Persondataret

Biometriske datas anvendelse ved tv-overvågning i et persondataretligt perspektiv

Af Sawmika Gengatharan
Juridisk Institut
Aalborg Universitet
2018

Fag:	Persondataret
Emne:	Biometriske datas anvendelse ved tv-overvågning i et persondataretligt perspektiv
Engelsk titel:	Biometrical data used in accordance with CCTV in a privacy perspective
Projektart:	Specialeafhandling
Uddannelsessted:	Aalborg Universitet – Juridisk Institut
Uddannelse:	Jura
Vejleder:	Charlotte Bagger Tranberg
Afleveringsdato:	5. december 2018
Sidetal:	70
Normalsider:	59,65
Anslag:	143.167
Afhandling af:	Sawmika Gengatharan
Studienummer:	20123922

Forsidebillede:https://www.google.dk/search?biw=1432&bih=699&tbm=isch&sa=1&ei=_98BXI2EA4fawQKn3pPwDA&q=biometri+GDPR&oq=biometri+GDPR&gs_l=img.3...26612.39962..40101...6.0..2.420.3029.9j4j4j1j1.....0....1..gws-wiz-img.....0j0i24j0i30j0i5i30.EeieDe6UUiA#imgrc=xlRGx9PrC9RZrM:

Indholdsfortegnelse

Abstract

This thesis will examine the challenges of biometrical data used in accordance with CCTV in a privacy perspective. The General Data Protection Regulation (GDPR) is applicable with effect from 25th of May 2018. The biometrical data is seen as sensitive personal data when used for purpose of unique identification and should be prohibited as a baseline. CCTV is regulated in The Danish CCTV Law "tv-overvågningsloven".

To investigate the challenges of using biometrical data in accordance with CCTV in a privacy perspective, the problem statement and the supplementary questions are answered through the case "TechX" and the relevant regulations from GDPR and The Danish CCTV Law. The case is based on a start-up business whose aim is to prevent theft in shops through biometrical CCTV and facial recognition.

The analysis will focus on who the Controller is and whether the rules in GDPR are complied. TechX can only utilize the technology if there is a legal basis in; GDPR Article 9 to process biometrical data, Article 10 to process personal data regarding criminal convictions and offences, and finally The Danish CCTV Law §§ 2 and 4c in regards to CCTV. Furthermore the general principles in GDPR Article 5 must be complied; the Controller must fulfill the Rights of the data subject and the processing of the data must be transparent.

The analysis concludes that TechX and the shops do not have a legal basis to process the biometrical data, other than if they are able to get consent from the data subject. A person would not give their consent before committing theft in the shop. It is estimated, that based on the disproportional time it takes to read the privacy policy and to scan the face in accordance to make a template for facial recognition, it is not possible to get consent from the customers. Furthermore it is not a well-known technology in Denmark why most people may not give their consent to such radical methods. The regular CCTV records can be processed, as the legal basis is to be found in The Danish CCTV Law §§ 2(1), no. 3 and 4c. The personal data about criminal convictions and offences cannot be processed with legal basis in GDPR. It somehow has a legal basis in The Danish CCTV Law as a private business, in some circumstances, can process and transmit CCTV records in a crime preventive perspective.

The processing of the biometrical data is not estimated to be proportional as the regular CCTV can fulfill the purpose as well.

Kapitel 1 - Introduktion

1.1 Indledning

En verden hvor vi som mennesker er underlagt en konstant overvågning, lyder som et afsnit af Big Brother eller andre populære reality serier. Med nutidens reality programmer såsom Big Brother, Paradise Hotel osv., er konstant overvågning noget som mange frivilligt vælger. Man kan gang på gang forundres over, at mennesker frivilligt vil vælge dette. I Danmark er det dog stadig et frivilligt valg at underlægge sig sådanne retningslinjer og overvågning. Det er dog ikke alle, der er så privilegerede, at de frivilligt kan til- og fravælge sådan konstant overvågning. Den kinesiske regering forventer at indføre totalovervågning med ansigtsgenkendelse og pointsystemer inden udgangen af 2020. Hver eneste borger vil blive rated ud fra, hver handling denne foretager sig. Hvordan er situationen i Danmark og er det en tendens der kan opstå her?

I takt med den teknologiske udviklings indpas i vores samfund følger store risici. Teknisk udstyr vi benytter til daglig som telefoner og computere, er blot nogle af de enheder, der gemmer på vigtige personoplysninger om os. Apples nye modeller af iPhone og MacBook benytter henholdsvis ansigtsgenkendelse og fingeraftryk til at give brugeren adgang til enheden, hvor der tidligere blev benyttet en personlig kode. Vores fingeraftryk og ansigtets biometri er lagret i vores mobile enheder og er dermed i stor risiko for at ende i de forkerte hænder. Den 25. maj 2018 fik databeskyttelsesforordningen[4] (fremover refereret som forordningen eller GDPR) også kendt som GDPR (General Data Protection Regulation) virkning. I et samfund med stigende anvendelse og lagring af data er det en nødvendighed at fastlægge klare retningslinjer for beskyttelse af persondata.

Med ikrafttrædelsen af GDPR er en af de væsentlige ændringer at biometriske data med henblik på identifikation, som tidligere blev anset for en almindelig oplysning, er kategoriseret under

[4] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF

særlige kategorier af personoplysninger (fremover refereret som følsom oplysning). Denne ændring vil sandsynligvis medføre en ændret praksis, og det vil i større grad være svært for virksomheder at behandle biometriske data sammenlignet med tidligere. Den teknologiske udvikling medfører en hel del nye og spændende teknologier og muligheder, som kan lette arbejdsbyrden på mange områder, men hvorvidt dette er i overensstemmelse med databeskyttelsesforordningen, må tiden vise.

1.2 Problemformulering

Den nye databeskyttelsesforordning medfører nogle ændrede regler for biometriske data, idet disse nu bliver anset for følsomme oplysninger ved identifikation. Tv-overvågningsloven[5] regulerer almindelig tv-overvågning, hvoraf det fremgår, at private virksomheder kan installere tv-overvågning under nogle nærmere fastsatte regler. Problematikken opstår i det tilfælde, hvor biometriske data anvendes sammen med almindelig tv-overvågning til at overvåge personer. Det er en udvikling, der kan resultere i en ændret tankegang omkring følsomme data på sigt og i værste fald medføre tilstande lignende Kina. Der er endnu intet praksis på området, hvorfor denne afhandling vil undersøge problemstillingen nærmere.

For at undersøge denne problemstilling nærmere, vil følgende problemformulering forsøges besvaret:

Hvad er de persondataretlige udfordringer ved anvendelse af biometri ved tv-overvågning i forhold til databeskyttelsesforordningen?

Til hjælp for besvarelsen af problemformuleringen, vil følgende underspørgsmål blive besvaret i analysen:

- *Hvilke retsgrundlag er relevante i forhold til behandling af biometriske data og tv-overvågning i henholdsvis databeskyttelsesforordningen og tv-overvågningsloven?*
- *Hvilke udfordringer opstår der, idet biometriske data ikke er omfattet af tv-overvågningsloven?*

[5] Lovbekendtgørelse nr. 1190 af 11. oktober 2007 om tv-overvågning

- *Hvilke persondataretlige udfordringer kan der være, når en privat virksomhed ønsker at anvende biometrisk overvågning?*
- *Har kategoriændringen for biometriske data en indflydelse på fremadrettet praksis?*
- *Hvilke udfordringer kan der være i forhold til indhentelse af et eventuelt samtykke fra den registrerede?*
- *Er det i overensstemmelse med proportionalitetsprincippet at anvende biometrisk overvågning?*

1.3 Afgrænsning

Denne afhandling vil fokusere på at behandle de dele af teorien, der omhandler den ovennævnte problemstilling. Der vil derfor primært være fokus på tv-overvågningsloven og databeskyttelsesforordningen.

Der vil alene være grundlag for at nævne de for analysen relevante bestemmelser, der er i tv-overvågningsloven, som tidligere var kapitel 6a i persondataloven[6].[7] Her fremgår blandt andet bestemmelser om behandling ved kriminalitetsforebyggende øjemed og erhvervsdrivendes mulighed for deling af personoplysninger om gerningspersoner eller formodede gerningspersoner.

Casen, der danner baggrund for analysen, omhandler anvendelse af ansigtsgenkendelse ved overvågning i forretninger for at forebygge tyveri fra tidligere gerningspersoner. I forhold til GDPR behandles der følsomme oplysninger og oplysninger om straffedomme og lovovertrædelser. Teorien bag dette vil alene blive behandlet nærmere i det omfang det findes nødvendigt i forhold til analysen, idet det ellers vil blive for omfattende og irrelevant. I forhold til forordningens artikel 9 om behandlingshjemmel for følsomme oplysninger vil det blive vurderet, hvorvidt TechX har hjemmel til behandling af biometriske oplysninger, og i givet fald, hvilken hjemmel disse oplysninger kan blive behandlet på baggrund af. Det er ikke alle betingelser i artikel 9, stk. 2, litra a-j, der er relevante for nærværende case, hvorfor det kun er de relevante bestemmelser, der vil blive behandlet. I analysen vil TechX og forretningerne blive nævnt sammen som fælles

[6] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer
[7] Lovforslag nr. 205, indledning, side 3

dataansvarlige, men det vil alene være TechX, der nævnes ved behandlingen, der sker fra den centrale database.

De almindelige overvågningsoptagelser reguleres af tv-overvågningsloven og idet casen omhandler en privat virksomhed, vil det alene være de relevante bestemmelser herfor, der medtages i afhandlingen. Få relevante bestemmelser i forordningens artikel 6 om lovlig behandling, vil blive gennemgået, idet der ved behandling af overvågningsoptagelser vil blive behandlet oplysninger om lovovertrædelser, som behandles efter reglerne for almindelige oplysninger. Disse bestemmelser vil dog ikke blive vurderet nærmere i analyseafsnitte, idet der allerede er hjemmel til behandling i tv-overvågningsloven, og det centrale for afhandlingen er de biometriske data.

Der gøres derudover opmærksom på, at verifikation i forhold til biometriske data alene vil berørt overfladisk, idet der i casen fokuseres på identifikation ved biometriske data.

Oplysninger og personoplysninger anvendes synonymt i afhandlingen.

1.4 Metode

Der anvendes i denne afhandling retsdogmatisk metode til at besvare problemstillingen, herunder til at analysere casen ved hjælp af denne metode. Den retsdogmatiske metode klarlægger gældende ret ved at systematisere, beskrive, fortolke og analysere.[8]

GDPR og tv-overvågningsloven vil være de primære retskilder, der bliver anvendt i afhandlingen, dog er den historiske persondatalovs principper stadig gældende i de fleste tilfælde, hvorfor der eksempelvis tages udgangspunkt i denne lovs definition og de forskellige begreber sammenholdt med andre kilder, for eksempel afgørelser fra Datatilsynet. Forarbejder og præambelbetragtninger vil have en stor indflydelse i afhandlingen, idet dette er tankerne bag gældende ret, hvoraf det kan ses, hvilke overvejelser, der har været med til at skabe gældende ret. Derudover anvendes der fagbøger, fagtekster og en betænkning som en sekundær kilde med henblik på at inddrage flere overvejelser omkring retsområdet.[9]

[8] Munk-Hansen, 2014, side 85-98 og 189-204
[9] Rienecker, 2012, side 173-177

1.4.1 Afhandlingens opbygning

Denne specialeafhandling er opbygget i 5 kapitler, der skal give et struktureret overblik over afhandlingen.

Kapitel 1 er en introduktion til afhandlingen. Afsnit 1.1 er en kort introduktion til emnet "biometriske datas anvendelse i tv-overvågning", hvorfor dette emne er relevant, og hvilken betydning det har i samfundet. Afsnit 1.2 er problemformuleringen, som vil danne grundlag for hele afhandlingen. Afsnit 1.3 er en afgrænsning af afhandlingen, hvor der både vil være en positiv og negativ afgrænsning, hvorunder afgrænsningen begrundes. Afsnit 1.4 er metodeafsnittet, som vil beskrive, hvilke metoder og retskilder der er anvendt, og hvilke kildetyper de anvendte kilder hører under.

Kapitel 2 er en nærmere beskrivelse af databeskyttelsesforordningen, hvor relevante begreber for afhandlingen vil blive gennemgået nærmere. De udvalgte persondataretlige principper og bestemmelser er valgt med udgangspunkt i casen i analyseafsnittet.

Kapitel 3 indeholder en nærmere gennemgang af tv-overvågning, tv-overvågningsloven, biometriske data og anvendelse af biometriske data ved tv-overvågning. Det er alene de for casen relevante bestemmelser i tv-overvågningsloven, som gennemgås. Fokus vil særligt være på §§ 1, 2, 3, 4c og 4e.

Kapitel 4 er det analyserende afsnit. Her vil der være en kort introduktion til casen, TechX, afhandlingen er bygget på, hvorunder fakta beskrives. Den teori, der er beskrevet i henholdsvis kapitel 2 og 3, vil blive anvendt på casen, hvorved jus anvendes på fakta i en analyse af problemstillingen. De analyserede persondataretlige principper og bestemmelser er valgt med udgangspunkt i casen, hvorfor det kun er de relevante begreber, der undersøges nærmere. Der vil blive forsøgt at finde en løsning på TechX's udfordringer i forhold til databeskyttelsesforordningen. Derudover vil analysen føre til en vurdering af, hvorvidt TechX lovligt kan anvende deres produkt og tilbyde en dertilhørende serviceydelse. Til hvert af de behandlede punkter i analysen, vil der være en delkonklusion.

Kapitel 5 er det afsluttende kapitel, hvor konklusionen og perspektiveringen fremgår. Afhandlingens teori og analyse vil blive opsummeret, hvorefter der vil være en konklusion til

problemformuleringen. Der vil derudover i perspektiveringen fremgå nogle relevante problemstillinger, som er relevante for afhandlingen.

Kapitel 2 – Databeskyttelsesforordningen

2.1 Databeskyttelsesforordning

Den 25. maj 2018 fik databeskyttelsesforordningen virkning.[10] Forordningen ophæver det hidtil gældende databeskyttelsesdirektiv [11] , som har reguleret de EU-retlige regler, mens persondataloven har reguleret national ret i Danmark.[12] Forskellen på et direktiv og en forordning er, at et direktiv ikke har direkte virkning i medlemsstaterne, mens en forordning har direkte virkning.[13] I forordningen har medlemsstaterne bemyndigelse til at supplere forordningen, således at den passer med medlemsstaternes nationale ret. En forordning har direkte virkning, og de supplerende nationale love må derfor ikke være i strid med GDPR. Danmark har indført databeskyttelsesloven, hvilket er en samlet lov for de supplerende bestemmelser, Danmark har valgt at supplere forordningen med.[14]

Forordningens anvendelsesområde er følgende: ”*Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register*”.[15]

2.2 Personoplysning

”Personoplysning” er et meget bredt begreb. Det følger af forordningens artikel 4, nr. 1:

[10] GDPR artikel 99, nr. 2
[11] Europa-Parlamentet og Rådets direktiv af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (95/46/EF)
[12] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/, afsnit: databeskyttelsesloven, d. 4/12-2018
[13] https://europa.eu/european-union/eu-law/legal-acts_da, d. 4/12-2018
[14] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/, afsnit: databeskyttelsesloven, d. 5/10-2018
[15] GDPR artikel 2

> ”*»personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); 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*”.[16]

Dette er enhver oplysning, der omhandler en person eller en oplysning, der kan føre til identifikation af en person. En personoplysning kan eksempelvis være oplysninger om en persons fysiske, psykiske, økonomiske, kulturelle eller seksuelle forhold. Dette er dog blot få eksempler på, hvilke oplysninger en personoplysning kan omfatte. Fælles for dem alle er, at det er specifikke oplysninger, der kan henføres til en given person. En anden form for personoplysning er informationer, der kan identificere en person, uden at personen umiddelbart kan genkendes direkte ud fra informationen. Dette kan eksempelvis være et medlemsnummer eller en kode. Hvis det gennem dette nummer er muligt at opnå yderligere oplysninger om en person, vil det pågældende nummer være en personoplysning. Det er dermed ikke et krav, at oplysningen skal kunne henføres direkte til en specifik person, men hvis oplysningen kan lede til andre personoplysninger om en given person, eller at to eller flere oplysninger skal kombineres med hinanden for at føre til en given person, er dette også en personoplysning.[17]

Som ovenfor nævnt anses pseudonymiserede personoplysninger for at være en identificerbar personoplysning og er reguleret af forordningen, da det er muligt at finde den registreredes identitet ved supplerende oplysninger. Krypterede oplysninger anses ligeledes for en personoplysning i de tilfælde, hvor det er muligt at gøre dem læsbare igen. Hvis oplysningerne er irreversibelt krypteret, hvilket vil sige, at de er anonymiserede på en måde, hvorpå det ikke længere er muligt at tilbageføre dem til original format, vil de ikke være omfattet af definitionen.[18] GDPR omfatter ikke oplysninger, som er anonymiserede på en måde, hvor den registrerede ikke er identificeret, identificerbar eller ikke længere identificerbar. Vurderingen udmåles ud fra en

[16] Persondatalovens § 3, nr. 1.
[17] Waaben, 2015, side 135-136
[18] Waaben, 2015, side 140-141

rimelighedsbetragtning for alle muligheder, som kan anvendes i takt med teknologiens udvikling, omkostninger og tidsforbrug.[19]

Billeder, video, stemmer, genetiske kendetegn, biometriske data som fingeraftryk[20] og lignende, kan også indeholde personoplysninger, der kan henføres til en given person. Der kan være tale om videoovervågning fra en forretning, hvor personens ansigt kan genkendes, eller måden hvorpå personen bevæger sig. Det kan være et billede, hvor tatoveringer eller modermærker er blottet. Disse kan være særegne for personer, og det kan derfor medvirke til at identificere en person.[21]

2.3 Oplysningskategorier

GDPR sondrer principielt mellem to kategorier af personoplysninger: *følsomme oplysninger* og *almindelige oplysninger*, samt en tredje kategori, som regulerer oplysninger om straffedomme og lovovertrædelser. Dette er en særlig kategori som eksempelvis angår oplysninger om lovovertrædelser, adresse til et fængsel, hvor indsatte er bosiddende eller andre oplysninger, der kan henføre til en lovovertrædelse. Behandlingshjemlen er ikke reguleret i forordningen, men i stedet i de enkelte medlemsstater.[22]

En væsentlig forskel på GDPR og persondataloven i forhold til denne afhandling er, at biometriske data tidligere kategoriseredes som en almindelig oplysning, hvor det i forordningen kategoriseres som en følsom oplysning.[23] I Datatilsynets afgørelse, journalnummer 2003-212-0143, om brug af fingeraftryk i et elektronisk rabatkort til offentlig transport på Bornholm, udtalte Datatilsynet, at fingeraftryk ifølge persondataloven ansås for at være en almindelig oplysning, idet biometriske data på daværende tidspunkt ikke var nævnt i bestemmelsen om følsomme oplysninger.

