk. 4 og databeskyttelseslovens §§ 22-23. Undtagelserne til oplysningspligten efter artikel 14, stk. 1-4, findes i artikel 14, stk. 5, og databeskyttelseslovens §§ 22-23. Det er vigtigt at noterer sig, at det er alene forhold vedrørende oplysningspligten efter artikel 14, at man som dataansvarlig kan undlade at give bipersoner underretning, jf. artikel 14, stk. 5, litra b.

Formålet med oplysningspligten er at skabe gennemsigtighed og overblik vedrørende personregistreringer, hvorfor virkningen ved manglende overholdelse ikke vil medføre ugyldighed. Årsagen skal findes i at gennemsigtighed ikke er en retsgaranti for afgørelsers rigtighed. Det vil tale for en ugyldig afgørelse, hvis sagen i øvrigt er mangelfuldt belyst. Det vil dog være op til en konkret vurdering af hele sagen.[127]

Forvaltningsmyndigheders underretningspligt efter bestemmelserne i artikel 13 og 14, må næppe anses for at have karakter af en afgørelse efter forvaltningsloven. Meget taler for, at en sådan beslutning har karakter af en beslutning i forvaltningslovens forstand, da der alene er tale om processuel karakter. Beslutningen træffes som led i forbindelse med sagsbehandlingen. Det vil desuden

[124] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 464
[125] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 464
[126] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 464f.
[127] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 465f.

stemme dårligt overens med hensynene bag oplysningspligten, hvis forvaltningsmyndigheder i en given situation er underretningspligtige efter bestemmelserne i artikel 13 og 14 og i databeskyttelseslovens §§ 22-23. Hvis der er tale om en afgørelse i forvaltningens forstand, så er der underretningspligt i forbindelse med at give meddelelse om en afgørelse. Datatilsynet ville dog skulle tage stilling til, om der skulle gives underretning ved en klagesag, da det er relevant for vurderingen af en klagesag. Opsummeret må det derfor udledes, at så snart der er tale om en klage fra den registrerede om oplysningspligten, så vil sagen skulle vurderes som en afgørelse, hvorimod det ved almindelig sagsbehandling blot vil være en beslutning i forvaltningens forstand.[128]

7.4 Indsigtsret artikel 15

Det fremgår af artikel 15, at den registrerede har mulighed for at få indsigt i egne personoplysninger, der bliver brugt som led i en behandling. I henhold til artikel 15, stk. 1. er der flere muligheder i forbindelse med indsigtsretten. Enten kan den registrerede få en bekræftelse om, at der behandles personoplysninger, jf. artikel 15, stk. 1. Hvis der i forvejen bliver behandlet personoplysninger om den registrerede, er der mulighed for at få adgang til disse. Hvis der bliver behandlet personoplysninger om den registrerede, har den registrerede lov til at få adgang til dem i form af en kopi.[129]

Indsigtsretten er med til at give bedre persondatasikkerhed samt større gennemsigtighed i forbindelse med behandlingen af personoplysninger, eftersom den registrerede kan bede om indsigt.[130] For at få indsigt kræves det, at den registrerede retter henvendelse til den dataansvarlige. Det er den dataansvarliges job at udlevere det rigtige materiale. Hvis den dataansvarlige finder ud af, at der er store mængder af data, er der intet til hindrer for at bede den registrerede om at præcisere, hvilke typer af sager der ønskes indsigt i.[131] I tilfælde som beskrevet ovenfor vil den dataansvarlige have mulighed for at oplyse den registrerede om, hvilke sager den registrerede er involveret i med henblik på at kunne præcisere, hvilke sager der ønskes indsigt i. Den dataansvarlige skal dog være opmærksom på, at en anmodning om indsigt ikke kan afvises, fordi den registrerede ikke kan eller vil præcisere sin anmodning om indsigt. Den dataansvarlige vil derfor skulle give indsigt i alle oplysninger som bliver behandlet om den registrerede.[132]

[128] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 466f.
[129] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 518
[130] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 518
[131] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 522
[132] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 522

Udgangspunktet er at den dataansvarlige en måned efter modtagelse af en indsigtsanmodning skal have den besvaret, i visse tilfælde kan den dataansvarlige få lov til at forlænge fristen til to måneder.

I en sag om indsigt indgår der ofte hovedpersoner og bipersoner. En hovedperson er den person som selve behandlingen/sagen omhandler, det er derfor disse oplysninger som den registrerede kan få indsigt i. En biperson indgår ofte i de forskellige sager, der kan være tale om en pårørende, familiemedlem til en part eller tv-overvågning, hvor der indgår andre mennesker end hovedpersonen. Hvis en hovedperson anmoder om indsigt, er der kun mulighed for at få oplysninger omkring sig selv udleveret. Det betyder, at den dataansvarlige skal overstrege en oplysning omkring bipersoner eller sløre bipersonerne, hvis der er tale om tv-overvågning. En biperson har derfor også ret til at få indsigt i de data, som er behandlet om denne. Hvis den dataansvarliges system ikke direkte er indrettet til at finde bipersoner, kan den dataansvarlige anmode om flere oplysninger fra bipersonen for at kunne finde frem til de rigtige oplysninger.

I forbindelse med indsigtsretten kan den dataansvarlige risikere, at flere registrerede misbruger indsigtsretten. Det fremgår ikke af artikel 15, hvor ofte en registreret må udnytte indsigtsretten. Den eneste beskrivelse af tidsrummet fremgår af betragtning 63. Heraf fremgår det, at den registrerede må bede om indsigt "med rimelige mellemrum".[133] Denne beskrivelse kan dog give anledning til en del fortolkning, eftersom der ikke direkte er defineret, hvad rimelige mellemrum betyder. Dog medfører denne beskrivelse, at den dataansvarlige kan afvise overdrevne anmodninger, samt anmodninger som måtte være grundløse.

Der kan være tilfælde, hvor den registrerede er repræsenteret af en anden person eller juridisk person, jf. databeskyttelsesforordningens artikel 27. I databeskyttelsesforordningen og databeskyttelsesloven er der ingen regler om, hvilke personer som må repræsentere den registrerede. Oftest vil der være tale om en advokat, revisor eller et familiemedlem. Hvis der er tale om en sagkyndig, altså en advokat eller revisor, vil den dataansvarlige oftest ikke skulle have dokumentation for fuldmagtsforholdet med mindre, at den dataansvarlige i sagsbehandlingsperioden ikke har været i kontakt med den registrerede.[134]

[133] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 519
[134] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 525

Den dataansvarlige skal være sikker på, at der ikke udleveres dokumenter til uvedkommende. Derfor skal den dataansvarlige opstille foranstaltninger, som benyttes til at identificere den registrerede. Disse regler er særligt vigtige, hvis indsigten bliver afgivet over telefon, da den dataansvarlige her skal sikre, at det er den registrerede, som de udleverer dokumenterne til.

Som beskrevet ovenover giver indsigtsretten den registrerede ret til at få at vide, om der bliver behandlet oplysninger om den registrerede, samt hvilke oplysninger der bliver behandlet. Det fremgår af artikel 15, stk. 1, litra a-h, hvilke typer af oplysninger, den registrerede kan få indsigt i.

Det fremgår af litra a, at den registrerede har ret til at få oplyst, til hvilket formål oplysningerne behandles. Den dataansvarlige skal ikke kunne specificere formålet, men skal være i stand til at give en generel beskrivelse af formålet.[135]

Ifølge litra b, skal den dataansvarlige kunne fortælle den registrerede, hvilke typer af personoplysninger som bliver behandlet. Der kan her være tale om almindelige personoplysninger eller følsomme personoplysninger. Der vil herudover være mulighed for at få en kopi af disse personoplysninger, jf. stk. 3.[136]

Efter litra c har den registrerede ret til at få indsigt i de modtagere eller kategorier af modtagere, som oplysningerne er eller kan være sendt videre til. Denne bestemmelse er med til at skabe gennemsigtighed i sagsbehandlingen, men er også med til at sikre, at den registreredes personoplysninger ikke videresendes til et tredjeland eller international organisation, hvor oplysningerne vil være uvedkommende. Den dataansvarlige vil derfor ikke kunne begrænse sig til at give kategorier af modtagere, men skal derimod angive de konkrete modtagere. Det vil være muligt at give kategorier, hvis der ikke har været videresendt informationer på indsigtstidspunktet.[137]

I henhold til litra d, fremgår det at den registrerede har ret til at få at vide, det påtænke tidsrum, hvor oplysningerne vil blive opbevaret. Hvis det ikke er muligt, så skal den dataansvarlige oplyse, hvilke kriterier der blev anvendt til at fastsætte det påtænkte opbevaringstidsrum.[138]

Af litra e fremgår det, at den registrerede har ret til at få berigtiget eller slettet sine oplysninger, eller begrænset behandlingen af den registreredes personoplysninger eller ret til at gøre indsigelse mod en sådan behandling. Disse punkter bliver nærmere belyst i artikel. 16, 17, 18 og 21, se også afsnit 7.5 for en behandling af disse rettigheder.

[135] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 529
[136] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 529
[137] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 529
[138] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 529

Det fremgår af litra f, at den registrerede har ret til information om retten til at indgive en klage til en tilsynsmyndighed.[139]

Ifølge litra g, har den registrerede ret til at få indsigt i, hvor oplysningerne stammer fra, hvis de ikke er indsamlet hos den registrerede. Pligten gælder ikke, hvis den dataansvarlige ikke kender til oprindelsen. Det må dog antages, at den offentlige forvaltning i forbindelse med en sagsbehandling har registeret, hvor oplysningerne stammer fra, jf. offentlighedslovens § 13, navnlig reglen om notatpligt.[140]

Efter litra h, fremgår det at den registrerede har ret til at få indsigt i forekomsten af automatiske afgørelser. [141]

Det fremgår af artikel 15, stk. 2., at hvis personoplysninger overføres til tredjelande eller international organisation, har den registrerede ret til i henhold til artikel 46, at blive informeret om de fornødne garantier. Forskellen mellem stk. 1, litra c. og stk. 2. er, at den dataansvarlige i stk. 2. skal informere den registrerede om de fornødne garantier som er anvendt ved overførslen, hvis artikel 46 udgør overførelsesgrundlaget.[142]

I henhold til stk. 3. fremgår det, at den registrerede har ret til at få en kopi af de personoplysninger, som bliver behandlet. En kopi kan sendes på flere forskellige måder, dog skal der være tale om en sikker overdragelse. Oplysningerne kan sendes via e-Boks, et sikkert elektronisk program, som kan tilgås via den registreredes computer.[143]

7.5 Berigtigelse, sletning, begrænsning og indsigelse – artikel 16, 17, 18 og 21

Inden Databeskyttelsesforordningen trådte i kraft, var forholdet om berigtigelse, retten til sletning og retten til begrænsning, reguleret i persondatalovens § 37, stk. 1. Her havde den dataansvarlige pligt til at berigtige, slette eller blokere oplysninger, som viste sig at være urigtige eller vildledende, efter anmodning fra den registrerede. Det forhold er nu blevet opdelt i tre selvstændige artikler. Artikel 16 regulerer retten til berigtigelse, artikel 17 regulerer retten til sletning og artikel 18 regulerer retten til begrænsning af behandling.[144] Førhen havde den dataansvarlige mulighed for at vælge, hvilken korrigeringsmetode, der skulle benyttes i forbindelse med urigtige oplysninger. Den nye opdeling medfører, at den registrerede nu selv har et valg i forhold til hjemmelsgrundlaget som benyttes.

[139] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 530
[140] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 530
[141] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 530
[142] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 530-531
[143] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 531-532
[144] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 536

7.5.1 Retten til berigtigelse

Det fremgår af databeskyttelsesforordningens artikel 16 at:

"*Den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med behandlingen ret til få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring*".

Det følger i forlængelse af artikel 5, stk. 1, litra d, at personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges, dvs. princippet om "rigtighed".[145][146]

I praksis opstår spørgsmålet om ret til berigtigelse typisk i tre situationer: 1) der er enighed mellem den dataansvarlige og den registrerede om, at oplysningerne er urigtige, 2) der er uenighed om, hvorvidt oplysningerne er urigtige, eller 3) oplysninger har karakter af en subjektiv eller faglig vurdering.[147]

Situation 1: Hvis der er enighed.

Hvis der er enighed, så vil oplysningerne blot skulle berigtiges.

En privat dataansvarlig vil skulle rette de urigtige oplysninger, jf. dt.j.nr. 2018-31-0147 om Rejsekort A/S. Her manglende berigtigelse af personoplysninger i form af lokationsdata. Det var ikke Datatilsynets opfattelse at artikel 16, 2. pkt. gav en ret til blot at supplere med oplysninger. De havde derfor ikke levet op til artikel 5, stk. 1, litra d og i øvrigt artikel 16, da de ikke havde præsteret at berigtige informationen som efterspurgt.

Ved en offentlig myndighed gælder derimod regler for at dokumentere det grundlag, som en afgørelse eller en anden beslutning i sin tid blev truffet på. Offentlige dataansvarlige må derfor berigtige oplysninger uden at fjerne de forkerte oplysninger, dette kan ske i form af en note, så man nemt kan se, hvad der har lagt grund til en afgørelse.

Situation 2: Hvis der ikke er enighed.

Den dataansvarlige har ikke pligt til at berigtige oplysningerne, men har dog pligt til at give et objektivt og sagligt begrundet afslag på berigtigelsen. Den dataansvarlige har pligt til at registrere,

[145] Databeskyttelsesforordningen - Karnov note 143
[146] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 537
[147] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 538

hvad den registrerede mener er korrekt. Den dataansvarlige kan derfor gemme egen "saglige" vurdering, så længe der indskrives et notat om, at den registrerede mener noget andet.

Situation 3: Oplysningerne har karakter af subjektiv eller faglig vurdering.

Denne situation minder om situation 2, hvor den registrerede mener, noget ikke er korrekt. Det kan være en læge, der kommer med en faglig vurdering, samtidig med den registrerede har fået en anden læge til at komme med en erklæring, der modsiger den første faglige vurdering. Hvis den dataansvarlige vurderer, at den første læges vurdering stadig er korrekt, vil den dataansvarlige have mulighed for at beholde det. Den registrerede kan altså ikke få berigtiget dette eller slettet informationen jf. artikel 17, stk. 3, litra b.[148] Det understøttes af Dt.s j. nr. 2006-313-0376. Sagen drejede sig om en klage over, at en amtskommune og en kommune behandlede oplysninger, der angaves at være urigtige og udokumenterede. Oplysningerne var forskellige subjektive meninger fra sagsbehandleres observationer og vurderinger i forbindelse med en persons anbringelse udenfor hjemmet. Da de faglige vurderinger var forskellige, kunne det ikke vurderes fra tilsynets side, hvad der var korrekt. Derved skulle uenighederne fremgå af sagen, men begge typer oplysninger skulle stadig fremgå af sagen.

Det kan konkluderes efter 2. pkt., at den registrerede har ret til at få vedlagt supplerende erklæringer, hvis der ikke er enighed. Den dataansvarlige kan derfor ikke nægte at supplere oplysningerne, hvis den registrerede mener, der er tale om ufuldstændige personoplysninger, da der er pligt til at gøre sagen fuldstændig og/eller ajourført, hvilket den først er med den registreredes kommentarer.

7.5.2 Retten til sletning "at blive glemt"

Det fremgår af artikel 17 af databeskyttelsesforordningen at, den registrerede kan få slettet oplysninger uden unødig forsinkelse, hvis en af bestemmelserne i artikel 17, stk. 1, litra, a-f er overholdt. Stk. 2 omhandler den dataansvarliges pligt til underretning, hvis man har offentliggjort personoplysninger, som den dataansvarlige er forpligtet til at slette. Stk. 3 er undtagelserne til stk. 1 og 2.[149]

Bestemmelsen forpligter alene den dataansvarlige, og ikke en eventuelt databehandler og angår alene oplysninger, som den dataansvarlige har offentliggjort jf. C-398/15.[150]

Det fremgår efter artikel 17, stk. 1, litra a, at der er ret til sletning, hvis oplysningerne om den registrerede ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet eller på anden vis behandlet. Bestemmelsen er parallel med artikel 5, stk. 1, litra e (opbevaringsbegrænsning).

[148] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 538ff.
[149] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 544
[150] Karnovs note til databeskyttelsesforordningens artikel 17 – sag: Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce

Litra a må dog antages at have et selvstændigt forhold, når den registrerede gør brug af sin ret til sletning uden unødig forsinkelse i tilfælde, hvor den dataansvarlige ellers kunne afvente f.eks. udløbet af en generelt fastsat slettefrist.[151]

Det fremgår af litra b, at der er ret til sletning, hvis den registrerede trækker det samtykke, der er grundlaget for behandlingen tilbage, jf. artikel 6, stk. 1, litra a, eller artikel 9, stk. 2, litra a, og at der ikke er andet retsgrundlag for behandlingen. Retten til at trække sit samtykke tilbage fremgår af artikel 7, stk. 3.[152]

Det fremgår af litra c, at der er ret til sletning, hvis den registrerede gør berettiget indsigelse mod behandling af sine personoplysninger, jf. artikel 21, stk. 1, eller i medfør af artikel 21, stk. 2, gør indsigelse mod behandling af sine personoplysninger med henblik på direkte markedsføring.[153]

Det fremgår af litra d, at der er ret til sletning, hvis behandling af personoplysninger er blevet behandlet ulovligt. Dette skal ses sammenholdt med artikel 5, hvor den dataansvarlige kan være pålagt at slette oplysningerne straks, jf. artikel 5, stk. 1, litra d.[154]

Det fremgår af litra e, at der er ret til sletning, hvis det er nødvendigt for at overholde en retlig forpligtelse til at slette, der følger af enten EU-retten eller af national ret.[155]

Det fremgår af litra f, at der er ret til sletning, hvis personoplysningerne er blevet indsamlet i forbindelse med udbud af informationssamfundstjenester som er omhandlet i artikel 8, stk. 1.[156]

En dataansvarlig, som modtager underretningen, bliver ud fra bestemmelsens ordlyd i artikel 17, stk. 2, ikke direkte forpligtet til at slette de pågældende oplysninger, men det må antages, at en sådan dataansvarlig i lyset af underretningen må vurdere, om oplysningerne skal slettes hos den pågældende dataansvarlige, jf. principperne i artikel 5, stk. 1, litra e, og artikel 17, stk. 1. Som det fremgår af betragtning 66, er der tale om en udvidelse af retten til sletning i tilfælde, hvor en dataansvarlig har offentliggjort personoplysninger. Underretningsforpligtelsen i artikel 17, stk. 2, suppleres af artikel 19, hvorefter den dataansvarlige har underretningspligt ifm. berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, medmindre det viser sig umuligt eller uforholdsmæssigt vanskeligt.[157][158]

[151] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 545f
[152] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 546
[153] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 546
[154] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 546
[155] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 546
[156] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 546
[157] Databeskyttelsesforordningens artikel 17. Karnovs note 146.
[158] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 548f

Et eksempel på betydningen af stk. 2 kunne være, en medarbejder har givet samtykke til offentliggørelse af video-hilsen på virksomhedens hjemmeside. Medarbejderen præsenterer sig selv og sine arbejdsområder. Medarbejderen fortryder af personlige årsager og trækker samtykket tilbage. Virksomheden har jf. stk. 1, litra b pligt til at slette denne hilsen. Virksomhedens dataansvarlige kan se, at en anden virksomhed har downloadet denne hilsen. Den dataansvarlige skal derfor underrette virksomheden om, at der er sket anmodning om sletning. Virksomheden, som har downloadet denne hilsen, skal herefter ud fra formålet vurdere, om en lovlig behandling af personoplysninger kan fortsætte, eller om de har pligt til at slette det.[159]