2.3.1 Almindelige oplysninger

Der er i forordningen ikke en beskrivelse af, hvilke oplysninger, der er almindelige oplysninger. Artikel 6 omhandler almindelige oplysninger, og er den bestemmelse, hvori behandlingshjemlen for almindelige oplysninger skal findes. Den indeholder ikke på samme måde som artikel 9 en

[19] GDPR, præambel, betragtning 26
[20] Datatilsynet, j.nr. 2003-212-0143
[21] Waaben, 2015, side 135-136
[22] Vejledning, Databeskyttelsesforordningen, 2017, side 8
[23] Betænkning nr. 1565 om forordningen, side 194

opremsning af, hvilke oplysninger der er almindelige. Forordningens artikel 9 om følsomme oplysninger er udtømmende, hvorfor alle andre oplysninger, som ikke er nævnt i denne artikel, som udgangspunkt kategoriseres som almindelige oplysninger.[24]. Som nævnt i afsnit 2.3 er der særlige regler for straffedomme og lovovertrædelser, hvorfor det må antages, at alle andre oplysninger end disse og følsomme oplysninger er almindelige oplysninger. Eksempler på almindelige oplysninger kan være: "*… identifikationsoplysninger som f.eks. navn og adresse, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke-følsomme oplysninger*".[25]

2.3.2 Følsomme oplysninger

Som nævnt i afsnit 2.3.1, er artikel 9 udtømmende, og det er derfor alene de oplysninger, der er nævnt i bestemmelsen, som er følsomme.

Ordlyden af forordningens artikel 9, stk. 1 lyder som følger:

> "*Behandling af personoplysninger om 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 er forbudt*".[26]

En almindelig oplysninger kan i nogle tilfælde anses for at være en følsom oplysning. Dette sker i tilfælde, hvor oplysningen i en given kontekst omdannes til en følsom oplysning. Det er dermed væsentligt at vurdere, hvorvidt en almindelig oplysning kan anses for at være følsom, ud fra den kontekst oplysningen er registreret i. Peter Blume giver et eksempel i sin bog om, at et navn på en person der er registreret ved en bestemt afdeling på et sygehus, kan anses for at være en følsom oplysning, idet dette kan henføres til helbredsoplysninger, som er følsomme oplysninger.[27]

2.3.3 Oplysninger om straffedomme og lovovertrædelser

Forordningens artikel 10 vedrører oplysninger om straffedomme og lovovertrædelser:

[24] Vejledning, Databeskyttelsesforordningen, 2017, side 8
[25] Vejledning, Databeskyttelsesforordningen, 2017, side 8
[26] GDPR artikel 9, stk. 1
[27] Blume, 2016, side 82

> ”*Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af artikel 6, stk. 1, må kun foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder. Ethvert omfattende register over straffedomme må kun føres under kontrol af en offentlig myndighed*”.[28]

Ifølge bestemmelsen er det som udgangspunkt kun offentlige myndigheder eller andre, der behandler under kontrol af en offentlig myndighed, der må foretage behandling efter denne bestemmelse. Hvis privatpersoner skal behandle oplysninger efter denne bestemmelse, skal det være under kontrol af en offentlig myndighed eller fremgå af EU-retten eller medlemsstaternes nationale ret, hvoraf det følger, at der skal stilles nogle sikkerhedsgarantier for registreredes rettigheder.[29] Det fremgår af tv-overvågningsloven, at der under særlige forudsætninger, i kriminalitetsforebyggende øjemed må behandles og videregives oplysninger. Dette er eksempelvis i tilfælde af tyveri og røveri. Overvågningsmateriale må behandles, herunder videregives, hvis det er i kriminalitetsforebyggende øjemed.[30] Heraf må det antages, at også oplysninger om lovovertrædelser behandles, idet optagelserne videregives med henblik på advarsel af andre relevante parter.

Oplysninger om straffedomme og lovovertrædelser behandles efter reglerne i forordningens artikel 6, stk. 1, såfremt der er behandlingshjemmel.[31]

2.4 Behandling

Behandling af personoplysninger er ifølge forordningen et vidt begreb, hvorfor enhver håndtering af oplysninger som udgangspunkt er behandling. Definitionen er i artikel 4, nr. 2 anført således:

> “*»behandling«: enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af*

[28] GDPR artikel 10
[29] Betænkning nr. 1565 om forordningen, side 233
[30] Tv-overvågningslovens § 2, nr. 3 og § 4c
[31] Betænkning nr. 1565 om forordningen, side 244

personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse".[32]

Det er i artikel 4, nr. 2 anført, at sletning og tilintetgørelse er behandling. Dette kan umiddelbart forstås som ikke at være en behandling, idet de fjernes fra databasen. Den registrerede kan have en interesse i, at de pågældende oplysninger bevares, hvorfor det er medtaget som behandling. Den registrerede kan eksempelvis i tilfælde af en erstatningssag mod den dataansvarlige, have en interesse i at oplysningerne ikke slettes. Ud fra dette må det antages, at enhver berøring af personoplysninger antages for at være behandling.[33]

Behandling foretaget af fysiske personer af rent privat karakter, er ikke omfattet af reglerne i forordningen. Dette gælder både almindelige og følsomme oplysninger som udveksles mellem to private personer.[34]

Politi, anklagemyndighed og andre myndigheder, der retsforfølger eller efterforsker strafbare forhold er ligeledes ikke omfattet af bestemmelserne i forordningen.[35] Der er særlige regler på dette område, da det er nødvendigt at behandle almindelige oplysninger, følsomme oplysninger og oplysninger om strafbare forhold under andre forudsætninger.

2.5 Dataansvarlig

Forordningen skelner mellem dataansvarlig og databehandler. Baggrunden herfor er de væsentlige forskelle i de krav, der stilles til henholdsvis den dataansvarlige og databehandleren. Såfremt der er tvivl om, hvem der er dataansvarlig og databehandler, vil det føre til en forringet beskyttelse af

[32] GDPR artikel 4, nr. 2

[33] Blume, 2016, side 59

[34] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvornaar-behandler-du-personoplysninger/, afsnit: Behandlinger – undtaget fra databeskyttelsesreglerne, d. 21/11-2018

[35] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvornaar-behandler-du-personoplysninger/, afsnit: Behandlinger – undtaget fra databeskyttelsesreglerne, d. 21/11-2018

den registrerede, da denne kan have svært ved at rette henvendelse til den dataansvarlige, for at kunne gøre krav på sine rettigheder.[36] Nærmere herom i afsnit 2.12.

Den dataansvarlige er i forordningens artikel 4, nr. 7 defineret som:

> "*… 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*".[37]

Den dataansvarlige behøver derfor ikke nødvendigvis, at være en fysisk person. Den dataansvarlige er den, der *bestemmer*, hvilket formål oplysningerne må behandles ud fra, hvordan de må behandles, og hvem der må behandle dem. Det overordnede ansvar for oplysningerne er dermed placeret hos den dataansvarlige, hvorfor det også er dennes ansvar, at behandlingen af oplysningerne sker på forsvarlig vis og i overensstemmelse med forordningen.[38]

> "*Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres*".[39]

Dette kan blandt andet opnås ved, at den dataansvarlige sikrer sig, at der er behandlingshjemmel til behandling af oplysninger om de registrerede, som kræver, at mindst ét af de i forordningens artikel 6 oplistede punkter opfyldes jf. forordningens artikel 6.[40] Et andet krav til den dataansvarlige er, at denne skal være i stand til at efterkomme de i forordningens kapitel 3 oplistede rettigheder, der tilkommer den registrerede. Den registrerede skal for eksempel oplyses

[36] Vejledning om dataansvarlige og databehandlere, side 4-5
[37] GDPR artikel 4, nr. 7
[38] Vejledning om dataansvarlige og databehandlere, side 5-6
[39] GDPR artikel 24, stk. 1
[40] Vejledning om dataansvarlige og databehandlere, side 5-6

om, at der indsamles oplysninger om denne, og til hvilket formål disse vil blive benyttet. Derudover har registrerede ret til at få slettet eller berigtiget oplysninger hos den dataansvarlige. Dette er blot nogle af de rettigheder, den registrerede besidder. Nærmere om dette i afsnit 2.12.

Såfremt der sker brud på persondatasikkerheden, er det den dataansvarliges ansvar at indberette dette til Datatilsynet uden unødig forsinkelse, og senest 72 timer fra at denne er blevet bekendt med bruddet.[41] Af forordningens artikel 33 følger en række krav til omfanget af oplysningerne, som skal indberettes til Datatilsynet.

Den dataansvarlige skal overfor interne og eksterne interessenter kunne dokumentere, at de udførte tekniske og organisatoriske foranstaltninger medfører tilstrækkelig beskyttelse af de registrerede persondata og dermed er i overensstemmelse med forordningen. Hvis Datatilsynet aflægger besøg for at undersøge sikkerheden hos dataansvarlige, skal denne påvise sikkerheden overfor Datatilsynet eller anden tilsynsmyndighed. Der skal derudover løbende føres kontrol med, at disse foranstaltninger fortsat lever op til forordningens beskyttelsesstandard.[42]

2.6 Databehandler

Databehandleren er ifølge GDPR artikel 4, nr. 8 defineret som: "… *en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne*"[43]

Som beskrevet i afsnit 2.5 bestemmer den dataansvarlige behandlingsformålet, behandlingsformen og hvem, der må behandle oplysningerne. Databehandleren er derimod den, der *behandler* oplysningerne på vegne af den dataansvarlige. Det er derfor den dataansvarlige, der har ansvaret for, at databehandlere behandler oplysningerne i overensstemmelse med GDPR.[44]

> "*Hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en*

[41] GDPR artikel 33
[42] Betænkning nr. 1565 om forordningen, side 408-409
[43] GDPR artikel 4, nr. 8
[44] Vejledning om dataansvarlige og databehandlere, side 5-6

sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder".[45]

Databehandleren skal i medfør af forordningens krav sørge for at stille de fornødne garantier, hvis der overleveres oplysninger, som skal behandles på vegne af den dataansvarlige. Der er i forordningen krav om, at der skal forekomme en bindende aftale mellem databehandler og dataansvarlige for at sikre, at databehandleren ikke handler i strid med forordningen og instruktionen fra den dataansvarlige og dermed udsætter den registrerede for ringere persondatasikkerhed. [46] Derudover må databehandleren ikke benytte sig af en anden databehandler, medmindre dette er godkendt af den dataansvarlige.[47] Databehandleren handler indenfor instruktioner fra den dataansvarlige og skal efterleve forordningens krav på vegne af den dataansvarlige, som har overdraget personoplysningerne.

2.7 Fælles dataansvar

Der skal som udgangspunkt være en klar afgrænsning af, hvem der er dataansvarlig, og hvem der er databehandler. Der kan dog i nogle tilfælde være tvivl om, hvilken part der har hvilken rolle. EU-domstolen fastslog i sagen C-210/16 fra 5. juni 2018 om Facebook og fansider, at der kan forelægge et fælles dataansvar[48], hvilket betyder, at der kan være to eller flere dataansvarlige. I det tilfælde, hvor der er fælles dataansvar, er det essentielt, at ansvarsområderne er klart og gennemsigtigt afgrænset. Grunden til at denne afgrænsning er vigtig, er for at sikre den registreredes rettigheder, og for at Datatilsynet kan føre kontrol med om virksomheden, organet, foreningen m.m. er compliant med databeskyttelsesforordningen. [49] De dataansvarlige skal fastlægge de ansvarsområder, de hver især har, medmindre det allerede fremgår af EU-retten eller medlemsstaternes nationale ret. Det kan derudover fastlægges, hvem af de dataansvarlige der skal agere kontaktperson, når de registrerede ønsker at gøre brug af deres rettigheder.[50]

[45] GDPR artikel 28, stk. 1
[46] GDPR artikel 28, stk. 3
[47] GDPR artikel 28, stk. 2
[48] Sag, C-210/16
[49] GDPR præambelbetragtning 79
[50] Betænkning nr. 1565 om forordningen, side 425

2.8 Grundlæggende behandlingsprincipper

2.8.1 Lovlighed, rimelighed og gennemsigtighed[51]

De grundlæggende betingelser ved behandling af personoplysninger er beskrevet i forordningens artikel 5. Her står det beskrevet, at personoplysninger skal: "… *behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)*".[52]

Denne bestemmelse stammer fra princippet om god databehandlerskik, jf. persondatalovens § 5. Gennemsigtighed er dog en tilføjelse i forordningen, som ikke stod i persondatalovens § 5. Der findes ikke en præcis beskrivelse af, hvad god databehandlingskik er, udover at behandlingen skal være lovlig og rimelig.[53]

I ordet *lovlighed* ligger, at mindst ét af de i artikel 6, stk. 1 oplistede krav, skal opfyldes for almindelige personoplysninger, mens mindst ét af artikel 9, stk. 2's krav skal opfyldes for følsomme oplysninger. Hvis ikke mindst ét af de oplistede behandlingsgrundlag er tilstede, kan hjemlen eventuelt findes i anden lovgivning. Såfremt mindst ét af kravene i forordningen eller anden lovgivning er opfyldt, er der et lovligt behandlingsgrundlag for behandling af personoplysninger. Hvis dette ikke er tilfældet må personoplysningerne ikke behandles.[54]

For oplysninger om straffedomme og lovovertrædelser gælder det, at det som udgangspunkt ikke er lovligt at behandle for private, medmindre det fremgår af EU-retten eller national ret.[55] I Danmark kan private virksomheder behandles og videregives oplysninger i kriminalitetsforebyggende øjemed jf. tv-overvågningslovens § 2, nr. 3 og 4c, hvilket må anses for oplysninger om lovovertrædelser, idet gerningspersoner, der har begået tyveri eller røveri, vil fremgå af optagelserne.