Undtagelser er fastlagt i stk. 3. Den registrerede har derved ikke ret til at blive glemt i visse situationer. Oplysninger kan efter litra a, besvares i det omfang, behandling er nødvendig for at udøve retten til ytrings- og informationsfrihed. Se også databeskyttelseslovens § 3, stk. 1 og forordningens artikel 85 om behandling og ytrings- og informationsfrihed.[160]

Oplysninger kan efter litra b, bevares i det omfang, det er nødvendigt for at overholde en retlig forpligtelse, som den dataansvarlige er underlagt for at udføre en opgave i samfundet interesse eller som henhører under offentlig myndighedsudøvelse. Det må derfor antages, at artikel 17, ligesom § 37 (og § 5, stk. 4) i den tidligere persondatalov, ikke indeholder en selvstændig ret til at blive glemt i den offentlige sektor. Årsagen til dette skyldes, offentlige myndigheder har pligt til at dokumentere oplysninger, en beslutning eller afgørelse er truffet på. Det er derfor nødvendigt for dokumentationspligten at beholde oplysningerne, selvom de så måtte være forkerte. Det understøttes af et § 20-spørgsmål afgivet af justitsministeren d. 30. juni 1998. Her fremgik det, at en myndighed i almindelighed ikke er berettiget til at fjerne/destruere bestemte dokumenter, der indgår i en sag. Det kan kun ske, hvis der er lovhjemmel hertil, jf. Dt.s j.nr. 2018-32-0286:

Her fremgik det, at en kommune ved først at besvare en borgers anmodning om sletning efter 5 måneder og 21 dage ikke havde levet op til databeskyttelsesforordningen artikel 12, stk. 3. Datatilsynet fandt derimod ikke grundlag for at tilsidesætte kommunens vurdering af, at borgeren ikke havde krav på sletning af oplysninger i forbindelse med, at hendes sag hos kommunen var afsluttet. Datatilsynet henviste til artikel 17, stk. 3, litra b, og bemærkede, at en offentlig myndighed – under henvisning til offentlighedslovens regler om notat- og journaliseringspligt samt arkivlovens regler – i almindelighed ikke er berettiget til at slette bestemte dokumenter, der indgår i en sag, og at sletning

[159] Datatilsynets vejledning om de registrerede rettigheder pkt. 6.2.
[160] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 550

normalt kun kan ske, hvis der er lovhjemmel dertil. Datatilsynet fandt på denne baggrund, at behandling af oplysningerne i borgerens sag ikke var gået ud over princippet om opbevaringsbegrænsning, jf. artikel 5, stk. 1, litra e.[161]

Et eksempel, hvorpå der kan ske sletning er, Dt.s j.nr. 2018-32-0065:
Her havde Statsadvokaten for særlig økonomisk og international kriminalitet videregivet nogle oplysninger til skattemyndighederne, som de havde fremskaffet uden hjemmel i retsplejeloven. Da de var blevet klar over dette, havde de derfor destrueret informationerne igen, men skattemyndighederne ville herefter ikke slette disse oplysninger, da de var konkrete for behandlingen af skattesagen. Datatilsynet gjorde det dog klart at personoplysninger, som er indhentet uden hjemmel i lov, ikke må indhentes i henhold til persondataloven. Skattemyndighederne skulle derfor slette disse oplysninger, selvom det gik imod princippet om dokumentationspligt. Årsagen skulle findes i, at de ikke burde have haft oplysningerne, da de var tilvejebragt i strid med retsplejelovens regler.[162]

Oplysninger kan efter litra c bevares i det omfang, behandlingen er nødvendig af hensyn til samfundsinteresse på folkesundhedsområdet, jf. artikel 9, stk. 2, litra i.[163]

Efter litra d, kan oplysninger bevares i det omfang, behandlingen er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. Om fortsat opbevaring til arkivformål henvises til databeskyttelseslovens § 14.[164]

Efter litra e, kan oplysninger bevares i det omfang, det er nødvendigt for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Se her også artikel 9, stk. 2, litra f.[165]

Slutteligt kan det siges, at artikel 17, stk. 3. har mange betydelige undtagelser, som gør, at det er begrænset, hvad den registrerede kan få slettet i den offentlige sektor. Der vil være flere tilfælde, hvor det er muligt i den private sektor, at få slettet oplysninger, men i mange situationer, vil det nok mere være korrigering af urigtige oplysninger i form af berigtigelse eller en begrænsning af en eventuel behandling, frem for sletning.[166]

[161] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 551
[162] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 551f.
[163] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 552
[164] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 552
[165] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 552
[166] Nielsen & Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven med kommentarer (2020), s. 552f

7.5.2.1 Sletning på den registreredes initiativ

I dette afsnit vil afhandlingen kigge på, om den registrerede har mulighed for at få slettet sine oplysninger hos den offentlige myndighed. Ovenfor i afsnit 7.5.1 er de generelle regler for artikel 17, "retten til at blive glemt" gennemgået.

Den offentlige myndighed er underlagt specielle regler, når det kommer til dokumentation af sager. Forvaltningen skal være sikker på, at alt bliver noteret, således der er mulighed for at dokumenterer en afgørelse overfor en borger. Det kan af den grund være svært for den offentlige myndighed at slette oplysninger, efter de har modtaget eller fået dem. Det fremgår af databeskyttelsesforordningens artikel 17, stk. 3, litra b, at hvis behandlingen er nødvendig for at overholde en retlig forpligtigelse, eller er nødvendig for at udføre en opgave i samfundets interesse, eller en opgave som henhører under offentlig myndigheds udøvelse, som den dataansvarlige er blevet pålagt, så vil der ikke være mulighed for den registrerede til at få slettet sine oplysninger.

I afgørelse Dt.s j. nr.: 2018-32-0286 som er belyst i afsnit 7.5.2 , der omhandler den registreredes rettighed til at blive glemt ved en kommune, kunne afhandlingen udlede, at kommunen godt kunne tilsidesætte den registreredes anmodning om sletning, jf. undtagelsen i artikel 17, stk. 3 litra b.

Det må udledes, at en myndighed ikke er forpligtiget til at slette personoplysninger, da den som tidligere beskrevet skal overholde sin dokumentationspligt i form af notatpligten og journaliseringspligten, som er forklaret i afsnit 6.1.2 og 6.1.3. Grunden til at disse regler skal overholdes er, at borgeren skal have mulighed for at indgive en klage over afgørelsen, hvis der ikke er enighed omkring resultatet. Den offentlige myndighed skal derfor kunne dokumentere sagens gang. Ydermere må det gøres klart, at der er få tilfælde, hvor reglen om sletning kan anvendes. Et eksempel er, hvis personoplysningerne bliver behandlet ulovligt eller, at der er tale om en fejljournalisering fra den offentlige myndighed. Hvis der er tale om en fejljournalisering, skal den offentlige myndighed rette op på fejlen ved at re-journalisere dokumentet og vedlægge et notat om, at denne handling er foretaget.

Den offentlige myndighed har som udgangspunkt kun to muligheder, når det kommer til reglerne om sletning. Enten bliver dokumenterne slettet som led i dataminimering, når slettepolitikken vurderer at oplysningerne ikke længere er nødvendige, ellers kan den offentlige myndighed vælge at anvende reglerne om arkivering og på den måde få oplysningerne slettet. I det efterfølgende afsnit vil arkiveringsreglerne blive kort introduceret.

7.5.2.2 Arkivering

Et alternativ til sletning, som forvaltningen benytter sig af, er at sende personoplysninger til arkiv i overensstemmelse med reglerne i arkivloven. Afhandlingen vil derfor gennemgå disse regler kort i det følgende afsnit.[167]

Arkivering er et alternativ, som ofte bliver anvendt af forvaltningen for at undgå at bryde reglerne om sletning samt dataminimering, jf. databeskyttelsesforordningens artikel 5.

I databeskyttelseslovens § 14, findes der hjemmel til at overføre oplysninger, som er omfattet af databeskyttelsesloven til opbevaring i et arkiv efter arkivlovens regler.

Det fremgår af arkivlovens § 1, stk. 1, at det kun er den offentlige forvaltning samt domstolene, som har adgang til at arkivere. Af stk. 2, 3, 4 og 5 fremgår der visse undtagelser, men fælles for dem er, at virksomheder som er organiseret på baggrund af et privatretligt grundlag, falder uden for lovens anvendelsesområde.[168]

Når personoplysninger, der er indsamlet og behandlet med administrative formål i forvaltningen, ikke længere er aktuelle for den administrative behandling, skal de slettes. Hvis oplysningerne vurderes at skulle bevares i henhold til historisk, samfundets interesse eller videnskabeligt øjemed, skal de arkiveres i henhold til arkivlovens § 21.[169]

Det fremgår af databeskyttelsesforordningens artikel 89, at der skal være fornødne garantier til stede, når personoplysninger bliver overført til arkivformål. I arkivlovens §§ 23 og 39 a, er der implementeret garantier for at kunne leve op til forordningens artikel 89.

I henhold til arkivlovens § 23, kan arkivenheder, som indeholder oplysninger om enkeltpersoners private forhold såsom økonomi, tidligst være tilgængelig efter 75 år. Denne bestemmelse afhjælper spørgsmålet om, hvorvidt en databehandler eller dataansvarlig har mulighed for at tilgå oplysninger om den registrerede.

Udover garantien om tilgængelighed findes retten til indsigt i egne personoplysninger, som er blevet overført til et offentligt arkiv, jf. Arkivlovens § 39a. Retten til indsigt i arkivloven minder meget om retten til indsigt efter databeskyttelsesforordningen. Der er dog et par undtagelser som udspringer fra forordningens artikel 89, stk. 3, hvor det fremgår, at når personoplysninger behandles til arkivformål, så må der fastsættes undtagelser fra den registreredes rettigheder.

Hvis den registrerede ønsker indsigt i personoplysninger, der er omfattet af databeskyttelsesforordningens anvendelsesområde, skal indsigten begæres efter arkivlovens § 39a.