[51] GDPR artikel 5, stk. 1, litra a
[52] GDPR artikel 5, stk. 1, litra a
[53] Betænkning nr. 1565 om forordningen, side 92
[54] Betænkning nr. 1565 om forordningen, side 92
[55] GDPR, artikel 10

Rimelighed er ikke en målestok. Det er en konkret vurdering i de enkelte tilfælde, hvorvidt behandlingen er rimelig. Denne vurdering kan tages af Datatilsynet ud fra en betragtning af *god databehandlingsskik*.[56]

Gennemsigtighed skal sikre, at den registrerede på en lettilgængelig og letforståelig måde skal kunne modtage enhver kommunikation og information vedrørende de registrerede personoplysninger. Derudover skal der benyttes et klart og enkelt sprog, så den registrerede er i stand til at forstå, hvad dette indebærer.[57] De pågældende informationer kan vedrøre den registreredes rettigheder, formålet for indsamlingen af oplysningerne, informationer om den dataansvarlige, herunder kontaktoplysninger m.m., informationer om databehandleren, risici, varighed af opbevaringen af oplysningerne og lignende. Nogle af disse punkter er nærmere uddybet under afsnit 2.12 om registreredes rettigheder.[58]

Gennemsigtighed indebærer også, at de opbevarerede data ikke lagres længere tid en nødvendigt. Hvis oplysningerne ikke længere er relevante, skal de slettes. Det er altså ikke en acceptabel grund, at oplysningerne muligvis kan blive relevante på et senere tidspunkt. Den dataansvarlige skal derfor indføre slettefrister eller anden form for kontrol, for at sikre sig at oplysninger ikke opbevares unødigt. Derudover skal urigtige oplysninger, enten fordi de ikke er korrekte eller ajourførte, straks berigtiges eller slettes. Derudover bør der være en sikkerhed for, at oplysningerne bliver behandlet med forsigtighed. Gennemsigtighed er derfor et princip om, at den registrerede skal have et indblik i, hvordan dennes oplysninger behandles.[59]

2.8.2 Formålsbegrænsning

Forordningens artikel 5, stk. 1, litra b angiver, at behandling af personoplysninger skal formålsbegrænses:

> "*... 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*

[56] Betænkning nr. 1565 om forordningen, side 92
[57] GDPR, præambelbetragtning 39
[58] GDPR, præambelbetragtning 39
[59] GDPR, præambelbetragtning 39

statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)".[60]

Det fremgår af præambelbetragtning nr. 39, at formålet for behandlingen af personoplysningerne skal være udtrykkeligt og legitimt. Formålet skal være fastlagt på tidspunktet for indsamlingen af oplysningerne.[61] Det skal dermed være tydeligt for den registrerede, hvad formålet med behandlingen er, og at der skal være et legitimt behandlingsgrundlag. Forudberegnelighed er en væsentlig sikkerhed for den registrerede, da der på denne måde vil være transparens, og den registrerede på den måde kan forudse, hvad de registrerede oplysninger anvendes til.[62]

2.8.3 Dataminimering og proportionalitet

Det fremgår af forordningens artikel 5, stk. 1, litra c, at personoplysninger skal "… *være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)*"[63]

Dataminimering er som ordet allerede antyder, at der skal ske en minimering af de data der behandles. Det er kun de relevante oplysninger, der må opbevares, og hvis nogle oplysninger ikke længere er nødvendige at opbevare til formålet, skal de dermed slettes. Det betyder også, at der løbende skal ryddes ud i de data der opbevares, da det kun er de absolut nødvendige data, der må opbevares.[64]

Den dataansvarlige må kun indsamle oplysninger, der er *tilstrækkelige*, hvilket skal forstås på den måde, at der kun må indsamles oplysninger, der er nødvendige for at opfylde formålet. Derudover skal oplysningerne være *relevante* for formålet, hvilket ikke er ensbetydende med, at alle relevante oplysninger må indsamles, idet de relevante oplysninger også skal være tilstrækkelige som nævnt ovenfor.[65] Den dataansvarlige må derfor ikke opbevare oplysninger, som er "nice-to-have", der kan anvendes på et senere tidspunkt.

[60] GDPR artikel 5, stk. 1, litra b
[61] GDPR, præambelbetragtning 39
[62] Blume, 2016, side 71
[63] GDPR artikel 5, stk. 1, litra c
[64] Betænkning nr. 1565 om forordningen, side 97
[65] Blume, 2016, side 72-73

Proportionalitetsprincippet er ligeledes relevant ved vurderingen af dataminimering. Det er, som nævnt ovenfor, nødvendigt at vurdere, hvilke oplysninger der må opbevares, og dette kan blandt andet afgøres ved at foretage en proportionalitetsvurdering. Her skal det vurderes, hvorvidt formålet med rimelighed kan opfyldes uden at behandle de pågældende oplysninger eller på en mindre indgribende måde.[66]

2.8.4 Rigtighed

Der er i forordningens artikel 5, stk. 1, litra d et krav om rigtighed, at oplysninger 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 (»rigtighed«)*".[67] Denne bestemmelse skal skabe en sikkerhed for, at de oplysninger der opbevares og behandles er korrekte og ajourførte. Det skal forhindre, at der behandles urigtige og forældede oplysninger om de registrerede. Såfremt der er urigtige oplysninger, skal de straks slettes eller berigtiges.[68]

I forhold til biometriske oplysninger, kan det eksempelvis ved ansigtsgenkendelse være forældede oplysninger, hvis den registrerede har været ude for en ulykke, der har ændret på ansigtstrækkene, eller hvis der er foretaget plastikoperationer, hvor strukturen på ansigtet er ændret. I disse tilfælde vil den oprindelige scanning af ansigtet ikke kunne anvendes, idet punkterne der måles på, vil være anderledes efter operationen. Nærmere herom i afsnit 3.1 om biometriske data.

2.8.5 Opbevaringsbegrænsning

Det er ifølge forordningens artikel 5, stk. 1, litra e ikke tilladt at opbevare oplysninger, hvor det er muligt at identificere de registrerede, i længere tid end det er nødvendigt, hvis formålet for behandlingen ikke længere er tilstede. Der er nogle få undtagelser til, hvornår oplysningerne må opbevares i længere tid, selvom formålet ikke længere er tilstede: "*… personoplysningerne alene*

[66] Betænkning nr. 1565 om forordningen, side 97
[67] GDPR artikel 5, stk. 1, litra d
[68] GDPR artikel 5, stk. 1, litra d

behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1…"[69]

Ved opbevaring af oplysningerne til ét af de i artikel 5, stk. 1, litra e nævnte grunde, skal der iværksættes passende organisatoriske og tekniske foranstaltninger for at beskytte den registreredes rettigheder.[70] Det er i præambelbetragtning nr. 39 anført, at den dataansvarlige bør fastsætte tidsfrister for sletning af data eller periodisk gennemgang af oplysninger, for at sikre sig, at der ikke er oplysninger, som er opbevaret med henblik på et bestemt formål.[71]

2.8.6 Integritet og fortrolighed

Det er i forordningens artikel 5, stk. 1, litra f anført, at personoplysninger skal behandles på en måde, så der ikke sker et brud på behandlingssikkerheden, ved hjælp af *"passende eller organisatoriske foranstaltninger"* [72]. Dette omfatter tab af data, uautoriseret adgang eller anvendelse af de registrerede data.[73] Et eksempel på foranstaltninger der kan foretages, kan være back-up af oplysningerne ved hjælp af lagring i en anden server.

I forordningens artikel 32 er der oplistet en række krav, der skal sikre, at behandlingen sker på en sikker og forsvarlig måde.

2.9 Lovlig behandling

Som tidligere nævnt, skal mindst ét af de i artikel 6, stk. 1, litra a-f oplistede betingelser være gældende, såfremt der er tale om lovlig behandling af personoplysninger.[74] Ved behandling af følsomme oplysninger, er det som udgangspunkt forbudt at behandle, medmindre mindst ét af de i artikel 9, stk. 2, litra a-j oplistede betingelser gør sig gældende.[75]

2.9.1 Samtykke

Ifølge artikel 6, stk. 1, litra a, kan behandling af personoplysninger foretages med samtykke fra den

[69] GDPR artikel 5, stk. 1, litra e
[70] Betænkning nr. 1565 om forordningen, side 99
[71] GDPR, præambelbetragtning 39
[72] Betænkning nr. 1565 om forordningen, side 100
[73] GDPR, præambelbetragtning 39
[74] GDPR artikel 6, stk. 1
[75] GDPR artikel 9, stk. 1 og 2

registrerede. Dette samtykke skal være givet til ét eller flere specifikke formål, hvorfor det ikke er nok at få et generelt samtykke til behandling af oplysningerne i alle henseende. Derudover er det i præambelbetragtning 32 anført, at tavshed, passivitet og forud afkrydsede felter ikke anses for værende et gyldigt samtykke, idet der skal ske en aktiv handling, når den registrerede giver sit samtykke. Såfremt der er flere formål til behandling af personoplysningerne, er det væsentligt, at der gives samtykke til alle formålene. Det er ikke nok alene at give samtykke til behandling af oplysningerne, men der skal gives et aktivt samtykke til alle formålene.[76] Nærmere gennemgang af samtykkereglerne i afsnit 2.11.

2.9.2 Nødvendig for dataansvarlige eller tredjemands legitime interesser

Det fremgår af forordningens artikel 6, stk. 1, litra f, at der må behandles oplysninger om en registreret uden dennes samtykke, i tilfælde af, at dette er nødvendigt for at varetage den dataansvarliges eller en tredjemands legitime interesser. Der skal dog i vurderingen lægges vægt på, om den registreredes grundlæggende rettigheder eller interesser går forud for den dataansvarliges eller tredjemands legitime interesser. Det er i betænkning nr. 1565 anført, at der kan forelægge en legitim interesse, hvis den registrerede er kunde hos den dataansvarlige og med rimelighed må forvente, at indsamling kan finde sted med det pågældende formål. Hvis den registrerede derimod ikke med rimelighed kan forvente dette, kan dennes grundlæggende rettigheder og interesser gå forud for behandlingen. [77] Det fremgår derudover af præambelbetragtning nr. 48 at:

> ”*Dataansvarlige, der indgår i en koncern eller institutioner, som er tilknyttet et centralt organ, kan have en legitim interesse i at videregive personoplysninger inden for koncernen til interne administrative formål, herunder behandling af kunders eller medarbejderes personoplysninger*”.[78]

[76] GDPR præambelbetragtning 32

[77] Betænkning nr. 1565 om forordning, side 134-135

[78] GDPR, præambelbetragtning 48

2.10 Behandlingshjemmel for følsomme oplysninger

Behandling af følsomme oplysninger er som udgangspunkt forbudt jf. forordningens artikel 9, stk. 1. Der er dog nogle undtagelser til denne regel i artikel 9, stk. 2, litra a-j, som vil blive gennemgået i de følgende afsnit. Artikel 9 omhandler behandling af særlige kategorier af personoplysninger[79], hvilket i det daglige bliver omtalt som følsomme oplysninger.

2.10.1 Samtykke

> "*Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke*".[80]

Ifølge artikel 9, stk. 2, litra a, kræver behandling af følsomme personoplysninger *udtrykkeligt* samtykke fra den registrerede.[81] Såfremt det i EU-retten eller medlemsstaternes nationale ret er bestemt, at forbuddet mod behandling af følsomme oplysninger i artikel 9, stk. 1 ikke ophæves ved registreredes samtykke, er artikel 9, stk. 2, litra a ikke gældende. [82]

Der er ikke i forarbejderne eller forordningen angivet et formkrav, men det er dog praktisk at modtage samtykket på skrift, såfremt der skulle blive uenighed omkring, hvorvidt samtykket foreligger. Samtykket skal endvidere gives til et eller flere specifikke formål.

Udtrykkeligt samtykke blev i databeskyttelsesdirektivet antaget for at være klart og utvetydigt. Der er ifølge betænkning nr. 1565 ikke sket en skærpelse af kravet for et gyldigt samtykke i artikel 9, stk. 2, litra a i forhold til artikel 6, stk. 1, litra a. Ordet "*udtrykkelig*" er blot for at understrege vigtigheden af, at der ikke må forekomme den mindste tvivl om, hvorvidt samtykket foreligger. Når der gives samtykke til behandling af følsomme oplysninger, er det vigtigt at samtykket gives til ét eller flere specifikke formål. Som tidligere nævnt skal det udtrykkeligt fremgå, hvad der gives samtykke til, således at der ikke er tvivl om, at den registrerede har givet samtykke til netop denne behandling.[83] Specifikationskravet er også gældende for samtykke efter artikel 6, stk. 1, litra a,

[79] GDPR artikel 9
[80] GDPR artikel 9, stk. 2, litra a
[81] Betænkning nr. 1565 om forordning, side 209
[82] Betænkning nr. 1565 om forordning, side 209
[83] Betænkning nr. 1565 om forordning, side 210-211

men ved følsomme oplysninger er det særligt vigtigt at lægge vægt på dette i forhold til kravet om udtrykkelighed. Nærmere gennemgang af samtykkereglerne i afsnit 2.11

2.10.3 Nødvendig af hensyn til retskrav

Det fremgår af forordningens artikel 9, stk. 2, litra f: "*Behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol*". [84] Behandling af oplysninger kan foretages, såfremt det er nødvendigt for at fastlægge, forsvare eller gøre et retskrav gældende. Dette gælder uanset om det er indenretsligt, udenretsligt eller administrativt.[85] Domstolene kan også i deres egenskab som domstol behandle disse oplysninger med henblik på at få fastlagt et retskrav. Det er op til virksomheden at påvise, at behandlingen er nødvendig.[86]

2.11 Samtykkeregler

Samtykkebestemmelserne i forordningens artikel 6, stk. 1, litra a og artikel 9, stk. 2, litra a er ikke formuleret ens. Umiddelbart kan det virke som, at der er et skærpet krav til samtykke jf. artikel 9, stk. 2, litra a, hvilket i praksis ikke er tilfældet, idet der i samtykkereglerne jf. artikel 7 er fire betingelser, der skal opfyldes, før der er et gyldigt samtykke. Disse betingelser vil bliver gennemgået nærmere senere i afsnittet.

Forordningens artikel 4, nr. 11 beskriver definitionen af et samtykke og betingelserne herfor: "*samtykke fra den registrerede: 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*".[87]

Udover disse gyldighedsbetingelser for samtykket, er der yderligere fire betingelser, der skal opfyldes for samtykket. Disse fire betingelser er oplistet i artikel 7.

Ifølge artikel 7, stk. 1, skal den dataansvarlige kunne påvise, at samtykke til behandling af

[84] GDPR artikel 9, stk. 2, litra f
[85] GDPR præambelbetragtning nr. 52
[86] Betænkning nr. 1565 om forordning, side 215-216
[87] GDPR artikel 4, nr. 11

personoplysninger er givet af den registrerede. For at kunne påvise, at samtykket er fra den registrerede, kræver dette at samtykket er afgivet i et dokumenterbart format, det kan f.eks. være skriftligt.[88]

Artikel 7, stk. 2 omhandler flere forhold i en skriftlig erklæring. Hvis det er tilfældet, at der er flere forhold, der skal gives samtykke til, skal det på en tydelig og enkel måde beskrives, hvad der gives samtykke til. Det skal være lettilgængeligt og letforståeligt for den registrerede at gennemskue, hvad der præcis bliver givet samtykke til. Såfremt dette ikke overholdes, vil samtykket i erklæringen ikke være gyldig.[89] Registerudvalget har i betænkning nr. 1345 anført, at "udtrykkelig" skal fortolkes som et *klart* og *utvetydigt* samtykke.[90]

I artikel 7, stk. 3 fastsættes det, at den registrerede til enhver tid kan trække sit samtykke tilbage, og at denne skal være oplyst om denne mulighed inden samtykket afgives. Hvis den registrerede ønsker at trække sit samtykke tilbage, skal det være ligeså let at trække tilbage, som det var at afgive det. Det kan dermed ikke besluttes, at samtykke alene kan trækkes tilbage ved at ringe i et bestemt tidsrum eller til en bestemt medarbejder.[91] Der bør gøres opmærksom på, at der ved behandling af personoplysninger alene på grundlag af samtykke, kan være en risiko forbundet hermed. Hvis behandlingen alene sker på grundlag af samtykke, og den registrerede ønsker at trække samtykket tilbage, kan det have den betydning, at behandling af oplysninger skal stoppes og slettes. Hvis behandlingen derimod iværksættes ud fra et andet behandlingsgrundlag end samtykke, vil der ikke opstå en situation, hvor behandlingen må ophøre på grundlag af registreredes ønske om at trække samtykket tilbage.[92]

Den sidste af de fire betingelser står i artikel 7, stk. 4. Denne vedrører frivilligheden i samtykket. Hvis opfyldelse af kontrakten eller ydelsen er betinget af registreredes samtykke til behandling af oplysninger, som ikke er nødvendige i forhold til opfyldelse af kontrakten eller ydelsen, vil der blive lagt vægt på dette i vurderingen af, om samtykket er afgivet frivilligt.[93]

[88] GDPR artikel 7, stk. 1
[89] GDPR artikel 7, stk. 2
[90] Betænkning nr. 1565 om forordningen, side 210
[91] GDPR artikel 7, stk. 3
[92] Waaben, side 540
[93] GDPR artikel 7, stk. 4

2.12 Registreredes rettigheder

Databeskyttelsesforordningens kapitel 3 indeholder en række bestemmelser om den registreredes rettigheder. Disse rettigheder er reguleret for at beskytte den registrerede mod blandt andet unødvendig lagring af personoplysninger og for at give et overblik over, hvilke oplysninger der er registreret.

2.12.1 Gennemsigtighed

Gennemsigtighed omfatter flere bestemmelser i forordningen, hvor formålet er, at den registrerede skal have de rette forudsætninger ved behandlingen. Artikel 12, stk. 1 beskriver således:

> "*Den dataansvarlige træffer passende foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 og enhver meddelelse i henhold til artikel 15-22 og 34 om behandling til den registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, navnlig når oplysninger specifikt er rettet mod et barn. Oplysningerne gives skriftligt eller med andre midler, herunder, hvis det er hensigtsmæssigt, elektronisk. Når den registrerede anmoder om det, kan oplysningerne gives mundtligt, forudsat at den registreredes identitet godtgøres med andre midler*".[94]

Princippet om gennemsigtighed omfatter enhver information, der er rettet mod den registrerede eller offentligheden. Informationerne kan gøres tilgængelige elektronisk på et websted, hvis de er rettet mod offentligheden.[95] Såfremt de er rettet mod den registrerede, er det ikke tilstrækkeligt at oplyse om dette på et websted, idet oplysningerne skal gives til den registrerede for at oplysningspligten er opfyldt. Ifølge artikel 12, stk. 1, som indeholder et formkrav, skal oplysningerne gives skriftligt og elektronisk, såfremt dette er hensigtsmæssigt.[96]

Det fremgår af artikel 12, stk. 2, at den dataansvarlige har pligt til at *lette udøvelsen*, hvilket vil sige, at den dataansvarlige skal muliggøre en medgørlig måde til blandt andet at anmode om indsigt, få slettet oplysninger og få berigtiget oplysninger. Med andre ord, skal det være let for den

[94] GDPR artikel 12, stk. 1

[95] GDPR præambelbetragtning nr. 58

[96] Betænkning nr. 1565 om forordningen, side 263

registrerede at udøve sine rettigheder. Dette kan eksempelvis gøres ved at lave genveje med direkte link på hjemmesiden. Udøvelsen af rettighederne sker på den registreredes opfordring, og den dataansvarlige må ikke afvise imødekommelse af anmodningen om udøvelse af rettighederne i artikel 15-22, medmindre den registrerede ikke er mulig at identificere. Dette er op til den dataansvarlige at påvise.[97]

Den dataansvarlige skal senest en måned efter anmodningen give den registrerede svar på anmodningen, herunder om der kan forekomme forsinkelser og i så fald en begrundelse for dette. Der er fastsat en maksimumsforlængelse på 2 måneder for at tage hensyn til en anmodnings kompleksitet og i tilfælde af, at det må forventes at tage længere tid at imødekomme anmodningen.[98] Derudover skal det være gratis for den registrerede at gøre brug af sine rettigheder. Hvis det vurderes at anmodningen er grundløs eller overdreven, kan der enten opkræves gebyr eller anmodningen kan afvises.[99] De specifikke krav til gennemsigtighed i forhold til forordningens artikel 13-14 og 15-22 er gennemgået nærmere i de følgende afsnit.

2.12.2 Oplysningspligt ved indsamling hos den registrerede

Såfremt oplysninger indsamles hos den registrerede er forordningens artikel 13 gældende.

Den dataansvarlige har pligt til at oplyse den registrerede om en række informationer ved indsamlingen af oplysninger. Nogle af disse informationer skal også fremgå af fortegnelsen jf. forordningens artikel 30, som virksomheden, organet eller lignende skal føre for behandlings-aktivitet, i tilfælde af tilsynskontrol.[100] Når der indsamles oplysninger hos den registrerede, er der oplistet en række oplysninger i artikel 13, stk. 1 litra a-f, der skal gives til den registrerede ved tidspunktet for indsamlingen.

Den registrerede skal oplyses om;

- *Identitet* og *kontaktoplysninger* for den dataansvarlige og en repræsentant i tilfælde af at en sådan haves.[101]
- *Kontaktoplysninger for en databeskyttelsesrådgiver* såfremt en sådan haves.[102]

[97] Betænkning nr. 1565 om forordningen, side 264
[98] Betænkning nr. 1565 om forordningen, side 272-273
[99] GDPR artikel 12, stk. 4
[100] Betænkning nr. 1565 om forordningen, side 286
[101] GDPR artikel 13, stk. 1, litra a

- *Formålet* med behandlingen og *retsgrundlaget* herfor.[103] Retsgrundlaget kan være behandlingshjemlen i forordningens artikel 6 eller 9, men det kan ligeledes være en anden lov. I begge tilfælde skal den dataansvarlige henvise til det præcise retsgrundlag.[104]
- De *legitime interesser*, såfremt behandlingen sker på baggrund af artikel 6, stk. 1, litra f.[105]
- *Kategorier af modtagere* eller *modtagere* af de indsamlede oplysninger.[106] Med *kategori af modtagere* menes der sandsynligvis en overordnet modtagergruppe. Der skal kun gives oplysninger om disse, hvis der er nogen på tidpunktet for indsamlingen, idet forordningen anvender begrebet "eventuelle".[107]
- Oplysninger om *overførsel til tredjelande*, hvis dette er tilfældet.[108] Dette skal hun oplyses såfremt det er relevant. Hvis ikke der overføres til tredjelande, vil denne bestemmelse ikke være relevant.[109]

For at sikre en rimelig og gennemsigtig behandling er der i forordningens artikel 13, stk. 2, litra a-f, oplistet nogle yderligere oplysninger, der nødvendige at give til den registrerede på tidspunktet for indsamlingen af oplysningerne.[110] I artikel 13, stk. 1 er det oplysninger, der skal gives til den registrerede, mens stk. 2 er oplysninger, der er nødvendige at give for at sikre en gennemsigtig og rimelig behandling.[111]

For at opnå en gennemsigtig og rimelig behandling, skal den registrerede oplyses om følgende ved indsamlingen af oplysningerne;

- *Tidsrummet* for opbevaringen af oplysningerne eller de kriterier tidsrummet vurderes ud fra, idet det ikke altid er muligt at vurdere tidsrummet ved tidspunktet for indsamlingen.

---

[102] GDPR artikel 13, stk. 1, litra b
[103] GDPR artikel 13, stk. 1, litra c
[104] Betænkning nr. 1565 om forordningen, side 287
[105] GDPR artikel 13, stk. 1, litra d
[106] GDPR artikel 13, stk. 1, litra e
[107] Betænkning nr. 1565 om forordningen, side 288
[108] GDPR artikel 13, stk. 1, litra f
[109] Betænkning nr. 1565 om forordningen, side 288
[110] GDPR artikel 13, stk. 2
[111] Betænkning nr. 1565 om forordningen, side 286

Dette skal sikre, at der ikke opbevares oplysninger længere end nødvendigt, og at den registrerede er bekendt med opbevaringsperioden.[112]

- Registreredes ret til; *indsigt*, *sletning*, *berigtigelse*, *begrænsning*, *indsigelse* og *dataportabilitet*.[113]
- Registreredes ret til at *trække samtykket tilbage*, såfremt behandlingen sker på baggrund af samtykke jf. artikel 6, stk. 1, litra a eller artikel 9, stk. 2, litra a.[114]
- Registreredes ret til at indgive en *klage* til tilsynsmyndigheden.[115]
- Hvorvidt meddelelse af oplysningerne er *lovpligtige eller et krav for opfyldelse eller indgåelse af en kontrakt*. Derudover skal det fremgå, hvorvidt den registrerede har pligt til at afgive oplysningerne og konsekvenserne såfremt registrerede ikke afgiver oplysningerne.[116]
- Hvorvidt der kan forekomme *automatiske afgørelser*, logikken heri og betydning og mulige konsekvenser for den registrerede.[117] Den registrerede skal opnå en forståelse af, hvordan afgørelserne træffes, og hvad der lægges til grund.[118]

I det tilfælde, hvor de indsamlede oplysninger ønskes anvendt til viderebehandling til et andet formål end det oprindelige, skal den dataansvarlige oplyse den registrerede om dette og andre relevante oplysninger jf. stk. 2 for at sikre en rimelig og gennemsigtig behandling.[119] Det er ikke nødvendigt at oplyse den registrerede om de oplistede oplysninger i forordningens artikel 13, stk. 1, litra a-f og 2, litra a-f og om viderebehandling, hvis den registrerede allerede er blevet oplyst om dette tidligere.[120]

[112] GDPR artikel 13, stk. 2, litra a
[113] GDPR artikel 13, stk. 2, litra b
[114] GDPR artikel 13, stk. 2, litra c
[115] GDPR artikel 13, stk. 2, litra d
[116] GDPR artikel 13, stk. 2, litra e
[117] GDPR artikel 13, stk. 2, litra f
[118] Betænkning nr. 1565 om forordningen, side 293
[119] Betænkning nr. 1565 om forordningen, side 294
[120] GDPR artikel 13, stk. 3 og 4

2.12.3 Oplysningspligt ved indsamling hos andre end den registrerede

Såfremt oplysningerne er indsamlet hos andre end den registrerede, er forordningens artikel 14 gældende.

Når der indsamles oplysninger hos andre end den registrerede, er der oplistet en række oplysninger i artikel 14, stk. 1 litra a-f, der skal gives til den registrerede ved tidspunktet for indsamlingen. Forordningens artikel 14, stk. 1, litra a, b, c, e og f er identiske med bestemmelserne i artikel 13, stk. 1, litra a, b, c, e og f. Den eneste forskel på oplysningspligten i artikel 13, stk. 1 og 14, stk. 1 er derfor litra d i begge artikler. Se derfor beskrivelsen i afsnit 2.12.2 for nærmere udspecificering af artiklernes litra a, b, c, e og f.

Som nævnt er den eneste forskel på artikel 13, stk. 1 og artikel 14, stk. 1 bestemmelsen i litra d. I artikel 14, stk. 1, litra d er det anført, at der skal gives oplysninger til den registrerede om "*de berørte kategorier af personoplysninger*"[121]. Som nævnt i afsnit 2.12.3 skal den dataansvarlige oplyse den registrerede om modtagere eller kategorier af modtagere jf. forordningens artikel 13, stk. 1, litra e. Den nye dataansvarlige, som modtager oplysninger fra den oprindelige dataansvarlige, skal herefter oplyse den registrerede om de modtagne kategorier af personoplysninger.[122]

I forordningens artikel 14, stk. 2, litra a-g er der oplistet en række oplysninger, som er nødvendige for at sikre en rimelig og gennemsigtig behandling af oplysningerne. Artikel 14, stk. 2, litra a, b, c, d, e og g er identisk med artikel 13, stk. 2, litra a, b, c, d og f og stk. 1, litra d. Se derfor afsnit 2.12.2 for nærmere udspecificering.

Artikel 14, stk. 2, litra f er derimod anderledes fra resten af artikel 13, stk. 2. Det fremgår af artikel 14, stk. 2, litra f, at den dataansvarlige skal oplyse den registrerede om kilden, hvorfra oplysningerne stammer, og eventuelt om de stammer fra en offentlig tilgængelig kilde. Det fremgår derudover af præambelbetragtning 61, at der skal gives generelle oplysninger, såfremt kilden til oplysningerne ikke er mulig at fastslå grundet brug af flere kilder.[123]

[121] GDPR artikel 14, stk. 1, litra d

[122] Betænkning nr. 1565 om forordningen, side 304

[123] GDPR præambelbetragtning nr. 61

Den dataansvarlige har pligt til at give den registrerede de i artikel 14, stk. 1 og 2 oplistede oplysninger:

- indenfor en *rimelig frist* efter indsamlingen og senest 1 måned efter indsamlingen jf. forordningens artikel 14, stk. 3, litra a. I det tidligere direktiv var det anført, at oplysningspligten var ved registreringen, hvilket generelt ansås for at være indenfor 10 dage. Det er i betænkningen til forordningen anført, at det må formodes, at det med *rimelig frist* må antages, at de 10 dage kan indeholdes i denne betegnelse.[124] Der er dog ikke en egentlig fastsat længde for, hvor lang tid *rimelig frist* er, hvorfor der er plads til fortolkning.
- senest ved første kommunikation, såfremt oplysningerne er indsamlet med henblik på kommunikation.[125]
- senest ved første videregivelse såfremt oplysningerne er indsamlet med henblik på videregivelse til en anden modtager.[126]

Ved viderebehandling af oplysningerne til et andet formål end det oprindelige gælder samme regler som i artikel 13, stk. 3.[127]

I artikel 14, stk. 5, litra a-d er der oplistet nogle undtagelser til den dataansvarlige oplysningspligt ifølge artikel 14, stk. 1 og 2. Dette gælder i tilfælde, *hvor* den registrerede allerede er oplyst, *hvis* det vil kræve uforholdsmæssig indsats eller er umuligt, *hvis* videregivelsen eller indsamlingen er udtrykkeligt fastsat i medlemsstaternes nationale ret eller EU-retten, og *hvis* oplysningerne ifølge EU-retten eller medlemsstaternes nationale ret skal forblive fortrolige med henblik på tavshedspligt.[128]

2.12.4 Retten til indsigt

Den registrerede har ret til at få indsigt i, om der er registreret oplysninger om denne hos den dataansvarlige, og i så fald hvilke oplysninger der er registreret om denne.[129] I det tilfælde, hvor

[124] Betænkning nr. 1565 om forordningen, side 305
[125] GDPR artikel 14, stk. 3, litra b
[126] GDPR artikel 14, stk. 3, litra c
[127] GDPR artikel 14, stk. 4
[128] GDPR artikel 5
[129] GDPR artikel 15, stk. 1

der er registreret oplysninger om den pågældende person, har denne ret til en række oplysninger omkring behandlingen. Oplysninger er anført i artikel 15, stk. 1, litra a-h og omfatter:

> "*a) formålene med behandlingen*
>
> *b) de berørte kategorier af personoplysninger*
>
> *c) de modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, navnlig modtagere i tredjelande eller internationale organisationer*
>
> *d) om muligt det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til fastlæggelse af dette tidsrum*
>
> *e) retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling af personoplysninger vedrørende den registrerede eller til at gøre indsigelse mod en sådan behandling*
>
> *f) retten til at indgive en klage til en tilsynsmyndighed*
>
> *g) enhver tilgængelig information om, hvorfra personoplysningerne stammer, hvis de ikke indsamles hos den registrerede*
>
> *h) forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.*"[130]

Hvis den dataansvarlige behandler store mængder data om den registrerede, kan den dataansvarlige dog anmode om at få præciseret, hvilken behandlingsaktivitet eller oplysninger den registrerede ønsker indsigt i. Retten til at få indsigt omfatter dog ikke adgang til oplysningerne på bekostning af krænkelse af andre personers rettigheder eller frihedsrettigheder, eksempelvis forretningshemmeligheder.[131] Den registrerede har ret til at få udleveret en kopi af de oplysninger, som bliver behandlet om den pågældende. Hvis den registrerede anmoder om indsigt gentagne gange alene for at pålægge den dataansvarlig unødig ekstra arbejde, må den dataansvarlige

[130] GDPR artikel 15, stk. 1, litra a-h
[131] GDPR præambelbetragtning nr. 63

pålægge et rimeligt gebyr for administration eller afvise anmodningen.[132] Dette er ikke ensbetydende med, at den registrerede ikke må anmode om indsigt flere gange. Den registrerede bør have ret til at få indsigt med *rimelig mellemrum*[133]. Hvad der ligger i betydningen af *rimelig mellemrum*, er et vurderingsspørgsmål. Det kan afhænge af branche, kutyme og hvor ofte der sker ændringer i registrerede oplysninger. Hvis der ofte sker opdateringer eller tilføjelser af oplysninger, bør der i lige så høj grad gives indsigt. Hvis der derimod ikke sker opdateringer eller ændringer ofte, bør registrerede ikke kunne få indsigt lige så ofte som i førnævnte tilfælde.