---

[167] Datatilsynets vejledning om de registreredes rettigheder juli 2018. s. 36
[168] Arkivlovens §1: Karnovs noter
[169] Arkivlovens §21: Karnovs noter

Det fremgår af denne bestemmelse, at der kan fremsættes begæring om indsigt i egne personoplysninger, der er helt eller delvis foretaget ved hjælp af automatisk databehandling, eller som er indeholdt i et register. Arkivlovens § 39 a, stk. 2. fastsætter, at den registrerede skal angive, hvilken myndighed der oprindeligt har behandlet oplysningerne. Grunden til denne bestemmelse er, at arkivet skal videresende begæringen til den pågældende myndighed, jf. stk. 3, da det er pågældende myndighed, der skal træffe afgørelse om retten til indsigt, jf. stk. 4.[170]

Der findes indsigt efter arkivlovens § 39 b, men oplysningerne som borgeren i dette tilfælde får adgang til, er ikke omfattet af databeskyttelsesforordningens anvendelsesområde.

Før den offentlige myndighed afleverer IT-systemer eller data til arkivering, er det vigtigt, at der ikke må slettes noget fra dens systemer, før informationerne er afleveret.

Når oplysningerne overføres fra den offentlige myndighed til arkivet, overgår ansvaret samtidig fra myndighedens dataansvarlige til arkivets dataansvarlige. Derfor må det antages, at den offentlige myndighed ikke længere behandler disse data og på den måde ikke kan få adgang til de samme data igen, hvilket udgør betingelserne for sletning. Sletning og arkivering er ikke helt det samme, eftersom data ikke bliver destrueret ved arkivering. Derimod må det antages, at arkivering er et alternativ til sletning, hvilket der direkte findes hjemmel til i databeskyttelsesloven § 14.[171]

Efter Rigsarkivets hjemmeside kan processen for arkivering beskrives på følgende måde: Kommunen udfylder en blanket til Rigsarkivet, herefter sender Rigsarkivet nogle skemaer, der skal udfyldes. Derefter bliver der holdt et møde omkring dataindhold og dokumentation af arkiveringsversionen samt en tidsplan for forløbet. Rigsarkivet udsteder en afleveringsbestemmelse, hvori arkiveringsversionen og afleveringsdatoen fremgår. Kommunen indsender dokumentation til godkendelse og udtrækker data fra systemet og producerer arkiveringsversionen (evt. ekstern it-leverandør). Kommunen eller it-leverandøren tester arkiveringsversionen med testprogrammet Ada, Rigsarkivets testprogram. Herefter afleveres arkiveringsversionen til Rigsarkivet. Rigsarkivet kvitterer for afleveringen og tester arkiveringsversionen.[172]

[170] Arkivlovens §39 a: Karnovs noter
[171] Databeskyttelseslovens § 14: Karnovs noter
[172] https://www.sa.dk/wp-content/uploads/2015/10/Kort-og-godt-om-aflevering-af-it-KOMMUNE2.pdf

7.5.3 Retten til begrænsning af behandling

Den registrerede har ret til at få begrænset behandlingen af sine personoplysninger, så disse ikke længere bliver behandlet, men kun opbevaret. Der fremgår 4 situationer af databeskyttelses forordningens artikel 18, hvorved den registrerede har ret til at få begrænset behandlingen.[173]

Første tilfælde er, hvor den registrerede bestrider rigtigheden af personoplysningerne. I dette tilfælde vil den dataansvarlige skulle begrænse behandlingen af personoplysningerne, imens der findes ud af, hvorvidt personoplysningerne er korrekte.[174]

I andet tilfælde behandler den dataansvarlige oplysningerne ulovligt, og den registrerede modsætter sig sletning af oplysninger, men anmoder om begrænsning af behandling. Umiddelbart virker dette som en meget speciel bestemmelse, da man skulle tro, at den registrerede ville ønske at få slettet sine personoplysninger, hvis de bliver behandlet ulovligt, men denne bestemmelse er dog ret vigtig, da den registrerede har mulighed at kunne dokumentere, at disse oplysninger har indgået i sagsbehandling, hvis det skulle ende ud i en retssag eller anden afgørelsessag.[175]

Det tredje tilfælde er, hvor den dataansvarlige ikke længere har brug for personoplysningerne til en behandling, men de er nødvendige for at et retskrav kan fastlægges, gøres gældende eller forsvares. Det må derfor antages, at det kun er en begrænsning af de oplysninger, som er nødvendige for at retskravet kan fastlægges, gøres gældende eller forsvares.[176]

Det fjerde tilfælde er, hvor den registrerede har gjort indsigelse efter databeskyttelsesforordningens artikel 21. Den dataansvarlige skal derfor i denne periode begrænse behandlingen af oplysningerne, hvor det kontrolleres, om den dataansvarlige legitime interesser går forude for den registreredes.[177]

I den periode hvor behandlingen skal begrænses, er det vigtigt, at der ikke er andre, der kan få fat personoplysningerne. I praksis ville man gøre det, at man begrænser brugerrettighederne i systemet sådan, at andre medarbejdere ikke ville kunne logge ind i den del af databasen. Herved undgår man, at andre medarbejdere/brugere får adgang til oplysningerne. Hvis der er tale om en hjemmeside, hvor oplysningerne ligger på, skal de også fjernes derfra midlertidigt. Når den dataansvarlige begrænser behandlingen af personoplysninger i eget system, skal dette også underrettes til andre, som oplysningerne er videregivet til, jf. databeskyttelsesforordningens artikel 19.

---

[173] Datatilsynets vejledning om den registreredes rettigheder, s. 37
[174] Datatilsynets vejledning om den registreredes rettigheder, s. 37
[175] Datatilsynets vejledning om den registreredes rettigheder, s. 37
[176] Datatilsynets vejledning om den registreredes rettigheder, s. 37
[177] Datatilsynets vejledning om den registreredes rettigheder, s. 37

Inden begrænsningen ophæves, skal den dataansvarlige underrette den registrerede om dette.[178]

7.5.4 Den registreredes ret til indsigelse

I henhold til databeskyttelsesforordningens artikel 21, har den registrerede ret til at fortage indsigelse mod den dataansvarliges behandling af personoplysninger. Muligheden for indsigelse finder kun anvendelse, hvis behandlingen er lovlig eller er nødvendig for den dataansvarlige, jf. præambelbetragtning 69.

Der kan derfor opstilles to krav til indsigelsesretten.

Første krav: Den registrerede har ret til indsigelse, hvis en af følgende behandlingsgrundlag bliver anvendt:

> *" a) Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som du som dataansvarlig har fået pålagt*
>
> *b) Behandlingen er nødvendig for, at du som dataansvarlig eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn."*[179]

Et af disse krav skal være opfyldt før reglen om indsigelse kan anvendes.

Det andet krav: Ved enhver indsigelse skal den dataansvarlige altid fortage en ny vurdering af, om oplysningerne, der bliver behandlet, er nødvendige for behandlingen, eller om disse kan minimeres.

Hvis den dataansvarlige kommer frem til, at alle oplysninger er nødvendige, skal den dataansvarlige forklare overfor den registrerede, at der er foretaget en ny og konkret vurdering af oplysnin-

[178] Datatilsynets vejledning om den registreredes rettigheder, s. 37-38
[179] Datatilsynets vejledning om den registreredes rettigheder, s. 44

gerne, og overfor den registrerede forklare disse begrundelser. Hvis behandlingen af disse oplysninger fremgår ved lov, kan den dataansvarlige allerede her afvise indsigelsen.[180] Hvis den dataansvarlige kommer frem til, at oplysningerne ikke er nødvendige, skal behandlingen af disse oplysninger stoppes.[181]

7.6 Opsummering af den registreredes rettigheder

Når der snakkes om berigtigelse, sletning og begrænsning, er det som nævnt tidligere lagt op til, at den registrerede nu selv kan vælge, hvilken hjemmel der skal benyttes, hvor det tidligere var den dataansvarlige, som frit kunne vælge. Afhandlingen har i afsnit 7.2 nævnt flere afgørelser fra datatilsynet, hvori der fremgår flere eksempler på situationer, hvor den dataansvarlige ikke har gjort sit arbejde godt nok i forhold til dataminering. I disse tilfælde, hvor den dataansvarlige ikke gør det godt nok, kan der udtales kritik og i særligt alvorlige situationer også ske politianmeldelse med formål om udstedelse af bødestraf.

Det fremgår flere steder i afhandlingen at sletning ikke kan finde sted i forvaltningen, da det ofte er umuligt grundet krav om dokumentationspligt. Det næstbedste de derfor kan gøre, er at berigtige informationerne. Berigtigelsen skal ske "uden unødvendig forsinkelse". Uden unødvendig forsinkelse er en bred størrelse, for hvad er unødig forsinkelse. Er der tale om vigtige oplysninger, skal målestokken nok ses meget strengt, hvorved det skal rettes med det samme. Det kunne f.eks. være livstruende situationer, hvor der er registeret en forkert blodtype i en journal. Derimod ville det nok være fint nok at vente med at opdatere en markedsføringsliste, før man benytter denne næste gang.[182] Har myndigheden offentliggjort en registreredes oplysninger online, og nogen har downloadet informationen, har den dataansvarlige pligt til at begrænse spredningen. Begrænsning er ikke dataminimering, det er en blokering af oplysninger, som den registrerede har indsigelse imod. De skal derfor tage step til at få fjernet eventuelle links, der deler informationen, og gøre folk, som har downloadet informationen, klar over, at den registrerede har trukket sit samtykke tilbage, hvorved de bliver tvunget til at tage stilling til, om de stadig må benytte informationen.

[180] Datatilsynets vejledning om den registreredes rettigheder, s. 44-45
[181] Datatilsynets vejledning om den registreredes rettigheder, s. 44
[182] Bent Ole Gram Mortensen: Dansk persondataret (2020), s. 220f.

8. Sammenspillet mellem aktindsigt og indsigtsretten.

I forbindelse med indsigtsretten gælder der nogle flere regler i forvaltningen, end der gælder ved en privat virksomhed. Forvaltningen skal udover at tage hensyn til indsigtsretten også informere den registrerede om, at der kan søges aktindsigt efter reglerne i hhv. forvaltningsloven samt offentlighedsloven. Forvaltningen er i den henseende forpligtet til at anvende det regelsæt, som er mest gunstig for den registrerede. I dette afsnit vil afhandlingen forklare den sondring, der ligger mellem, om forvaltningen skal vælge at benytte reglerne efter databeskyttelsesforordningen, forvaltningslovens eller offentlighedsloven.

I afsnit 7.4 er reglerne for indsigtsretten beskrevet, og i afsnit 6.2.1 er retten til partsindsigt i henhold til forvaltningsloven, samt afsnit 6.3 er retten til aktindsigt i henhold til offentlighedsloven beskrevet.

Der kan som udgangspunkt udledes fire forskellige situationer, hvor der skal vurderes, hvilke regelsæt som skal anvendes for enten at få indsigt, partsindsigt eller aktindsigt.

Det første tilfælde er en situation, hvor den registrerede ønsker at få oplysninger omkring sig selv, men er ikke part i nogen sag i forvaltningen. Når der er tale om, at den registrerede ønsker oplysninger om sig selv, vil hovedreglen være, at der gives indsigt efter databeskyttelsesforordningen samt offentlighedsloven. Hvis den dataansvarlige er i tvivl om, hvilket regelsæt den registrerede gerne vil have anvendt, kan den dataansvarlige kontakte den registrerede for at få det afklaret. Hvis den registrerede fra starten, kun anmoder om aktindsigt efter offentlighedsloven, påhviler der en vejledningspligt fra forvaltnings side, jf. forvaltningslovens § 7, stk. 1. Grunden til at forvaltningen er forpligtet ved lov om denne vejledningspligt er, at der vil være stor forskel på at begære indsigt efter de to regelsæt. Retten til indsigt efter databeskyttelsesforordningen kommer med flere supplerende oplysninger, som er beskrevet i afsnit 7.4, og indsigten kan derfor omfatte flere oplysninger end aktindsigt efter offentlighedsloven.

Det andet tilfælde er, hvor den registrerede ønsker indsigt i egne oplysninger og samtidig er part i en afgørelse. Eftersom den registrerede er part i en afgørelsessag, vil der i dette tilfælde være mulighed for både at anvende databeskyttelsesforordningens artikel 15, samt forvaltningslovens § 9-10. Hovedreglen er, at der gives indsigt efter både databeskyttelsesforordningen samt forvaltningsloven. Som i første tilfælde kan det offentlige risikere, at den registrerede kun anmoder om indsigt efter et af regelsættene. Der påhviler derfor forvaltningen en vejledningspligt efter forvaltningslovens § 7, stk. 1. Der vil nemlig kunne være forskel på den type af dokumenter som den registrerede modtager, hvis der kun søges om indsigt efter et regelsæt. I afsnit 7.4 og i afsnit 6.2 er det beskrevet, hvilke

dokumenter der kan begæres indsigt i efter hhv. databeskyttelsesforordningen samt forvaltningsloven. Fordelen ved at anmode om indsigt efter forvaltningsloven vil være, at den registrerede vil have ret til at se dokumenter, som er en del af afgørelsen, og som nødvendigvis ikke indeholder personoplysninger. Disse dokumenter følger ikke med ved indsigt efter databeskyttelsesforordningen, da disse dokumenter er uden for dennes formål.

Den tredje situation er, hvor den registrerede søger indsigt i oplysninger om andre personer eller oplysninger, som ikke er personoplysninger, og den registrerede ikke er part i en afgørelsessag. Når den registrerede søger indsigt på denne måde, finder databeskyttelsesforordningen ikke anvendelse, da der ikke er tale om egne personoplysninger. Forvaltningsloven finder heller ikke anvendelse, da den registrerede ikke er part i en afgørelsessag. Hvis der skal søges indsigt i disse sager, skal offentlighedslovens § 7-8 anvendes, da der søges om almindelig aktindsigt.

Den fjerde situation er, hvor den registrerede ønsker indsigt i oplysninger om andre eller sig selv, som ikke er personoplysninger, men er part i en afgørelsessag, hvori oplysningerne indgår. Som forklaret ovenfor kan databeskyttelsesforordningen ikke anvendes, da der ikke er tale om indsigt i personoplysninger. Offentlighedsloven kan heller ikke anvendes, da der søges indsigt i en afgørelsessag, hvor den registrerede er part. Hvis der skal søges indsigt i en afgørelses sag, hvor den registrerede er part, anvendes reglerne om partsindsigt i forvaltningslovens § 9-10.

9. Dataminimering i forvaltningen

9.1 Hvordan skal myndighederne tage stilling til reglerne?

Først og fremmest skal de tage stilling til, om de er omfattet af reglerne i forordningen (artikel 1-4). Herefter skal de sikre, at de har hjemmel, dette findes i behandlingsbetingelserne (artikel 6-10). Dernæst skal de altid følge principperne i artikel 5. De skal endvidere tage stilling til de registreredes rettigheder (artikel 12-23). Slutteligt skal de tage stilling til rammerne for behandlingen. Rammerne er specifikke for de enkelte organisationer, da de i nogen grad selv kan vælge, hvilke foranstaltninger der benyttes. Fælles for alle organisationerne er dog reglerne, som skal overholdes. Det vil sige, de skal alle kunne dokumentere et gyldigt samtykke, og kravet for dette er det samme for alle, store som små. Virksomheden/myndigheden skal altså have styr på sin behandlingsproces, da man skal dokumentere, hvordan man har tænkt sig at overholde reglerne (jf. artikel 5, stk. 2)

Når der tales om, at myndighederne skal overholde reglerne, skal den dataansvarlige indføre politikker og mekanismer i organisationen, som vil sikre, at forordningen bliver overholdt, procedurer for sletning af forældet materiale samt undervisning af medarbejdere i, hvordan de skal journalisere, så man kan sætte systemer op, som automatisk sletter ud fra fastsatte slettefrister.
Slettefristen skal være proportional med formålet som nævnt i afsnit 7.2.5.1 Der findes flere afgørelser på, at slettefrister kan variere afhængigt af formål. Hvis man låner bøger på biblioteket, har man behov for at vide, hvem personen er, der har lånt bogen, indtil den bliver returneret. Derefter er der ikke behov for oplysningerne, hvorfor der burde være en kort slettefrist, medmindre man har brug for opbevaring pga. lovgivning (bogføringsloven, forældelsesloven mv.) eller andre formål, så kan der være flere års slettefrist. Det skal derfor altid vurderes ud fra en konkret vurdering.

Af nyere praksis på området har afhandlingen valgt at behandle to afgørelser, som omhandler sletteprocedurer:

9.2 Dt.s. jnr.: 2019-431-0052 – Offentliggørelse af billeder på virksomheds Facebookside

500.000 billeder af børn og unge var offentliggjort på Epic Bookings Facebookside – Billederne var taget til fester og lignende arrangementer primært ved brug af et selfiekamera.

Datatilsynet fandt i sagen, at det samtykke, som personerne på billederne havde givet, ikke levede op til kravet om informeret, specifikt og frivilligt. Det var endvidere i strid med princippet om opbevaringsbegrænsning, at Epic Booking ikke havde fastsat en konkret slettefrist.

Det var Datatilsynets vurdering, at de afbillede personer nød en særlig beskyttelse, som børn og unge nyder efter databeskyttelsesreglerne. Epic Booking fik derfor påbud om at fastsætte slettefrister på maksimalt 60 dage for billeder, der fremover offentliggøres.

De vigtigste udpluk fra afgørelsen:

Det fremgår af sagens oplysninger, at Epic Booking behandlede oplysningerne til flere formål, herunder til drifts- og forretningsmæssige formål (f.eks. salg af billeder) samt til brug for markedsføring over for nye kunder.

Vedrørende virksomhedens samtykke

Datatilsynet finder, at Epic Bookings offentliggørelse af billeder på virksomhedens Facebook-side er i strid med databeskyttelsesforordningens artikel 6, stk. 1, litra a, da der ikke er indhentet et gyldigt samtykke fra de registrerede, jf. artikel 4, nr. 11. Datatilsynet har herved lagt vægt på, at de registrerede på tidspunktet for afgivelse af deres samtykke ikke har haft mulighed for at til- eller fravælge de forskellige behandlingsformål, hvilket ikke er i overensstemmelse med databeskyttelsesreglers krav til et gyldigt samtykke. De registrerede har således ikke haft mulighed for at træffe et informeret valg, ligesom de ikke har haft reel kontrol over behandlingen af oplysninger om sig selv.

Endvidere har tilsynet lagt vægt på, at det af den anvendte samtykketekst ikke fremgår, hvad formålene med behandlingen er, herunder at billederne tillige behandles til markedsføringsmæssige formål, ligesom teksten ikke indeholder information om opbevaringstiden.

Det er på den baggrund Datatilsynets vurdering, at den anvendte samtykketekst ikke er tilstrækkelig specifik og informeret, ligesom de pågældende ikke har givet et reelt frit samtykke. De anvendte samtykker er således ikke i overensstemmelse med kravene til et gyldigt samtykke efter forordningens artikel 4, nr. 11.

Oplysningspligt

Datatilsynet finder, at indholdet i den informationstekst, der opsættes i en nærmere afgrænset zone, ved og foran selfiekameraet, og det "speak", som gives ved et arrangement, ikke lever op til kravene i databeskyttelsesforordningens artikel 12, stk. 1, og artikel 13, stk. 1 og 2.

Datatilsynet har herved lagt vægt på navnlig, at oplysningsteksten ikke indeholder oplysninger om formålene med behandlingen, jf. artikel 13, stk. 1, litra c, og oplysninger om tidsrummet for offentliggørelsen af billederne på facebooksiden, jf. artikel 13, stk. 2, litra a. Oplysningen om opbevaringstiden er efter tilsynets vurdering nødvendig for at sikre en rimelig og gennemsigtig behandling, jf. artikel 13, stk. 2, litra a, og er således en (yderligere) oplysning, som den registrerede har ret til, og bør gives umiddelbart til den registrerede ved fotograferingen.

Opbevaringsbegrænsning

Epic Booking har oplyst, at billeder på facebooksiden offentliggøres (opbevares) uden tidsbegrænsning, idet kunderne forventer dette.