2.12.5 Retten til at blive glemt

Den registrerede har ret til at få slettet sine registrerede oplysninger uden *unødig forsinkelse* jf. forordningens artikel 17, stk. 1. Denne ret kaldes populært *retten til at blive glemt.* Den dataansvarlige har derudover pligt til at slette oplysninger uden *unødige forsinkelser,* hvis én af grundene i artikel 17, stk. 1, litra a-f gør sig gældende.[134]

Den registrerede har ret til at få slettet sine oplysninger, hvis der ikke længere er grundlag for behandling af oplysningerne, eller hvis behandling af oplysningerne ikke længere er nødvendige til det formål, de er indsamlet til.[135] Retten til at få slettet sine oplysninger, er ikke ensbetydende med, at den registrerede til enhver tid kan kræve oplysningerne slettet. Forordningens præambelbetragtning nr. 65 nævner en række grunde, der danner grundlag for, at den registrerede ikke bør få slettet sine oplysninger;

> ”*Yderligere opbevaring af personoplysningerne bør dog være lovlig, hvis det er nødvendigt for at udøve retten til ytrings- og informationsfrihed, for at overholde en retlig forpligtelse, for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, af hensyn til samfundsinteresser på folkesundhedsområdet, til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller*

[132] Betænkning nr. 1565 om forordningen, side 322
[133] GDPR præambelbetragtning nr. 63
[134] GDPR artikel 17, stk. 1
[135] GDPR præambelbetragtning nr. 65

statistiske formål, eller for at retskrav kan fastlægges, gøres gældende eller forsvares".[136]

Hvis oplysningerne alene behandles på grundlag af samtykke, og den registrerede trækker sit samtykke tilbage, er der naturligvis ikke længere grundlag for at behandle oplysningerne. Fordelen ved den registreredes ret til at få slettet sine oplysninger er, at oplysningerne kan kræves slettet inden de generelt fastsatte slettefristers udløb.[137]

Der er i forordningens præambelbetragtning nr. 65 især lagt vægt på behandling af oplysninger, som er indsamlet, mens vedkommende var barn. Her er det anført, at retten til at få slettet sine oplysninger særligt er relevant, når samtykket gives af et barn, da et barn formentlig ikke er i stand til at kende konsekvenserne af at give samtykket til behandling af personoplysninger. Det skal derfor være muligt at trække sit samtykke tilbage, uanset om registrerede stadig er barn eller samtykket først trækkes tilbage som voksen.[138]

2.12.6 Retten til begrænset behandling

Den registrerede har ret til at få begrænset behandlingen af oplysninger jf. forordningen artikel 18, stk. 1, såfremt et af de i artikel 18, stk. 1, litra a-d betingelser gør sig gældende.

Såfremt den registrerede bestrider, at oplysningerne er korrekte, skal den dataansvarlige begrænse behandlingen, indtil tvivlen er udredt jf. forordningens artikel 18, stk. 1, litra a. Ved ukorrekte oplysninger skal oplysningerne straks slettes eller berigtiges jf. artikel 5, stk. 1, litra d og det er derfor nødvendigt at begrænse behandlingen i tilfælde af, at oplysningerne ikke er korrekte.[139]

Behandlingen af oplysningerne skal derudover begrænses, hvis behandlingen er ulovlig og den registrerede modsætter sig at oplysningerne slettes jf. forordningens artikel 18, stk. 1, litra b. Ulovlig behandling kan være på baggrund af ukorrekte oplysninger, og der kan på denne baggrund

[136] GDPR præambelbetragtning nr. 65
[137] Betænkning nr. 1565 om forordningen, side 335
[138] GDPR præambelbetragtning nr. 65
[139] Betænkning nr. 1565 om forordningen, side 340

foreligge et erstatningskrav mod den dataansvarlige. En registreret kan modsætte sig sletning for eksempel i det tilfælde, hvor oplysningerne skal bruges som bevis i erstatningssagen.[140]

Behandlingen skal begrænses, hvis den dataansvarlige ikke længere skal bruge oplysningerne, men hvor det er nødvendigt at beholde dem i forhold til at fastlægge, forsvare eller gøre et retskrav fældende jf. forordningens artikel 18, stk. 1, litra c.

Behandlingen kan endvidere, jf. forordningens artikel 18, stk. 1, litra d, begrænses i en periode for afklaring, hvis den registrerede har gjort indsigelse mod behandlingen af oplysningerne ifølge forordningens artikel 21, stk. 1 vedrørende den dataansvarliges legitime interesser fremfor den registreredes interesser.

Hvis der er opnået begrænsning ud fra et af de i forordningens artikel 18, stk. 1, litra a-d oplistede begrundelser, må der ikke foretages anden behandling end opbevaring, medmindre den registrerede giver sit samtykke til behandlingen. Derudover må oplysningerne behandles, hvis det er til at fastlægge, forsvare eller gøre et retskrav gældende. I praksis kan begrænsningen ske ved at flytte de pågældende oplysninger fra systemet, gøre dem utilgængelige for dem, der er i berøring af oplysningerne, eller på anden måde tydeliggøre at oplysningerne ikke må behandles.[141]

2.12.7 Retten til dataportabilitet

Den registreredes ret til dataportabilitet er indført for, at den registrerede får større kontrol over sine oplysninger.[142] Det skal være muligt for den registrerede at modtage registrerede oplysninger fra den dataansvarlige til eget brug eller for at transmittere dem til en anden dataansvarlig. Efter anmodning fra den registrerede, kan oplysningerne også overføres fra den dataansvarlige til en anden part, som derefter ligeledes vil blive dataansvarlig, hvis det teknisk er muligt.[143] Det er i bestemmelsen angivet, at den registrerede har krav på at modtage de registrerede oplysninger "*i et struktureret, almindeligt anvendt og maskinlæsbart format*".[144] Der opfordres i præambel-

[140] Betænkning nr. 1565 om forordningen, side 341
[141] GDPR præambelbetragtning nr. 67
[142] GDPR præambelbetragtning nr. 68
[143] Artikel 29-gruppen, *Retningslinjer vedrørende retten til dataportabilitet*, WP 242 rev. 01, side 5-6
[144] GDPR artikel 20, stk. 1

betragtning 68 i forordningen til, at den dataansvarlige udvikler et indbyrdes kompatibelt system, der muliggør dataportabilitet.[145]

For at den registrerede kan gøre sin ret til dataportabilitet gældende, skal de tre kumulative betingelser i artikel 20 opfyldes. Den første betingelse for at gøre retten til dataportabilitet gældende er, *at* oplysningerne behandles på baggrund af et samtykke jf. forordningens artikel 20, stk. 1, litra a, eller *at* behandlingen er nødvendigt med henblik på opfyldelse af en kontrakt jf. artikel 20, stk. 1, litra b. Hvis ikke behandlingen af oplysningerne er iværksat på ét af disse grundlag, er retten til dataportabilitet ikke gældende.[146] Den næste betingelse er, at oplysningerne omhandler den registrerede, der ønsker at gøre sin ret gældende. Den sidste betingelse er, at retten til dataportabilitet ikke må krænke andres frihedsrettigheder eller rettigheder.[147]

2.12.8 Profilering

Profilering er i forordningen defineret som:

> "*… enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser*".[148]

Forordningens artikel 22, stk. 1 tildeler den registrerede en ret til ikke at være genstand for automatiske afgørelser, herunder profilering: "*Den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende*"[149]. Der er i artikel 22, stk. 2, litra a-c oplistet nogle undtagelser til forbuddet i artikel 22, stk. 1.

Profilering er baseret på Big Data, hvilket er betegnelsen for en stor mængde data, der enten er struktureret eller ustruktureret. Problematikken omkring Big Data er, at oplysningerne ved dataminimering kan sammenkobles, hvorved der dannes et bestemt handlemønster eller på en

[145] GDPR præambelbetragtning nr. 68
[146] GDPR præambelbetragtning nr. 68
[147] Betænkning nr. 1565 om forordningen, side 349
[148] GDPR artikel 4, stk. 4
[149] GDPR artikel 22, stk. 1

anden måde oprette en profil på den registrerede. Dette kan anvendes til at forudsige den registreredes fremtidige dispositioner og derved anvendes til eksempelvis markedsføring eller i værste fald automatiske afgørelser i strid med forordningen.[150]

Kapitel 3 – Biometriske data og tv-overvågning

3.1 Biometriske data

Biometri betyder "at måle liv", hvilket stammer fra det græske ord bios som betyder liv, og metron som betyder mål.[151] Biometriske data er i forordningens artikel 4, nr. 11 beskrevet: "*Biometriske data«: personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger*".[152]

Som det kan udledes af bestemmelsen, er biometriske oplysninger et målbart fysisk eller biologisk kendetegn eller egenskab ved en person. Det kan være nogle fysiske træk, som er særegen for hver enkelt person, herunder fingeraftryk, iris eller lignende. Noget andet kan være særlig adfærd ved en person, eksempelvis gangart eller bestemte gentagne bevægelser, der kan føre til entydig identifikation af personen.

Biometriske data er ifølge GDPR en følsom oplysning, hvis det er med henblik på entydig identifikation.[153] Hvornår der er tale om entydig identifikation eller ej, vil blive gennemgået nærmere længere nede i dette afsnit. Sammenlignet med andre oplysninger, er disse oplysninger som udgangspunkt ikke mulige at ændre på og ændres heller ikke naturligt i løbet af livet. Oplysningerne er permanente, og det er derfor ikke muligt igen at beskytte en persons biometriske oplysninger, hvis der først er sket et brud på datasikkerheden, og oplysningerne er lækket. Biometri er samtidig også den sikreste måde at identificere en person på, da det er helt unikt for den enkelte.[154] Det skal dog bemærkes, at fuld biometri kan anvendes på tværs af systemer til at identificere personer, hvorfor der er større risiko for misbrug. Den måde man

[150] Blume, 2016, side 59-60
[151] Tranberg, "Biometriske personoplysninger", afsnit 3
[152] GDPR artikel 4, nr. 14
[153] GDPR artikel 9, stk. 1
[154] Tranberg, "Biometriske personoplysninger", afsnit 2

eksempelvis scanner fingeraftryk på, er ved at måle ud fra et antal punkter i fingeraftrykket, som kan være forskellige afhængig af udstyret. Teknologien er ikke nået til, at fuld biometri er praktisk at anvende på nuværende tidpunkt.

En af grundene til, at det som udgangspunkt er forbudt at behandle biometriske data kan være, at brud på datasikkerheden kan have ekstreme konsekvenser for den registrerede, da oplysningerne kan misbruges, hvis de ender hos de forkerte personer. Hvis dette er tilfældet, vil den registrerede ikke have mulighed for at ændre identiteten, som det er muligt, hvis det i stedet havde været en af de almindelige oplysninger, som navn eller adresse. Dette er dog ikke ensbetydende med, at de almindelige oplysninger ikke skal opbevares under høj datasikkerhed.

Biometriske oplysninger opdeles som udgangspunkt i to grupper, henholdsvis adfærdsmæssige karakteristika og fysiologiske karakteristika.[155]

De adfærdsmæssige karakteristika er kendetegnet ved, som ordet siger, at disse måles ud fra, hvordan en persons adfærdsmønster udformer sig. Det kan eksempelvis være tastedynamik på et tastatur, gangart, gentagne bevægelser, stemmeanalyse og signaturanalyse.[156] Gangart kan eksempelvis analyseres ud fra bevægelsesmønster, herunder eventuelt hvis personen halter eller har hypermobile led, som medfører et særligt bevægelsesmønster.

De fysiologiske karakteristika er målt ud fra fysiske faktorer. Der er i Teknologirådets rapport oplistet en række eksempler på, hvad fysiologiske karakteristika eksempelvis kan være:

- ”*Fingeraftryksgenkendelse*
- *Ansigtsgenkendelse*
- *Håndscanning*
- *Irisgenkendelse*
- *Retinascanning*
- *Venescanning*
- *Øreformsanalyse*

[155] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 12
[156] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 12

- *Hjernebølgeanalyse*
- *Lugtanalyse*
- *Dna*".[157]

Et af de biometriske oplysninger, der er alment kendt, er fingeraftryk. Dette er genetisk bestemt og helt særligt for hver enkelt person. Det findes ikke to personer med ens fingeraftryk. Dette gælder uanset, om disse er enæggede tvillinger.[158] De biometriske oplysninger er derfor helt specielle for den enkelte person og bør behandles meget forsigtigt. Et område hvor der ofte anvendes fingeraftryk, er til efterforskning. Her vil det ud fra fingeraftryk være muligt at genkende en gerningspersonen, idet fingeraftryk er så særegen for den enkelte person, at det med sikkerhed kan fastlægges, hvorvidt fingeraftrykket stammer fra den pågældende. Politiet anvender fuld biometri af fingeraftrykket.

Det er i denne afhandling ikke nødvendigt at beskrive hver enkelt biometrisk teknologi nærmere, idet det ikke er alle, der er anvendelige ved tv-overvågning. Ansigtsgenkendelse og ganganalyse vil blive gennemgået nærmere i afsnit 3.4.

Ved anvendelse af biometriske oplysninger skelnes der mellem identifikation og verifikation. Ved identifikation vil systemet, ud fra de lagrede biometriske oplysninger, finde frem til en bestemt person. Ved verifikation vil der i systemet være nogle registrerede, hvor systemet alene vil udlede, at den pågældende person er registreret i systemet. Det vil på denne måde ikke være muligt at identificere, hvem af de registrerede, der har anvendt sine biometriske data for at få adgang. Et eksempel på identifikation er fingeraftryk, der er registreret i et system, der vil give adgang til et bankboksrum. Den pågældende person, der forsøger at få adgang til rummet, vil i systemet blive genkendt iblandt de andre registrerede. I samme situation vil det være verifikation i det tilfælde, hvor den pågældende person, der forsøger at få adgang til rummet, i stedet alene vil blive genkendt som én af de registrerede. Her vil det ikke være muligt at se, hvilken af de registrerede, der forsøger at få adgang, men blot at det er én af de registrerede. Verifikation kan derfor anses for at være mindre indgribende i det omfang, at det ikke fører til en entydig identifikation af den

[157] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 12
[158] https://videnskab.dk/sporg-videnskaben/har-enaeggede-tvillinger-identiske-fingeraftryk

registrerede.[159] Det fremgår af forordningens artikel 9, stk. 1 om følsomme oplysninger, at biometriske oplysninger skal føre til en entydig identifikation. I det tilfælde at det er verifikation, er det ikke en entydig identifikation og må derfor anses for at være en almindelig oplysning.

Ansigtsgenkendelse er indenfor de seneste år blevet en hyppig anvendt teknologi. Smartphoneproducenter som Apple anvender det blandt andet i deres seneste to lanceringer, hvor det bliver anvendt til at låse telefonen op med. Derved lagres de biometriske oplysninger om brugeren i telefonen.

Facebook har siden 2010 anvendt en photo tagging teknologi, der foreslår, hvem der er på billederne. Google har senere anvendt en teknologi, der kan sortere billederne ud fra ansigtsgenkendelse. Dette kan de gøre uden en egentlig scanning af personernes ansigt, idet den gentagne manuelle tagging af personer, kan danne baggrund for at udforme en algoritme for de enkelte personers biometri.[160]

MasterCard har eksperimenteret med ansigtsgenkendelse, som muligvis på sigt kan anvendes til at godkende en betalinger.[161] Ansigtsgenkendelse er en sikrer form end adgangskoder, idet adgangskoder kan misbruges. Ved ansigtsgenkendelse kan "koden" ikke ses ved at kigge over skulderen.

3.2 Tv-overvågning

Tv-overvågning anses, efter tv-overvågningslovens § 1, stk. 2, for at være automatisk eller fjernbetjent overvågning af personer, som sker regelmæssigt eller vedvarende ved hjælp af video, billeder eller lignende.[162] Tv-overvågningsloven regulerer, hvem og i hvilke tilfælde der må foretages tv-overvågning. Lagring og behandling af de indsamlede oplysninger, reguleres derimod af GDPR.[163] Tv-overvågningsloven afløser de tidligere bestemmelser i persondatalovens kapitel 6a

[159] Tranberg, "Biometriske personoplysninger", afsnit 2
[160] https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1/, d. 22/11-2018
[161] https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1/, d. 22/11-2018
[162] Tv-overvågningslovens § 1, stk. 2
[163] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/, afsnit: tv-overvågningsloven, d. 5/10-2018

om behandling af personoplysninger i forbindelse med tv-overvågning.[164] Da persondataloven ikke længere er gældende, er tv-overvågningsloven en supplerende lov til forordningen, som skal videreføre de bestemmelser, som ikke er reguleret af forordningen, men som var en del af den nationale lov.[165]

3.2.1 Lovens anvendelsesområde

Ifølge tv-overvågningslovens § 1, stk. 1 må privatpersoner som udgangspunkt ikke foretage tv-overvågning af "*gade, vej, plads eller lignende område, som benyttes til almindelig færdsel*". [166]

Med privatpersoner menes der både private fysiske personer og private juridiske personer, hvorfor erhvervsdrivende også er omfattet. Det er dog vigtigt at bemærke, at der er nogle undtagelser til denne bestemmelse, som vil blive gennemgået nærmere i afsnit 3.2.2. Offentlige myndigheder er ikke omfattet af tv-overvågningsloven[167].

Forbuddet gælder på veje, gader, pladser eller lignende, hvor der er almindelig færdsel. Dette kan fortolkes ud fra praksis ifølge færdselslovens § 1, hvor det er områder "*… som benyttes til almindelig færdsel af en eller flere færdselsarter*".[168] Hvorvidt området er privat eller offentlig ifølge vejloven, har ingen betydning idet denne afgrænsning ofte anvendes med henblik på andre formål. Et privat område ifølge vejloven kan derfor godt være omfattet af forbuddet i tv-overvågningslovens § 1. Tv-overvågning omfatter både optagelser som bliver gemt og optagelser som er live.[169]

3.2.2 Undtagelser

Forbuddet i tv-overvågningslovens § 1 om privatpersoners foretagelse af tv-overvågning medfører nogle undtagelser i § 2, stk. 1, nr. 1-4.

[164] Lovforslag nr. 205, indledning, side 3
[165] Lovforslag nr. 205, indledning, side 3
[166] Tv-overvågningslovens § 1, stk. 1
[167] Tv-overvågningsloven, Karnovs note nr. 1
[168] Færdselslovens § 1
[169] Tv-overvågningsloven, Karnovs note nr. 1

Ifølge § 2, stk. 1, nr. 1 må der foretages tv-overvågning af "… *tankstationer, fabriksområder, overdækkede butikscentre og lignende områder…* "[170] af de erhvervsdrivende, der har rådighed over områderne.

Ifølge § 2, stk. 1, nr. 2 må der foretages tv-overvågning af pengeautomater, vekselautomater og pengetransportbiler af den erhvervsdrivende, der har rådighed over disse. Overvågningskameraet skal dog være indstillet til kun at filme personer, der benytter automaterne eller er i umiddelbar nærhed af disse eller pengetransportbilen.

Ifølge §2, stk. 1, nr. 3 må "… *pengeinstitutvirksomheder, spillekasinoer, hotel- og restaurationsvirksomheder samt butikscentre og butikker, hvorfra der foregår detailsalg…*"[171] foretage tv-overvågning af deres indgange og facader og området omkring dette, såfremt det kan benyttes som adgangsveje eller flugtveje. Disse optagelser må lagres i kriminalitetsforebyggende øjemed.[172] Ifølge § 2, stk. 1, nr. 4 må der foretages liveoptagelser af "… *egne indgange, facader, indhegning eller lignende*".[173]

3.3.3 Kriminalitetsforebyggende øjemed

Tv-overvågning med lyd og billeder, som indeholder personoplysninger, må videregives i tre tilfælde, hvis det er i kriminalitetsforebyggende øjemed jf. tv-overvågningslovens § 4c, stk. 1.

- Der skal forelægge samtykke fra den registrerede jf. § 4c, stk. 1, nr. 1.
- Videregivelsen er lovbestemt jf. § 4c, stk. 1, nr. 2.
- Videregivelsen sker i kriminalitetsopklarende øjemed til politiet jf. § 4c, stk. 1, nr. 3.

Andre tilfælde, hvor der må ske videregivelse af tv-overvågning med lyd og billede, er i kriminalitetsforebyggende øjemed internt i virksomheder, herunder koncernstruktur, og til andre erhvervsdrivende. Der er i tv-overvågningslovens § 4c, stk. 2, nr. 1-4 oplistet nogle tilfælde, hvor overvågningen kan videregives. Overvågningen kan videregives, hvis formodede gerningsmænd eller personer, der har forsøgt at begå berigelsesforbrydelse eller lignende, omfattet af

[170] TV-overvågningslovens § 2, stk. 1, nr. 1
[171] Tv-overvågningsloven § 2, stk. 1, nr. 3
[172] Tv-overvågningsloven, Karnovs noter, nr. 8
[173] Tv-overvågningsloven § 2, stk. 1, nr. 4

straffelovens §§ 276-289a, fremgår af optagelserne jf. § 4c, stk. 2, nr. 1.[174] Hvis den formodede gerningsperson eller gerningspersoner samme dag er anmeldt til politiet for forbrydelsen, må oplysningerne videregives jf. § 4c, stk. 2, nr. 2. Hvis anmeldelsen findes grundløs eller den trækkes tilbage, skal de videregivne oplysninger slettes og modtagerne af oplysningerne, der har benyttet disse i kriminalitetsforebyggende øjemed, skal ligeledes slette dem.[175] Overvågningen må videregives, hvis der er konkrete grunde til at tro, at den formodede gerningsperson eller gerningspersoner vil begå en lignende forbrydelse mod andre erhvervsdrivende, som oplysningerne videregives til jf. § 4c, stk. 2, nr. 3. Denne bestemmelse kan anvendes i tilfælde, hvor samme gerningsperson har begået lignende forbrydelser flere gange eller flere steder eller, hvis forbrydelsen har været af grov karakter, og det må forventes at kunne ske igen. Overvågningen må kun videregives til andre erhvervsdrivende, der kan være i risiko for, at lignende kan ske.[176] Det kan eksempelvis være i et geografisk afgrænset område, hvor det må forventes, at gerningspersonen eller gerningspersonerne vil begå forbrydelse. Det kan også være en butikskæde, hvor der er sandsynlighed for, at de vil begå forbrydelsen i flere af kædens butikker. Dette er uanset geografisk afgrænsning.[177] Slutteligt kan der videregives overvågningsmateriale til lukkede systemer, eksempelvis indenfor egen organisation, erhvervssammenslutning, erhvervsorganisation eller lignende jf. § 4c, stk. 2, nr. 4. Det er ikke tilstrækkeligt, at det lukkede forum er en lukket gruppe på et socialt medie eller andre hjemmesider, idet det kræver et lukket forum på et intranet. Det er desuden et krav, at der er én eller flere fagpersoner, der vurderer, hvorvidt de indgivne materialer fra virksomhederne må deles med de andre personer, før det bliver delt. Materialet må kun være tilgængeligt for de relevante virksomheder og den systemansvarlige.[178]

Den systemansvarlige skal indhente tilladelse fra Datatilsynet, før der må ske videregivelse jf. § 4c, stk. 3. Datatilsynet vil foretage en konkret vurdering, herunder forholdet mellem privatlivets fred og formålet med videregivelse.[179]

[174] Tv-overvågningsloven, Karnovs noter, nr. 49
[175] Tv-overvågningsloven, Karnovs noter, nr. 52
[176] Tv-overvågningsloven, Karnovs noter, nr. 53
[177] Tv-overvågningsloven, Karnovs noter, nr. 54
[178] Tv-overvågningsloven, Karnovs noter, nr. 56
[179] Tv-overvågningsloven, Karnovs noter, nr. 60

Optagelserne må som udgangspunkt opbevares i op til 30 dage jf. § 4c, stk. 4, medmindre der er tale om en konkret tvist eller såfremt det bruges i forbindelse med kriminalitetsforebyggelse jf. artikel 4c, stk. 5. Der må kun opbevares data om den pågældende gerningsperson, og såfremt der er overskudsinformation i form af andre personer, skal disse anonymiseres.[180] Den registrerede som tvisten omhandler, skal indenfor 30 dage underrettes om registreringen, efter bestemmelserne i forordningens artikel 14.[181] Hvis denne ønsker en kopi, skal den dataansvarlige udlevere dette.[182]

3.3 Biometriske datas anvendelse ved tv-overvågning

Der er flere high-end forretninger, der anvender biometriske data til at spotte kunder, der er medlem af forretningernes VIP loyalitetsprogram og kasinoer. På den måde kan medarbejderne i forretningen blive opmærksomme på disse kunder, når de kommer ind. Dette er som led i den ekstra kundeservice, som VIP kunderne skal have.[183]

En anden måde de to teknologier kan anvendes på, er ved kriminaltekniske formål. Som tidligere nævnt i afsnit 3.1 er gang- og bevægelsesmønster også biometriske data.

3.3.1 Ansigtsgenkendelse

Ansigtsgenkendelse anvendes ofte til formål, hvor der er mange mennesker tilstede, da det ved hjælp af denne teknologi er muligt at identificere eller verificere personer på kort tid. Dette kaldes en 1:N identifikation, dog kan den også anvendes til 1:1 verifikation, hvor de biometriske data alene bliver sammenholdt med én registreret. I forhold til nærværende afhandling, vil 1:1 ikke være relevant. Ansigtsgenkendelse kan anvendes ved allerede opsatte overvågningskameraer, og det kræver derfor ikke specialfremstillede kameraer til formålet.[184]

Ved ansigtsgenkendelse vil ansigtet blive målt ud fra ca. 80 forskellige punkter i ansigtet, herunder længde mellem øjne, bredden på næsen, hvor dybt øjnene sidder inde og meget andet. Disse

[180] Tv-overvågningsloven, Karnovs noter, nr. 64
[181] Tv-overvågningsloven, Karnovs noter, nr. 65
[182] Tv-overvågningslovens § 4c, stk. 5
[183] https://www.itgovernance.eu/blog/dk/gdpr-ting-at-tage-hensyn-til-ved-bearbejdning-af-biometriske-data, afsnit: bearbejdning af biometriske data, d. 20/11-2018
[184] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 52

punkter vil blive omdannet til nogle tal som udgør en kode, hvilket er de registrerede biometriske data. Ansigtsgenkendelsesteknologien kan genkende ansigter fra en maksimal vinkel på 35°, hvorefter målingerne vil omdannes til et standardiseret format. Når overvågningskameraet registrerer et ansigt, vil der blive skabt en unik digital kode ud fra scanningen af ansigtet, hvilket muliggør en sammenligning af den allerede registrerede kode i databasen med den nye kode. Der bliver skabt en såkaldt template, der sammenlignes med de allerede eksisterende koder fra de registrerede. Såfremt de to koder er tilnærmelsesvis ens, vil en fysisk person sammenligne de to koder for at sikre, at de to registrerede koder kan henføres til den samme person. [185]

Teknologien kan anvendes til en hurtig identifikation og tilnærmelsesvis sikker identifikation af personer. En ulempe ved teknologien er dog, at den kan have svært ved at genkende de registrerede personer i tilfælde af ændringer af og omkring ansigtet, hvilket kan ske ved tilføjelse eller fjernelse af skæg, plastikoperationer, huer, hatte og lignende. Derudover er der en stor risiko for, at der kan ske misbrug af teknologien ved at overvåge personer uretmæssigt, idet teknologien kan anvendes på allerede opsatte overvågningskameraer eller almindelige overvågnings-kameraer.[186]

I en artikel fra Consumerreports fra 2015, bliver der redegjort for ansigtsgenkendelsesteknologiens anvendelse i forretninger, kasinoer, cruise skibe og kirker.

Forretningerne anvender biometriske data til ansigtsgenkendelses ved hjælp af overvågningskameraer i forretningerne. Dette sker på baggrund af samtykke fra deres kunder, som eksempelvis er medlem af en VIP klub. På denne måde kan medarbejderne fra forretningen se, at der kommer et VIP medlem ind, hvad personen hedder, et billede af personen fra overvågningskameraet, hvornår denne sidste har handlet, hvad der er handlet, alder og mange andre relevante oplysninger. Der kan på denne måde ydes en god service til kunden, som bliver mødt af en venlig ekspedient, der allerede kender navnet, og hvilke præferencer og shoppingvaner kunden har.[187]

Som nævnt anvendes ansigtskendelse på cruiseskibe, hvor blandt andet Disneys cruise skibe tager billeder af gæsterne under opholdet, hvorefter gæsterne ved hjælp af et Disney ID-kort, der

[185] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 52
[186] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 52-53
[187] https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1/, d. 22/11-2018

anvender ansigtsgenkendelse, kan finde alle de billeder, der er blevet taget af den pågældende person. På denne måde undgår gæsterne at skulle gennemse billederne af alle gæster.[188]

Nogle kirker anvender biometriske overvågningskameraer, for at kunne genkende de personer, der regelmæssigt kommer i kirken, da de kan være villige til at give et bidrag, eller hvis en person pludselig ikke længere kommer, kan kirken undersøge, om alt er vel.

3.3.2 Ganganalyse

Ved ganganalyse måles kropsbygning, gangrytme og skridtlængde. Det er derfor muligt på lang afstand og i mørke at genkende en registreret person. Analysen foretages ved at måle kroppen ud fra de ovennævnte faktorer i forskellige positioner fra siden. Her vil det blandt andet være, hvordan benene og fødderne er placeret i forhold til hinanden, og i hvilket tempo personen bevæger sig. De forskellige målepunkter vurderes sammen, hvorved et bevægelsesmønster kan fastlægges. En udfordring ved denne teknologi er dog, at overvågningskameraet skal filme fra den rette vinkel, for at kunne foretage en ganganalyse. Derudover kan bevægelsesmønstret ændres ved anderledes påklædning, eksempelvis stiletter i forhold til flade sko eller taske som påfører vægt og blødt eller hårdt underlag. Teknologien er ikke optimal i forhold til adgangskontrol, idet det bevægelsesmønstret kan ændres ved forskellige faktorer.[189] Denne type teknologi vil eksempelvis være optimal ved kriminalitetsopklarende sager, hvor der kan foretages yderligere efterforskning.

Kapitel 4 - Analyse

4.1 TechX

I dette kapitel behandles en case med den føromtalte teknologi, hvor både biometriske data og tv-overvågning anvendes i samme teknologi. Ved anvendelse af ansigtsgenkendelse, vil det være muligt at identificere de personer, der tidligere har begået tyveri og derved advare forretningerne om den pågældende person. Casen oprinder fra en iværksætter, der ønsker at udbyde teknologien

[188] https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1/, d. 22/11-2018
[189] Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, side 57

og en servicecentral til forretninger. Da virksomheden endnu ikke er etableret, kaldes denne part fremover for TechX.

TechX har endnu ikke taget stilling til de persondataretlige problemstillinger og er blot i opstartsfasen. Casen vil derfor blive behandlet i alle relevante henseende, uanset om produktet er i overensstemmelse med GDPR, eller at det allerede fra start kan fastlægges, at det strider mod forordningen. I de problemstillinger som TechX og forretningerne ikke er taget stilling til endnu, vil de krav som TechX og forretningerne skal opfylde blive nævnt.

4.2 Teknologiens formål

Formålet med teknologien er, at forretningerne skal have mulighed for at spotte tyve, så snart en person bevæger sig ind i forretningen. På denne måde kan personalet i forretningen være opmærksom på den pågældende person og derved forhindre eller formindske risikoen for tyveri. Mulige mistænkte genkendes ved ansigtskendelse. Ganganalyse anvendes ikke, idet dette kræver en omfattende registrering, hvis der ønskes en automatisk identifikation af personen. Analysen kan derimod anvendes efterfølgende i tilfælde af, at en person skal identificeres ud fra den almindelige overvågning. Der bliver lavet en scanning af alle personer, inden de går forbi kameraet og ind i butikken, for at kunne lave templates af hver person. Når en person begår tyveri i en af disse forretninger, vil de lagrede biometriske data blive sammenkoblet med informationen om, at denne person tidligere har begået tyveri i en forretning. Såfremt denne person igen bevæger sig ind i forretningen eller i en af de andre forretninger, der gør brug af TechX' overvågningskameraer, vil forretningen få en meddelelse om, at denne person har bevæget sig ind i forretningen. Jo flere forretninger der anvender overvågningskameraet, des større nytte har den for alle parter.

Det er ifølge tv-overvågningslovens § 4c, stk. 2, nr. 4 tilladt for forretninger at dele oplysninger om gerningspersoner eller formodede gerningspersoner i et lukket forum med andre forretninger, som oplysningen kan være relevant for i et kriminalitetsforebyggende øjemed. Dette er ganske almindelige billede- og lydoptagelser jf. tv-overvågningslovens § 4, stk. 1, hvorfor det må antages, at biometriske data ikke er omfattet. TechX har ikke behov for overvågningsoptagelserne for at kunne identificere formodede gerningspersoner, idet det alene er de biometriske data, der er nødvendige for at kunne identificere en formodet gerningsperson ud fra tv-overvågningen. TechX'

centrale service vil sidde og følge med live, idet dette er nødvendigt for at kunne meddele forretningerne om en formodet gerningsperson. Overvågningsoptagelserne er alene til efterfølgende identifikation, som det hidtil har været kendt. Der vil derfor i den videre behandling skelnes mellem, om det er de biometriske data eller overvågningsoptagelserne.

4.3 Oplysningstype

Overvågningskameraerne anvendes til at identificere personer på baggrund af ansigtsgenkendelse. Disse oplysninger er biometriske data jf. forordningens artikel 4, nr. 14 og reguleres i forordningens artikel 9, stk. 1 om følsomme oplysninger. Hvorvidt oplysningerne må behandles af TechX og forretningerne, vil blive analyseret nærmere i afsnit 4.5.