Datatilsynet vurderer, at en offentliggørelse uden tidsbegrænsning er i strid med princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e. Datatilsynet har herved lagt vægt på hensynet til de afbillede personer, herunder den særlige beskyttelse som børn og unge nyder efter databeskyttelsesreglerne, og behandlingens karakter (offentliggørelse på Facebook). Endvidere har Datatilsynet lagt vægt på, at en frist på maksimalt 60 dage efter tilsynets opfattelse vil være tilstrækkelig til at opfylde kundernes behov for at kunne tilgå billederne.

Opsummering

Denne afgørelse viser, at opbevaringsbegrænsningen skal være proportional med formålet. Det er ikke proportionalt, at en virksomhed kan nyde gratis markedsføring på ubestemt tid, ved at henvende sig til unge i festligt lag og ikke gøre dem opmærksom på, hvad det medfører. Datatilsynet vurderer, at når der er tale om børn og unge, så skal der være tale om 60 dage til at hente billederne ned til en selv, hvorefter virksomheden skal slette oplysningerne, hvilket måske er relativ kort frist. Denne frist må dog skulle ses ud fra et beskyttelsesperspektiv af børn og unge, hvorved en virksomhed, som håndterer fester for voksne, nok ville kunne slippe afsted med en længere slettefrist. Afgørelsen vil dog formentligt blive et udtryk for virksomheders billedpolitik fremadrettet, da Datatilsynet mener, at forretningsøjemed ikke er god nok grund for en længere opbevaring. Havde virksomheden derimod fastlagt en frist på 6 måneder, så ville Datatilsynet måske have godkendt en sådan sletteprocedure i stedet for at udtale kritik, da virksomheden i så fald havde taget aktivt stilling til en procedure for behandling af reglerne.

9.3 Dt.s j. nr. 2018-41-0016 - Tilsyn med Taxa 4x35's behandling af personoplysninger

Datatilsynet var i efteråret 2018 på et tilsynsbesøg hos Taxa 4x35 (herefter Taxa), hvor de kiggede på, om taxaselskabet havde fastsat frister for sletning af kundernes oplysninger - og om fristerne blev efterlevet.

Ifølge Taxa anonymiseres de oplysninger, der anvendes til kundens bestilling og afvikling af taxature, efter to år. Det var imidlertid kun kundens navn, der blev slettet efter en frist på 2 år. Kundens telefonnummer eksisterede stadig i systemet og blev først slettet efter fem år. Kundens taxature,

herunder opsamlings- og afleveringsadresser, kunne henføres til en fysisk person via telefonnummeret.

Årsagen til, at der ikke skete sletning af telefonnummeret, var ifølge selskabet, at det blev benyttet som nøgle til systemets database og derfor var nødvendigt for virksomhedens produkt- og forretningsudvikling.

Datatilsynet fandt, at man ikke kan fastsætte slettefrister, som er tre år længere end nødvendigt, fordi virksomhedens systemer ikke lever op til databeskyttelsesforordningen.[183]

Anonymisering af taxature

Taxa benyttede et system som hedder DDS Pathfinder, et system hvor deres kunder kan bestille taxature. For at kunden kan anvende systemet, skal der registreres en del oplysninger såsom navn, adresse, telefonnummer, dato for kørsel, start- og sluttidspunkt mv. Ifølge Taxa bliver oplysningerne anonymiseret efter 2 år, da de vurderer, at oplysningerne ikke længere tjener et formål herefter. Anonymiseringen består i at kundens navn slettes. Taxa oplyser i den forbindelse, at kundens telefonnummer bevares som datagrundlag for forretningsudvikling.

Datatilsynet fortog under tilsynet stikprøver af DDS Pathfinder. Datatilsynet fandt, at når de søgte på kundens telefonnummer i databasen, kunne de finde frem til kundens taxature efter 2 års fristen. Det var derfor af Datatilsynets opfattelse, at Taxa ikke havde foretaget en reel anonymisering, da oplysningerne ikke var uigenkaldelige.

Datatilsynet vurderede at Taxa ikke levede op til databeskyttelsesforordningens artikel 5, stk. 1, litra e, da det stadig var muligt at identificere den registrerede efter Taxas 2 års frist var udløbet.

Opbevaring af kundens telefonnummer i 5 år i forhold til kravet om dataminimering

I henhold til opbevaringen af kundens telefonnummer i 5 år kiggede Datatilsynet nærmere på, hvorvidt Taxa levede op til reglerne om dataminimering, jf. Databeskyttelsesforordningens artikel 5, stk. 1, litra c. Taxa oplyste i forbindelse med besøget, at det kun er kundens telefonnummer, som opbevares i 5 år efter kørslen, da det udelukkende skal bruges til forretningsudvikling. Telefonnummeret var den fælles referenceramme i DDS Pathfinder. I den forbindelse oplyste Taxa et andet unikt ID-nummer, der tjente samme formål som telefonnummeret efter de 2 år var passeret, men systemet kunne ikke bagudrettet erstatte telefonnumrene med ID-nummeret.

[183] https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/tilsyn-med-taxa-4x35s-behandling-af-personoplysninger?fbclid=IwAR3xoR4r62gklxfT8IXkVG6LzCRDqVFmZTqVSn-xpJQTJuSpTtWIgd9guvA

Datatilsynet mente, at anvendelsen af telefonnummeret ikke var i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra c, da der ikke var et formål med at behandle telefonnummeret, eftersom det kunne erstattes med et ID-nummer.

Datatilsynet bemærkede desuden, at omkostninger forbundet med migrering af oplysninger om taxature til en ny datastruktur ikke kunne begrunde en manglende sletning af kundens telefonnummer efter 2 års fristen.

Uklarhed om behandlingshjemmel

Datatilsynet havde i forbindelse med tilsynet spurgt Taxa, hvilke tanker de havde gjort sig ved fastlæggelsen af den 5-årige frist. De fortalte, at telefonnummeret var nøglen til deres system DDS Pathfinder og derfor var nødvendig for forretningsudviklingen. Efter tilsynet modtog Datatilsynet et brev fra Taxas advokat. Her fortalte advokaten, at opbevaringen af telefonnummeret i 5 år var i overensstemmelse med taxibekendtgørelsen, og at telefonnummeret var nøglen til DDS Pathfinder systemet. Datatilsynet bad advokaten om at uddybe denne begrundelse og henvise til, hvor denne bestemmelse i taxibekendtgørelsen kunne findes. Advokaten svarede tilbage, at begrundelsen om taxibekendtgørelsen beroede på en misforståelse, samt at telefonnummeret var nøglen til systemet.

Det var af Datatilsynets opfattelse at Taxa ikke levede op til kravene i databeskyttelsesforordningens artikel 5, stk. 1, litra b og artikel 5, stk. 2, da der igennem hele forløbet havde været uklarhed om hjemmelsgrundlaget for behandlingen af kundens telefonnummer i DDS Pathfinder.

Dokumentation af procedurer for sletning

I forbindelse med tilsynet havde Datatilsynet gennemgået Taxas efterlevelse af kravene til sletning af personoplysninger, herunder procedurerne for sletning samt dokumentation. Datatilsynet kunne konstatere, at dokumentation for sletteprocedurer var overfladisk samt mangelfuld i henhold til det materiale som datatilsynet havde adgang til. Datatilsynet havde efterspurgt dokumentation for *"opfølgning på, at sletning er foretaget korrekt i systemerne; håndtering af genindlæsning af tidligere slettede personoplysninger ved ibrugtagning af backup; og logning af sletninger i systemerne."*.

I henhold til kravene om dokumentation for, opfølgning på sletning og håndtering af genindlæsning af tidligere slettede personoplysninger ved ibrugtagning af backup har Taxa oplyst, at der ikke findes nogen form for dokumentation.

I henhold til logning af sletninger foretaget i systemet fandt Datatilsynet, at de udelukkende blev foretaget i et manuelt Excel-ark. Der var ikke tale om logning af konkrete sletninger, men der-

imod en historik over, hvem der havde foretaget sletningen, i hvilket system og hvornår det var foretaget. Taxa havde tilbage i 2018 iværksat implementering af en funktionalitet til logning af slettede oplysninger.

Det var Datatilsynets opfattelse, at Taxa ikke havde levet op til kravene i databeskyttelsesforordningens artikel 5, stk. 2, jf. artikel 5, stk. 1, litra e. Taxa kunne ikke dokumentere virksomhedens procedurer for opfølgning på sletning, håndtering af genindlæsning af tidligere slettede personoplysninger ved ibrugtagning af backup, samt at logningen var utilstrækkelig.

Opsummering

Denne afgørelse viser, hvordan virksomheder skal leve op til kravene om opbevaringsbegrænsning, anonymisering, dataminimering, behandlingsformål samt dokumentation for sletningsprocedurer.

I forhold til opbevaringsbegrænsning samt anonymisering viser denne afgørelse, at hvis en virksomhed kan fremsøge oplysninger ved hjælp af en "nøgle", så har de ikke levet op til kravet om anonymisering, da oplysningen i så fald ikke er uigenkaldelig. Der har kun været tale om pseudoanonymisering, som er en sikkerhedsforanstaltning og derfor ikke fuldt anonymiseret efter databeskyttelsesforordningen.

I forhold til dataminimering viser afgørelsen, hvornår en oplysning ikke længere er relevant for behandlingsformålet. I den konkrete situation, har virksomheden beholdt telefonnummeret i 3 år udover formålet, hvilket skulle være slettet efter de 2 år eller anonymiseret.

I forhold til behandlingsformålet fremgår det, at der skal være en konkret hjemmel for behandling af personoplysninger. Dette var ikke opfyldt i den pågældende sag, da man opbevarede personoplysninger i 5 år, hvor man kun havde hjemmel til 2 år.

I forhold til dokumentation for sletteprocedurer viser afgørelsen, at virksomheder skal have mere fokus på generelle sletteprocedurer samt dokumentation herfor, da Datatilsynet skal kunne føre kontrol. I dette tilfælde kunne virksomheden ikke dokumentere de sletninger, som var foretaget, samt procedurerne herfor.

9.4 Slettefrister for data

Afhandlingen har efter gennemgangen af reglerne sat to fiktive forløb op vedrørende en måde at dataminimere på, i form af procedurer som en måde at overholde databeskyttelsesreglerne på. Et i henhold til sletning og et i henhold til anonymisering.

Afhandlingen har fundet inspiration i et fiktivt forløb fra datatilsynets hjemmeside vedrørende slettefrister.

Det fremgår at man skal have flere lag i sine IT-systemer, så man derved kan lave separate regler for behandlingen. Det vil sige faktura har en slettefrist på 5 år, jf. bogføringsloven, mens der for markedsføring fastsættes en frist på 2 år på samtykket, jf. forældelsesloven og markedsføringslovens § 10. Hvis kunden sletter sin profil, skal systemet slette oplysningerne efter 6 måneder. Virksomheden skal kun gemme de fornødne data og alle andre skal slettes, når de ikke er nødvendige. Ved at dele systemerne op, er det nemmere for virksomheden at automatisere en eventuel sletnings procedure, den skal dog stadig tjekke, at oplysningerne bliver slettet korrekt. Dette gøres i form af en opfølgning af procedure, da der altid kan ske fejl i den første "oprydnings" fase. Hvis der foretages backup af system data, så skal logning være slået til, så man kan finde frem til data og slette det, hvis det ikke er teknisk muligt at slette i backuppen, så skal det gøres efterfølgende. Derfor er logning en god ide, da man herved kan sikre at få alt nødvendigt data slettet. En sådan log bør – ud fra princippet om dataminimering – ikke indeholde direkte personhenførbare oplysninger, men kan i stedet angive fx, at en given række i en tabel er slettet på et givent tidspunkt.[184]

En kort opsummering vil derfor være, at virksomheden skal tage stilling til slettefrister for forskellige personoplysninger med baggrund i behandlingens formål. Virksomheden skal fastlægge og dokumentere sletteprocedure/slettefrister. Virksomheden skal overholde lovmæssige krav, som kan påvirke en slettefrist. Virksomheden skal dokumentere en procedure for opfølgning på, at sletning er forløbet som forventet. Virksomheden skal tænke sletning ind i behandlingen så systemerne, der benyttes, kan have forskellige slettefrister afhængigt af formålet.

Et alternativ til slettefristen er en arkivering frist jf. afsnit 7.5.2.2.

Af praksis vedrørende dataminimering og sletning kan nævnes:

9.5 Anonymisering af data

Det andet fiktive forløb beskriver tankeprocesser en forvaltningsmyndighed kunne have i forbindelse med viderebehandling til videnskabelige og historiske forskningsformål af konkrete personers præstationsevner indenfor sport. Her er et spørgsmål vedrørende dataminimering og anonymisering af data, hvad der skal til, før et datasæt er anonymiseret uigenkaldeligt.

Hvis den dataansvarlige har erstattet en identifikationsoplysning, f.eks. navn, CPR-nummer, adresse eller lignende med et kodenummer, men beholdt en "nøgle", hvorved der igen kan ske identificering af fysiske personer, er personoplysningerne ikke anonymiseret i databeskyttelsesforordningens forstand. Der er tale om pseudonymisering jf. afsnit 7.1.2 Dette er også tilfældet, selv om det

[184] https://www.datatilsynet.dk/emner/persondatasikkerhed/sletning

ikke er den dataansvarlige, som selv er i besiddelse af nøglen, hvis det er muligt og plausibelt for andre at finde tilbage til nøglen. Der er ikke tale om anonymisering, men blot en sikkerhedsforanstaltning, der gør det svært at koble et datasæt sammen med den registrerede, originale identitet.[185]
Når den dataansvarlige modtager en dataleverance. Hvornår vil disse data være anonymiseret? Til det formål indsættes flere step i vurderingen af, hvad der vurderes til at være godt nok.

Step 1: Leverandøren har filer som er lagret i foldere med navn, "Hans Hansen_1991-02-07-HH". Filerne er såkaldte metadata, som er f.eks. navn, fødselsdato, køn, erfaring niveau. Dertil indeholder filerne en masse tal, som bliver lavet af en maskine, baseret på bevægelighed af kroppen (punktkoordinator og i fremtiden ledvinkler). Den dataansvarlige kan som modtager finde tilbage til personerne via et kundekartotek. Der er ikke sket nogen dataminering.

Step 2: Leverandøren renser data for navneinformation, som bliver erstattet af mere anonymiseret karakter, f.eks. foldernavne som: M29-profesional-swimming_14kmh. Den dataansvarlige skal ikke bruge navnet, så det er væk, men ønsker at beholde de øvrige metadata, såsom alder, køn og erfaring, da disse har betydning for leverandørens behandlingsformål. Svømmer folk på 60 år længere end folk på 20? Hvis man sammenligner disse data, vil man kunne finde frem til, hvem der har svaret hvad i leverandørens kundekartotek. Det er derfor muligt at genskabe kundeinformationen. Der er sket dataminimering, som kan genskabes nemt.

Step 3: Den dataansvarlige kan erstatte fødselsdato med personens alder på optagelsestidspunktet og slette optagelsestidspunktet fra datasættet. Herved bliver datasættet yderlig anonymiseret i forhold til leverandøren. Beregning af fødselsdato ville kræve alder og optagelsestidspunkt, og optagelsestidspunktet er slettet. Det vil her kræve meget arbejde samt adgang til leverandørens database at finde frem til oplysningerne, som så skal sammenlignes for at finde frem til personerne, dog stadig teoretisk plausibelt. Der er sket dataminimering, som vurderes tilstrækkeligt med nuværende sikkerhedsforanstaltninger.

Step 4: Dataleverancen indeholder som nævnt maskindata, som er baseret på bevægelighed af kroppen. Udviklingen fremadrettet vil medføre at punktkoordinator erstattes af ledvinkler. Processering til ledvinkler sker på grundlag af en model, som hele tiden forbedres, og med tiden vil disse være så præcise, at det kan pege mod en person og være så præcis, at der kan ske identificering af enkeltpersoner. Det vil være temmelig besværligt og kræve en del databehandling og programmering at finde personen, men plausibelt. Skal der dataminimeres på ledvinklerne, vil det give et tab i forhold til de oprindelige data, da de empiriske data er mere valide. Med udviklingen for øje, kan det blive

[185] Artikel 29-gruppen: Udtalelse nr. 05/2014 om anonymiseringsteknikker s. 3

nødvendigt at lave dataminimering af ledvinkler, så data ikke kan genskabes. Det vurderes ikke at være nødvendigt med de nuværende teknologiske forudsætninger.

Step 5: Led vinklerne kan laves om til matematiske funktioner, hvorved data komprimeres flere tusinde gange. Data bliver tabt, og vil ikke kunne genskabes. Selv med adgang til leverandørens kundekartotek, vil det være vanskeligt at finde frem til personerne, dog stadig en teoretisk mulighed.

Ud fra det ovenstående eksempel er der givet indblik i en leverandørs datasæt og beskrevet, hvordan den dataansvarlige kan tage stilling til dataminimering og anonymisering af persondata. Den dataansvarlige vil derfor skulle lave en konkret vurdering, hvorvidt der skal behandles data ud fra step 1-5. Det er afhandlingens vurdering, at ved step 3 opnår man en anonymisering, som vil være tilstrækkelig, da det vil kræve begge datasæt, og leverandøren ikke har interesse i at udlevere disse til hvem som helst. Man vil derved kun kunne identificere personerne ved at hacke eller stjæle fortrolige oplysninger og sammensætte disse. Det vil derfor ud fra en rimeligheds betragtning være mest proportionalt, at man stopper ved step 3. Det vil dog altid være en konkret risikovurdering, som skal foretages, eftersom dataminimering handler om, at det er gjort tilstrækkeligt. I eksemplerne ovenfor er der tale on pseudonymisering, men for at forordningen ikke finder anvendelse, skal der altså være tale om anonymiserede data. Det er det først, når det er uigenkaldelig afidentificering af persondata, som sikrer, at en registreret ikke længere kan identificeres ved hjælp af de pågældende data.

10. Konklusion

Eftersom denne afhandling benytter sig af den retsdogmatiske metode, beskriver afhandlingen gældende ret og kommer ikke med et endegyldigt svar. Der vil derfor altid være tale om konkrete vurderinger i forhold til alle afgørelserne, da de kan påklages til domstolene for et endeligt facit.

Forvaltningen skal tage stilling til, om den er omfattet af reglerne i databeskyttelsesforordningen, dvs. at den behandler personoplysninger. Herefter skal den sikre, at den har hjemmel i henhold til behandlingsbetingelserne. Dernæst skal den altid følge principperne i artikel 5. Den skal endvidere tage stilling til de registreredes rettigheder. Slutteligt skal den tage stilling for rammerne for behandlingen, da den dataansvarlige nu skal kunne "*påvise*" at man overholder principper i artikel 5, hvor det tidligere var nok at "*sikre*" overholdes.

Afhandlingen har kigget på, hvilke muligheder den registrerede har for at foretage indsigt, partsindsigt og aktindsigt. Afhandlingen er kommet frem til, at forvaltningen skal give indsigt efter de regler, der er bedst for den registrerede, da den skal overholde sin vejledningspligt, jf. forvaltningslovens § 7, stk. 1. Der er udledt fire situationer; 1) den registrerede ønsker at få oplysninger omkring sig selv, men er ikke part i nogen sager. 2) Den registrerede ønsker indsigt i egne oplysninger og er samtidig part i en afgørelse. 3) Den registrerede søger indsigt i oplysninger om andre personer eller oplysninger, som ikke er personoplysninger, og den registrerede er ikke part i en afgørelsessag. 4) Den registrerede ønsker indsigt i oplysninger om andre eller sig selv, som ikke er personoplysninger, men er part i en afgørelsessag, hvori oplysningerne indgår. Det må konkluderes, at hvis den registrerede ønsker at anvende reglerne om berigtigelse, sletning, begrænsning eller indsigelse, så skal der være tale om personoplysninger, der er omfattet af databeskyttelsesforordningen.