Udover de biometriske data, behandles der ligeledes oplysninger om personer, der tidligere har begået tyveri. Lovovertrædelser reguleres i forordningens artikel 10, hvoraf det fremgår, at behandlingen kun må foretages under kontrol af en offentlig myndighed, eller hvis der er hjemmel i EU-retten eller i national ret. Tv-overvågningsloven regulerer i en vis grad lovovertrædelser , herunder behandling og videregivelse af disse oplysninger jf. tv-overvågningslovens §§ 2, nr. 3 og 4c. Hvorvidt TechX og forretningerne har hjemmel til at behandle de forskellige oplysningstyper, vil blive analyseret nærmere i afsnit 4.5.

4.4 Dataansvarlig og databehandler

TechX er dem, der er i besiddelse af oplysningerne, ved at de lagrer dem i deres eget system. Forretningerne er dermed hverken i besiddelse af oplysningerne eller har adgang til dem. Forretningen er blot en kunde hos TechX, som tilbyder en sikkerhedsservice ved at overvåge butikkerne ved hjælp af deres eget udstyr.

Der er i denne case to parter, henholdsvis TechX og forretningerne som gør brug af overvågningskameraet og servicen. I vurderingen af om henholdsvis TechX og forretningerne er dataansvarlig eller databehandler, vil der blive lagt vægt på, *hvem* der fastlægger formålet for indsamlingen af oplysningerne, og hvilke hjælpermidler der anvendes, eksempelvis, hvem der må

behandle oplysningerne, og *hvem* der behandler oplysningerne ud fra instruktioner fra den dataansvarlige.[190]

Ved vurderingen af, hvorvidt en part er dataansvarlig, lægges der vægt på, hvem der bestemmer behandlingsformålet. Som nævnt i afsnit 3.5.1, er det alene TechX, der har adgang til og er i besiddelse af de registrerede data. Forretningerne kan siges at være i berøring af oplysningerne ved, at det er oplysninger, der indsamles i deres forretninger og i en vis grad kan det siges, at de køber produktet og servicen med et formål. I princippet kan TechX's produkt og service benyttes til andre formål end til at genkende formodede gerningspersoner. TechX har bestemt, at formålet med behandling af oplysningerne er at beskytte forretningerne mod tyveri. Formålet er altså at lagre de biometriske data med henblik på at identificere tidligere gerningspersoner, som er registreret i systemet. Der er ingen tvivl om, at TechX har fastlagt formålet. Det må dog også bemærkes at forretningerne, som tidligere nævnt, i en vis grad har indflydelse på formålet, idet de tilkøber produktet og servicen med formålet om at forebygge tyveri. Formålet kan siges at være fastsat i fællesskab af forretningerne og TechX, idet forretningerne får installeret produktet og indsamler disse med henblik at forebygge tyveri, mens TechX har udviklet produktet og tilbyder en service for at forebygge tyveri. Der kan henvises til EU-domstolens sag C-210/16 fra 5. juni 2018, hvor EU-Domstolen fastlægger, at der kan forekomme fælles dataansvar.

Derudover lægges der vægt på, hvem der bestemmer, hvordan personoplysningerne behandles, herunder hvilke *hjælpemidler* der anvendes, og hvem der behandler oplysningerne. Forretningerne har selv valgt, at de vil anvende TechX' biometriske kamera og service til at forebygge tyveri, hvilket må antages at være et hjælpemiddel. Samtidig har TechX udviklet produktet for at forebygge tyveri, hvilket også anses for at være et hjælpemiddel.

Det kan umiddelbart se ud til, at der forelægger et fælles dataansvar. Såfremt der er statueret et fælles dataansvar, er det vigtigt, at de dataansvarliges respektive roller fastlægges. Både for deres indbyrdes tilrettelæggelse af arbejde og ansvar, og for at de registrerede på en gennemsigtig måde kan skabe et overblik over, hvem der er ansvarlige for de forskellige opgaver. Herunder vil det være yderst relevant at fastlægge, hvem af de to parter, der er ansvarlig for modtagelse af

[190] Vejledning om dataansvarlige og databehandlere, side 5

anmodninger fra de registrerede, som ønsker at udnytte deres rettigheder, idet de dataansvarlige skal lette udøvelsen for den registrerede jf. GDPR artikel 12, stk. 2.

Når det vurderes, hvem der er databehandler, vil det være væsentligt at undersøge, hvem der behandler oplysninger på vegne af den dataansvarlige og under dennes instruktion. Ved behandling menes der, hvilken som helst form for berøring med oplysningerne. Det fremgår af artikel 4, nr. 2, at behandling eksempelvis kan være: "… *indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse"*[191]

I denne case sker der indsamling, opbevaring, søgning, brug, formidling og mange andre former for behandling. Der er derfor ingen tvivl om, at der sker en behandling af oplysningerne. Idet det antages at både TechX og forretningerne er dataansvarlige, og der ikke er andre parter, som er i berøring af oplysningerne, er det ikke nødvendigt at vurdere, hvem der er databehandler.

Delkonklusion dataansvarlig og databehandler

TechX fastlægger formålet ved at udvikle produktet med henblik på at forebygge tyveri, mens forretningernes formål ligeledes er at forebygge tyveri, hvilket de vælger at gøre med TechX's produkt. Produktet kan anvendes til andre formål, men idet begge parter anvender produktet til at forebygge tyveri, anses forretningerne og TechX for at have fastsat formålet i fællesskab. Det kan heraf udledes, at der muligvis kan foreligge et fælles dataansvar mellem TechX og forretningerne. Det antages videre, at der er to dataansvarlige, og det er derfor vigtigt at fastlægge de to dataansvarliges ansvarsområder, idet der skal være gennemsigtighed. Det skal være muligt for den registrerede at udnytte deres rettigheder, uden det er en besværlig proces. De dataansvarlige skal sørge for at lette udøvelsen ved at fastlægge, hvem af de dataansvarlige, der skal modtage anmodninger fra de registrerede.

[191] GDPR artikel 4, nr. 2

4.5 Behandlingshjemmel

Der er i denne case tale om biometriske data, hvilket er en følsom oplysning og derfor omfattet af bestemmelser i forordningens artikel 9. Det er, som tidligere nævnt, som udgangspunkt forbudt at behandle biometriske data jf. forordningens artikel 9, stk. 1. Det er derfor afgørende, at mindst én af undtagelserne i artikel 9, stk. 2 er gældende. Behandlingshjemlen for biometriske data skal derfor findes i artikel 9, stk. 2, litra a-j.

4.5.1 Tv-overvågning

I forhold til behandlingshjemlen for de almindelige overvågningsoptagelser, er det tv-overvågningsloven, der er gældende. Behandlingshjemlen findes i tv-overvågningslovens § 2, stk. 1, nr. 3 og 4. Forretningerne skal tydeligt skilte med, at der foretages tv-overvågning jf. tv-overvågningslovens § 3. Såfremt TechX og forretningerne opbevarer optagelserne, skal de som udgangspunkt slettes indenfor 30 dage fra optagelserne er foretaget jf. tv-overvågningslovens §4c, stk. 4. Det er ikke nødvendigt at tage stilling til de almindelige optagelser i resten af afsnittet, idet hjemlen allerede er fundet.

4.5.2 Samtykke

Forordningens artikel 9, stk. 2, litra a kræver *udtrykkeligt* samtykke fra den registrerede til ét eller flere specifikke formål. Det vil sige, at samtykket skal være klart og utvetydigt.[192] Der må altså ikke være tvivl om, at der foreligger et samtykke til behandlingen af de registreredes biometriske oplysninger. Derudover fremgår det af præambelbetragtning nr. 32, at samtykke ikke kan afgives ved tavshed, passivitet og forud afkrydsede felter.[193] For at TechX kan anvende deres overvågningskamera og indsamle biometriske data, kræves udtrykkeligt samtykke fra samtlige personer, der registreres oplysninger om. Det vil sige, at der skal være samtykke fra hver enkelt person, der går forbi kameraet og ind i forretningen.

For at indhente samtykke kræver det som sagt, at det sker ved en aktiv handling. Det er ikke nok, at det er anført på et skilt, at forretningen overvåges, og at det er biometriske data, der registreres. Hvis det alene havde været et almindeligt overvågningskamera, ville det være

[192] Betænkning nr. 1565 om forordningen, side 210
[193] GDPR præambelbetragtning nr. 32

tilstrækkeligt at skilte med informationer vedrørende dette.[194] Samtykket kan eksempelvis indhentes ved at installere en skærm, hvor hver forbipasserende kunde skal læse en privatlivspolitik, hvor de påkrævede informationer ifølge forordningens artikel 13, om den dataansvarliges oplysningspligt er anført, hvorefter de aktivt skal give et samtykke ved at afkrydse en boks. For at dette på nogen tænkelig måde skal være realistisk, kræver det muligvis, at der ikke er adgang til det tv-overvågede område, før privatlivspolitikken er læst, og der er givet et aktivt samtykke. Hvorvidt dette i praksis er muligt at gennemføre er tvivlsomt. Det må antages at være umuligt for TechX og forretningerne at indhente samtykke fra samtlige kunder, der bevæger sig ind i forretningen, idet en person der påtænker at begå tyveri, aldrig ville give sit samtykke, og mange ikke ville ønske at bruge tid på at læse alt teksten og registrere deres biometriske oplysninger. Ved anvendelse af ansigtsgenkendelse, vil det være nødvendigt at opbevare oplysninger om personer, der har begået tyveri, for at overvågningskameraerne kan identificere en registreret person. Oplysningerne vil alene være mulige at indsamle, ved at personen nægtes adgang til forretningen uden at disse oplysninger afgives. Hvis samtykke opnås ved at nægte adgang, er samtykket imidlertid ikke "*... i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljetilkendegivelse ...*" og dermed ikke et gyldigt samtykke.[195]

Hvis ikke kunderne giver deres samtykke, og modtager de informationer som TechX og forretningerne har pligt til at oplyse om, er behandlingen ikke lovlig, medmindre der findes hjemmel i en anden af bestemmelserne i forordningens artikel 9, stk. 2, litra a-j.

4.5.3 Nødvendig af hensyn til retskrav

TechX og forretningerne kan behandle biometriske data, såfremt det er nødvendigt af hensyn til at fastlægge, forsvare eller gøre et retskrav gældende. Ved tyveri vil det være muligt at identificerer den registrerede ved hjælp af systemet. Der kan være en fordel ved at anvende ansigtsgenkendelse i forhold til almindelige overvågning, idet gerningspersonen ikke med sikkerhed kan identificeres ved almindelig overvågning. Dette er dog den mest udbredte metode i Danmark, hvilket i de fleste tilfælde fungerer fint. Formålet er imidlertid ikke, at gerningspersoner skal genkendes, men overvågningen med ansigtsgenkendelse skal fungere forebyggende. TechX og

[194] Tv-overvågningsloven § 3

[195] GDPR præambelbetragtning nr. 32

forretningerne kan derfor have svært ved at påvise nødvendigheden af at anvende biometrisk overvågning.

Delkonklusion af behandlingshjemmel

Der er hjemmel til behandling af almindelig tv-overvågning i tv-overvågningslovens § 2, nr. 3.

I praksis vil det være udfordrende, hvis ikke umuligt at opnå samtykke, idet personer der påtænker at begå tyveri, ikke vil give deres samtykke, og andre personer muligvis ikke vil ønske at bruge tid på at gennemlæse informationerne og registrere deres biometriske data.

Af hensyn til at forsvare, fastlægge eller gøre et retskrav gældende, skal TechX og forretninger påvise at behandlingen er nødvendig. Idet almindelig tv-overvågning fungerer fint i Danmark, vil det være problematisk at påvise, at det er nødvendigt med så indgribende en metode.

Det vurderes derfor, at samtykke er den eneste mulighed for at behandle oplysningerne. TechX og forretningerne vil ikke være omfattet af de andre betingelser, og det vil derfor kræve en tilladelse fra kunderne, der vil blive registreret med deres personoplysninger. Hvis der skal opnås samtykke fra samtlige kunder, skal der først gives adgang til forretningen, såfremt kunden har taget stilling til, om denne vil lade sig registrere. Dette vil ikke i praksis være muligt, idet forretningerne derved sandsynligvis vil miste deres kunder.

Det antages derimod i den videre analyse, at der opnås behandlingshjemmel ved samtykke, på trods af de udfordringer der kan opstå, idet analysen ellers ikke kan fortsætte.

4.6 Grundlæggende behandlingsprincipper

Databeskyttelsesforordningens artikel 5 indeholder nogle generelle betingelser for behandling af personoplysninger, som altid skal overholdes. Dette gælder uanset, hvilken type personoplysninger det er. Behandling af personoplysninger skal altid behandles i overensstemmelse med princippet om god databehandlingsskik.[196]

[196] Betænkning nr. 1565 om forordningen, side 81

4.6.1 Lovlighed, rimelighed og gennemsigtighed

Personoplysninger skal behandles med "*lovlighed, rimelighed og gennemsigtighed*".[197] Som tidligere nævnt, skal disse betingelser altid opfyldes ved behandling af personoplysninger.

Ved *lovlighed* menes, at personoplysningerne skal behandles ud fra en behandlingshjemmel. Behandlingen omhandler blandt andet biometriske data med henblik på identifikation, hvilket er en følsom oplysning, hvorfor det vil være betingelserne i forordningens artikel 9, stk. 2 litra a-j, der vil finde anvendelse. Det kunne udledes i afsnit 4.5.2, at der kan ske behandling på baggrund af samtykke jf. forordningens artikel 9, stk. 2, litra a. Princippet om lovlighed er opfyldt for de biometriske data.

Derudover behandles der oplysninger om straffedomme og lovovertrædelser jf. forordningens artikel 10, hvilket dog behandles efter betingelserne i artikel 6, stk. 1, litra a-f. Disse oplysninger behandles af offentlige myndigheder eller under kontrol af en offentlig myndighed, hvorfor TechX som udgangspunkt ikke kan behandle disse oplysninger. Der er dog i tv-overvågningsloven hjemmel til behandling af oplysninger om straffedomme og lovovertrædelser, idet opbevaring og videregivelse er tilladt under visse forudsætninger oplistet i tv-overvågningslovens § 4c, stk. 2, nr. 1-4. Optagelserne videregives af formodede gerningspersoner i kriminalitetsforebyggende øjemed.

I forhold til oplysninger om almindelig tv-overvågning, er der hjemmel i tv-overvågningslovens § 2, nr. 3, hvorefter oplysningerne behandles ifølge forordningens bestemmelser.

Der er som sagt ikke en liste over, hvilke overvejelser der bør danne grundlag for, om en behandling af personoplysninger er *rimelige*. Hvorvidt behandlingen er rimelig, må betragtes ud fra en overordnet vurdering af sagen i forhold til de givne informationer jf. forordningens artikel 13, stk. 2 og 14, stk. 2.

Gennemsigtighed er et princip som, at den registrerede skal have et indblik i, hvilke formål dennes oplysninger anvendes til og hvordan de behandles. I præambelbetragtning 39 fremgår det: "*Princippet om gennemsigtighed tilsiger, at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart*

[197] GDPR artikel 5, stk. 1, litra a

og enkelt sprog".[198] Den dataansvarlige skal på denne baggrund sikre, at den registrerede forstår de modtagne informationerne og det er udformet på en lettilgængelig og letforståelig måde. Det antages at der opsættes skærme ved indgangen, hvor de påkrævede informationer vil fremgå, og hvor et eventuelt samtykke skal indhentes efterfølgende. Dette må anses for at være en lettilgængelig metode, omstændighederne taget i betragtning. Denne metode vil dog være tidskrævende for kunderne i forretningerne, idet det vil tage tid at læse det og derefter lave templates ud fra en scanning af ansigtet. Dette er dog den eneste måde at gøre det på, hvis det skal være lettilgængeligt, idet oplysningerne skal gives samtidig med indsamlingen. Derudover skal det være letforståeligt, hvilket vil sige, at der skal anvendes et klart og enkelt sprog. Der må ikke være overflødige informationer, der gør det svært for den registrerede at gennemskue, hvad formålet med de givne informationer er. Dette kan TechX og forretningerne gøre ved at inddele teksten i afsnit og anvende korte og præcise sætninger.

Nogle af de relevante faktorer, som sikrer gennemsigtighed, vil blive behandlet nærmere i de følgende afsnit.