Når der snakkes om berigtigelse, sletning og begrænsning, udledes der, at med databeskyttelsesforordningen er der sket en ændring i retstilstanden fra tidligere praksis. Der er nu lagt op til, at den registrerede selv kan vælge korrigeringsmetode, der skal benyttes, hvor det tidligere var den dataansvarlige, som frit kunne vælge.

Vurderingen i forhold til, om der skal ske sletning indenfor forvaltningsretten, er en svær størrelse, idet principper som notatpligt og journaliseringspligt næsten umuliggør sletning, da forvaltningen skal gemme oplysningerne for at dokumentere, sagens forløb er behandlet sagligt og objektivt.

Det må konkluderes, at reglen om sletning efter databeskyttelses forordningens artikel 17, generelt er meget snæver, da den offentlige myndighed har hjemmel i artikel 17, stk. 3, litra b, til ikke at slette oplysninger som indgår i offentlig myndighedsudøvelse og særligt skal overholde notat- og journaliseringspligten. Det må derfor antages at denne bestemmelse er til pynt, når det kommer til den offentlige myndighedsudøvelse. Forvaltningsmyndigheder vil derfor benytte sig af arkivering, som er et alternativ til sletning, da de herved "opfylder" databeskyttelsesforordningen og bibeholder deres notat – og journaliseringspligt.

Når der tales om dataminimering for private virksomheder, må det konkluderes, at de skal slette data, når der ikke længere er et formål med behandlingen. Samme udgangspunkt gælder umiddelbart ikke for forvaltningen, da de har ret og pligt til fortsat at behandle personoplysninger som følge af notat- og journaliseringspligten. Forvaltningen skal begrænse videregivelse/deling samt sikre, at indsamlingen af personoplysninger begrænser sig til det data, som er tilstrækkeligt, relevant og nødvendigt for databehandlingen. Den dataansvarlige ved forvaltningen skal udvikle og dokumentere procedurer for opfyldelse af de grundlæggende principper, herunder sletningsfrister og følge op på, at der er sket sletning som forventet.

Det må konkluderes, at der skal ske dataminimering for at undgå en ophobning af data. Dette kan ske efter forskellige principper. Hvad enten forvaltningen vil benytte sig af sletning, anonymisering eller arkivering, er sagen irrelevant, så længe de overholder behandlingsreglerne i databeskyttelsesforordningen.

Benyttes der anonymisering skal personoplysningerne være uigenkaldelige, da den dataansvarlige skal forhindre identificering af den registrerede. Databeskyttelsesforordningen finder herved ikke længere anvendelse. Mange benytter sig dog af forskellige teknikker til at sikre anonymisering. I denne afhandling er et fiktivt eksempel benyttet, som beskriver pseudonymisering. Dette er blot en "sikkerhedsforanstaltning" og ikke anonymisering. "Nøglen" skal altså slettes, så data ikke kan genskabes før der er tale om anonymisering. Det er afhandlingens vurdering, at der ud fra en rimelighedsvurdering af sikkerhedsforanstaltningen kan være sket tilstrækkelig pseudonymisering efter nuværende teknikker ved step 3, men i fremtiden, kan det være at den dataansvarlige skal videre til step 4 eller 5, afhængigt af udviklingen i samfundets informationsteknologi.

11. Litteraturliste

11.1 Bøger

- Blume, Peter "*Retssystemet og juridisk metode",* 3. udgave, 2016. Jurist- og Økonomforbundets Forlag.
- Blume, Peter "*Databeskyttelsesret*" 5. udgave, 2018. Jurist- og Økonomforbundets Forlag.
- Blume, Peter "*Den nye persondataret – Forordning 2016/6798 om persondatabeskyttelse*" 1. udgave, 2016. Jurist- og Økonomforbundets Forlag. Side. 56-79
- Bønsing, Sten "*Almindelig forvaltningsret*", 4. udgave, 2018. Djøf Forlag
- Bønsing, Sten "*Forvaltningsret – Lærebog for statskundskab*" 2. udgave, 2018. Jurist- og Økonomforbundets Forlag
- Evald, Jens "*Retskilderne og den juridiske metode"*, 2. udgave, 2010. Jurist- og Økonomforbundets Forlag
- Mortensen, Bent Ole Gram "*Dansk persondataret*", 1. udgave, 2020. FairPublishing.
- Munk-Hansen, Carsten "*Retsvidenskabsteori*", Udgave 2, 2018. Djøf Forlag
- Nielsen, Kristian Korfits og Anders Lotterup "*Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer*", 1. udgave, 2020. Jurist- og Økonomforbundets forlag. Side 231-341 og 462-572.

11.2 Afgørelser

- Dt.s j. nr. 2005-212-0299 - Tivoli sagen
- Dt.s j. nr. 2006-313-0376 - Amtskommune og kommune behandling af subjektive oplysninger
- Dt.s j. nr. 2010-215-0469 - Google Street View Wifi-sagen
- Dt.s j. nr. 2011-632-0103 - Myndighed levede ikke op til krav om sikkerhedsforanstaltninger
- Dt.s j. nr. 2017-769-0056 - Justitsministeriets udtalelse til Datatilsynet om slettemuligheder
- Dt.s j. nr. 2018-31-0070 - TDC A/S sagen
- Dt.s j. nr. 2018-32-0065 - Statsadvokatens videregivelse af oplysninger uden hjemmel i lov
- Dt.s j. nr. 2018-32-0286 - Klage over manglende sletning

- Dt.s j. nr. 2018-41-0015 - Ilva A/S i dømt bøde for manglende slettefrister
- Dt.s j. nr. 2018-41-0016 - Tilsyn med Taxa 4x35's behandling af personoplysninger
- Dt.s j. nr. 2019-431-0052 - Offentliggørelse af billeder på virksomheds Facebook-side
- FOB 2003.699 - Advarsel for videregivelse af anonymiserede oplysninger til fagforening og indhentelse af oplysninger fra register
- Rt.s. j.nr. 1997-1413-023 - Telefirma intern videregivelse
- KEN nr. 9961 -22/12/2003 Indenrigsministeriet j. nr. 300007803 - Ankestyrelsens principafgørelse F-2-03 om bil - sletning af oplysninger – alkoholmisbrug – dokumentationshensyn – berigtigelse – notatpligt - konkret vurdering

11.3 Domme

- C-398/15 - Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce
- ILVA A/S dommen - afsagt den 12. februar 2021 Rettens nr. 13-3662/2020

11.4 Videnskabelige artikler og projekter

- Knudsen, Patrick Lykke & Pernille Ask Korsgaard "*AI kontra databeskyttelse - Konsekvenserne af persondataforordning 2016/679 for kunstig intelligens*", 2018
- Sevelsted, Maria N. & Nanna Buus Nielsen "*Det retlige sammenspil mellem databeskyttelsesretten og AI*", 2020
- *Artikel 29-gruppen vedrørende databeskyttelse - Udtalelse nr. 05/2014 om anonymiseringsteknikker - 0829/14/DA WP216*
- Valentiner-Branth, Anders, Rasmus Blaabjerg med flere. *"Samspillet mellem forvaltningsretten og databeskyttelsesretten", 2020*

11.5 Internetkilder

- Allerøds DPO, "*GDPR og informationssikkerhed i Allerød Kommune*", 2020 https://www.alleroed.dk/document/2724873e-7e20-47a4-97dc-c97e59643da7 (Sidst tilgået 18.05-2021)
- Datatilsynet vejledning om, "Lovgivning" https://www.datatilsynet.dk/databeskyttelse/lovgivning (Sidst tilgået 18.05-2021)
- Datatilsynets vejledning om, "*Databeskyttelsesrådet (EDPB)"*

https://www.datatilsynet.dk/internationalt/databeskyttelsesraadet-edpb/ (Sidst tilgået 18.05-2021)

- Datatilsynet, ”vejledninger” https://www.datatilsynet.dk/databeskyttelse/vejledninger (Sidst tilgået 18.05-2021)
- Datatilsynets vejledning om, ”*Hvad er personoplysninger*” https://www.datatilsynet.dk/databeskyttelse/hvad-er-personoplysninger (Sidst tilgået 18.05-2021)
- Datatilsynets vejledning om, ”*Sletning*” https://www.datatilsynet.dk/emner/persondatasikkerhed/sletning (Sidst tilgået 18.05-2021)
- Folketingets Ombudsmands vejledning om, ” *Officialprincippet*” https://www.ombudsmanden.dk/myndighedsguiden/generel_forvaltningsret/officialprincippet/ (Sidst tilgået 18.05-2021)
- Grønborg, Jørgen U. ”*Persondataforordningens præambel*” https://themis.dk/synopsis/docs/Lovsamling/Persondatapersondataforordningens_praeambel.html (Sidst tilgået 18.05-2021)
- Justitsministeriet.dk ”*Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565”*
- Laursen, Hanne Biehl ”*Delt dataansvar*” https://gdprguide.arkivo.dk/vaelg-emne/ansvar-roller/faelles-ansvar (Sidst tilgået 18.05-2021)
- https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/betaenkning_1565_del_i_bind_1.pdf (Sidst tilgået 18.05-2021)
- Nielsen, Aske og Sørensen Rasmus. ”GDPR.dk” https://gdpr.dk/databeskyttelsesforordningen/kapitel-8-retsmidler-ansvar-og-sanktioner/artikel-83-generelle-betingelser-for-paalaeggelse-af-administrative-boeder/ (Sidst tilgået 18.05-2021)
- Mortensen, Henning ” *GDPR: Hvorfor er privacy vigtigt?*”, 2019 https://wiredrelations.com/gdpr-hvorfor-er-privacy-vigtigt/ (Sidst tilgået 18.05-2021)
- Rigsarkivet ”*Kort og godt om aflevering af it-systemer*” https://www.sa.dk/wp-content/uploads/2015/10/Kort-og-godt-om-aflevering-af-it-KOMMUNE2.pdf (Sidst tilgået 18.05-2021)