Delkonklusion grundlæggende behandlingsprincipper

De grundlæggende principper, der altid skal være opfyldt, er lovlighed, rimelighed og gennemsigtighed.[199] TechX og forretningerne opfylder delvist kravet til lovlighed, idet de biometriske data kan behandles jf. forordningens artikel 9, stk. 2, litra a og almindelig tv-overvågning kan behandles jf. tv-overvågningslovens § 2, nr. 3. Oplysninger om straffedomme og lovovertrædelser kan dog ikke behandles, idet dette skal foretages af en offentlig myndighed eller under kontrol af denne. Der er dog i en vis grad hjemmel til behandling af oplysninger om straffedomme og lovovertrædelser i form af opbevaring og videregivelse af oplysninger i kriminalitetsforebyggende øjemed jf. tv-overvågningslovens §§ 2, nr. 3 og 4c, stk. 2. TechX må siges at videregive oplysninger om formodede gerningspersoner i kriminalitetsforebyggende øjemed. Udfordringen er dog, at det er TechX, der videregiver oplysningerne og ikke den erhvervsdrivende selv, som er forretningerne.

[198] GDPR præambelbetragtning nr. 39
[199] GDPR artikel 5, stk. 1, litra a

TechX kan teoretisk set opfylde princippet om gennemsigtighed ved at give informationer til den registrerede på en kort og præcis måde, eventuelt opdelt i punkter, for at kommunikationen og viderebringe informationer på en lettilgængelig og letforståelig måde. Informationerne kan eventuelt viderebringes ved en privatlivspolitik. I praksis vil det være udfordrende at kommunikere og viderebringe informationer på en gennemsigtig måde.

4.6.2 Formålsbegrænsning

Hvorvidt oplysninger om den resterende del af de registrerede, som ikke har begået tyveri, vil blive anset for at være lagret med henblik på "nice-to-have-informations" kan diskuteres. Oplysningerne kan være lagret i tilfælde af, at de registrerede kunder, der ikke har begået tyveri, eventuelt på et senere tidspunkt kan begå tyveri, hvorved disse oplysninger muligvis falder ind under formålet. Dette vil ikke blive anset for at være tilstrækkelig registrering af data, idet der skal opbevares store mængder data, som ikke kan anses for at blive opbevaret af nødvendighed for at opfylde formålet, som er, at forretningerne skal advares om tidligere gerningspersoner. Det kan ikke med sikkerhed siges, at en pågældende person på sigt kan begå tyveri, hvorfor det er i strid med forordningens principper om formålsbegrænsning at behandle oplysninger om de resterende kunder.

Det kan være svært at vurdere, hvorvidt indsamlingen falder ind under formålet, idet oplysningerne vil blive behandlet fra det øjeblik, hvor den registrerede går ind foran overvågningskameraerne. De vil blive behandlet indtil den pågældende person igen kommer ud. Her kan der eventuelt sikres en automatisk sletning, såfremt personen ikke har begået tyveri. Hvis oplysningerne slettes og det senere opdages, at pågældende person har begået tyveri, vil sletning ikke være i overensstemmelse med formålet. Spørgsmålet er herefter, hvorvidt det er i overensstemmelse med forordningen at opbevare oplysninger i en given tidsperiode for at afvente eventuelle tilbagemeldinger om tyveri. Ifølge tv-overvågningsloven, må videoovervågning opbevares i 30 dage, hvorefter de skal slettes. Dette er imidlertid kun gældende for almindelig overvågning. I TechX' tilfælde, er der samtidig tale om behandling af biometriske data, der er en følsom oplysning, hvormed der medfølger et stort ansvar idet misbrug af disse oplysninger kan medføre alvorlige konsekvenser for den registrerede.

Oplysningerne skal registreres i systemet, før det er muligt at identificere formodede gerningspersoner. Det vil ikke være muligt at indhente samtykke fra en gerningsperson efterfølgende, hvorfor det er nødvendigt at indsamle oplysningerne på forhånd. Den næste problemstilling er, hvorvidt kunderne vil give deres samtykke til behandling af oplysningerne.

TechX skal foretage en formålsbegrænsning ved at slette de overflødige oplysninger. Dette kan eksempelvis gøres ved, at kundens biometriske data registreres, når denne bevæger sig ind i forretningen. Når kunden igen kommer ud af forretningen, kan oplysningerne ved hjælp af Privacy By Design automatisk blive slettet fra TechX's centrale system, hvilket dog vil kræve nogle ændringer i produktet fra TechX's side. Det ændrer dog ikke på, at oplysningerne stadig behandles i tidsrummet fra indsamlingen til at kunden kommer ud igen. Dette giver naturligvis også udfordringer i det tilfælde, hvor en gerningsperson ikke bliver opdaget med det samme.

Delkonklusion formålsbegrænsning

TechX skal formålsbegrænse behandlingen ved, at der ikke opbevares oplysninger om andre registrerede end de formodede gerningspersoner. Disse oplysninger er overflødige, og det er derfor ikke nødvendigt at opbevare disse, idet det ikke vedrører formålet med behandlingen. Dette kan eventuelt gøres ved Privacy By Design, hvor systemet indstilles til, at de overflødige oplysninger slettes, når kunden går ud af forretningen. Det anses dog stadig for behandling, idet der bliver indsamlet oplysninger og dermed behandles disse, indtil kunden kommer ud igen.

4.6.3 Dataminimering og proportionalitet

For de almindelige overvågningsoptagelser gælder, at overskudsinformation ikke må opbevares, hvorfor alle andre personer end de formodede gerningspersoner skal anonymiseres.[200] De optagelser der opbevares i 30 dage eller derover på baggrund af andre legitime grunde, skal derfor anonymiseres i forhold til de personer, som ikke er omfattet af baggrunden for at opbevare optagelserne. I dette tilfælde er der udover de almindelige optagelser også biometriske oplysninger. De udarbejdede templates må, ifølge princippet om dataminimering, alene omfatte de formodede gerningspersoner, idet de templates der vedrør de andre personer må anses som "nice-to-have" informationer.

[200] Tv-overvågningsloven, Karnovs noter, nr. 64

TechX og forretningerne indsamler oplysninger om hver enkelt kunde, der bevæger sig ind i forretningen. Der vil derfor blive behandlet følsomme oplysninger om utallige mennesker. Formålet med produktet og servicen er, at registrerede der tidligere har begået tyveri, der skal kunne identificeres i systemet. Det vil derfor i princippet være tiltrækkeligt alene at behandle oplysninger om disse personer. Behandling af oplysninger om den resterende del af kunderne, som ikke har begået tyveri, vil ifølge artikel 5, stk. 1, litra c være i strid med princippet om dataminimering. Ved indsamling af disse enorme mængder af data, også kaldet Big Data, vil størstedelen af dem ikke være relevante for formålet med indsamlingen. Oplysningerne er ikke relevante, idet formålet er, at forretningerne skal have mulighed for at være opmærksomme på tidligere gerningsmænd. I ordlyden af forordningens artikel 5, stk. 1, litra c nævnes det blandt andet, at oplysningerne skal begrænses til det, der er nødvendigt for at kunne opfylde formålet. Oplysninger er ikke nødvendige at opbevare, da disse personer ikke er nødvendige at genkende på overvågningen i forhold til formålet om, at formodede gerningspersoner skal identificeres. Indsamling af biometriske data om alle de kunder, der går ind i forretningerne, kan derfor ikke anses for at være proportionalt, idet der er mindre indgribende metoder at tage i brug. Problemstillingen ved indsamlingstidspunktet er dog, at det ikke er muligt at forudse, hvem af kunderne der vil begå tyveri, og det er ikke muligt at opnå samtykke til at indsamle biometriske data efterfølgende, idet en gerningsperson aldrig ville tillade dette. Opbevaringen af oplysningerne kan dog muligvis begrænses til kun at omfatte de formodede gerningspersoner efter indsamlingen. Dette vil blive undersøgt nærmere i afsnit 4.6.5.

Delkonklusion dataminimering og proportionalitet

TechX og forretningerne indsamler oplysninger om alle de kunder, der går ind i forretningerne. Der vil derfor blive opbevaret enorme mængder af data, som ikke er nødvendige for at opfylde formålet med behandlingen. Det er kun nødvendigt at opbevare data om de formodede gerningspersoner, idet formålet er at forebygge tyveri i forretningerne. Formålet er ikke muligt at opnå på en mindre indgribende måde i første omgang, idet en gerningsperson ikke vil give sit samtykke til behandling af personoplysninger efterfølgende.

4.6.4 Rigtighed

I forhold til biometriske data sker der normalvis ikke betydelige ændringer, idet oplysningerne er biologisk bestemt. Der kan dog i særlige tilfælde være grundlag for at ajourføre dem, hvis en registreret har fået foretaget plastikkirurgiske indgreb, og der derved er sket en ændring i de punkter og mål, som de biometriske målinger er skabt ud fra. TechX vil være nødt til at foretage nye scanninger af ansigtet for at kunne berigtige oplysningerne eller slette dem, idet der ikke må opbevares urigtige oplysninger. Såfremt den registrerede ønsker oplysningerne slettet, skal dette foretages, idet oplysningerne er indsamlet på baggrund af samtykke. Der vil ikke være andre legitime grunde til at kunne behandle oplysningerne. De almindelige optagelser kan dog som udgangspunkt opbevares i 30 dage fra indsamlingen jf. tv-overvågningslovens § 4c, stk. 4, idet der ikke er biometriske data forbundet med de almindelige overvågningsoptagelser og dermed heller ingen urigtige oplysninger. Hvis TechX videregiver optagelser af formodede gerningspersoner, som senere har vist sig ikke at have begået tyveri, eller ikke er den rigtige person, vil der være tale om urigtige oplysninger, som skal slettes.

Delkonklusion rigtighed

TechX vil alene i få tilfælde være i besiddelse af urigtige oplysninger i forhold til biometriske data, idet disse ikke umiddelbart ændres. Der kan dog forekomme ændringer i ansigtets biometri i tilfælde af alvorlige ulykker eller plastikkirurgiske indgreb. I så fald skal oplysningerne slettes eller berigtiges. Urigtige oplysninger kan forekomme ved de almindelige optagelser, ved at der behandles eller videregives oplysninger om forkerte personer, eller en formodet gerningsperson ikke er skyldig.

4.6.5 Opbevaringsbegrænsning

Det fremgår af forordningens artikel 5, stk. 1, litra e, at det ikke er tilladt at opbevare personoplysninger, hvor det er muligt at identificere den registrerede, længere tid end nødvendigt. TechX og forretningernes formål er at opbevare oplysninger i en lang periode, idet det ikke kan forventes, at en gerningsperson nødvendigvis vil begå tyveri igen indenfor en kort periode. Formålet er at oprette en database, hvor formodede gerningspersoner kan identificeres. Det er derfor nødvendigt for de dataansvarlige at opbevare de biometriske oplysningerne i en lang periode. Det er dog ikke alle de indsamlede oplysninger, der er nødvendige at opbevare, idet de

registrerede, som ikke er formodede gerningspersoner, ikke er nødvendige at identificere på et senere tidspunkt. Det er alene nødvendigt at opbevare templates på de formede gerningspersoner, hvorfor de dataansvarlige skal slette de resterende registrerede kunder.

Det fremgår af tv-overvågningsloven, at overvågningsoptagelser som udgangspunkt skal slettes indenfor en frist på 30 dage jf. § 4c, stk. 4. TechX kan opbevare oplysningerne i mere end 30 dage jf. tv-overvågningslovens § 4c, stk. 5, hvis det er i forbindelse med en konkret tvist, hvilket det vil være, hvis en gerningsperson bliver stoppet eller opdaget. Oplysninger kan ligeledes opbevares i en længere periode end 30 dage, hvis behandlingen sker i kriminalitetsforebyggende øjemed jf. tv-overvågningslovens § 4c, stk. 2[201], hvilket det vil være, hvis en gerningsperson gentagne gange begår tyveri eller ved et af de andre tilfælde, som er nævnt i tv-overvågningslovens § 4c, stk. 2. Det er dog essentielt, at det alene er de personer den konkrete tvist omhandler, der kan identificeres på optagelserne, mens de resterende personer skal anonymiseres, hvilket fremgår af artikel 5, stk. 1, litra c.

Delkonklusion opbevaringsbegrænsning

For TechX og forretningerne er det nødvendigt at opbevare oplysningerne i en lang periode, idet formålet er, at identificere formodede gerningspersoner. Det kan dog være svært at sige, hvor lang tid, det er nødvendigt at opbevare oplysningerne, idet forretningerne i hele den periode de eksisterer, har brug for at kunne identificere personerne. Det er ikke i TechX's og forretningernes tilfælde muligt at gøre de biometriske data uidentificerbare, idet hele formålet er at identificere formodede gerningspersoner.

De almindelige optagelser må opbevares i 30 dage, hvorefter de skal slettes jf. tv-overvågningslovens § 4c, stk. 4. TechX og forretningerne kan dog opbevare oplysningerne i en længere periode, idet det er muligt for dem, at opfylde betingelserne i tv-overvågningslovens § 4c, stk. 2 og oplysningerne kan ligeledes opbevares ved en konkret tvist.

4.6.6 Integritet og fortrolighed

Princippet om integritet og fortrolighed skal sikre, at der er foretaget tilstrækkelige foranstaltninger i forhold til behandlingssikkerheden. De dataansvarlige kan sikre sig mod tab ved at lave en back-up af de indsamlede data, som skal sørge for, at der altid er en kopi af

[201] Tv-overvågningslovens § 4c, stk. 5

oplysningerne et andet sted. Derudover skal de sikre, at der ikke er uautoriserede, der får adgang til oplysningerne eller til at anvende de registrerede data. Dette kan ske ved et særligt sikret system eller adgangskoder. Derudover skal de sørge for, at uautoriserede ikke får adgang til back-up, eksempelvis ved at de opbevares et andet sted eller i et sikret lokale.

Delkonklusion integritet og fortrolighed

TechX kan sikre sig mod tab og uautoriseret adgang ved at lave en back-up af de lagrede data og eventuelt opbevare en back-up et andet sted eller i et aflåst lokale.

4.7 Gennemsigtighed

De indsamlede data bliver indsamlet direkte hos den registrerede, idet der er et fælles dataansvar, og både TechX og forretninger er dataansvarlige, og idet der ikke er andre parter, indsamles oplysninger direkte ved den registrerede, hvorfor forordningens artikel 13 anvendes. TechX og forretningerne skal som dataansvarlige oplyse den registrerede om nogle oplysninger som fremgår af forordningens artikel 13, stk. 2, for at sikre en rimelig og gennemsigtig behandling. I det tilfælde, at informationerne gives i form af en privatlivspolitik, skal TechX og forretningerne sikre sig, at den registrerede har modtaget informationerne før der gives adgang til forretningen. For at kunne indsamle de biometriske data, skal der laves en scanning af ansigtet. I samme proces kan der gives informationer til den registrerede ved en privatlivspolitik, der eventuelt skal godkendes for at sikre, at oplysningerne er modtaget. Informationerne skal gives til den registrerede ved indsamlingen ifølge forordningens artikel 13, stk. 1. For at sikre at den registrerede har modtaget oplysningerne, vil det muligvis være nødvendigt at give informationerne på en skærm, hvor de skal læse oplysninger, før de kan komme ind. Nogle af de informationer den registrerede skal modtage er kontaktoplysninger på TechX og den pågældende forretning, hvem der er dataansvarlig, og hvem af de dataansvarlige der skal kontaktes, hvilke rettigheder den registrerede har ifølge forordningens kapitel 3, og hvad formålet med indsamlingen og behandlingen er. Der skal gives uddybende forklaring på, hvad for nogle teknologier, der anvendes og hvilke oplysninger der behandles. Det skal derfor fremgå, at der anvendes ansigtsgenkendelse ved hjælp af biometri til

identifikation af formodede gerningspersoner og oplysninger om lovovertrædelser, hvorved der både behandles biometriske oplysninger og oplysninger om lovovertrædelser.[202]

Den registrerede skal informeres om, hvor længe oplysningerne opbevares og risiciene ved behandlingen. For de almindelige optagelser skal det anføres, at slettefristen er 30 dage jf. tv-overvågningsloven. Ved behandling af biometriske data er der en stor risiko forbundet, idet disse oplysninger ikke som udgangspunkt kan ændres eller ændres gennem livet. Denne risiko skal den registrerede oplyses om.

Delkonklusion gennemsigtighed

Oplysningerne indsamles direkte hos den registrerede og denne skal derfor have nogle informationer som er oplistet i forordningens artikel 13, stk. 2 for at sikre gennemsigtighed. Informationerne omfatter blandt andet kontaktoplysninger på TechX og den pågældende forretning, hvilke rettigheder den registrerede har ifølge forordningens kapitel 3, hvad formålet med indsamlingen og behandlingen er, slettefrister og risikoen forbundet med behandlingen. Det må antages, at TechX og forretningerne installerer en skærm, hvor alle de nødvendige informationer jf. forordningens artikel 13 fremgår på en klar og enkel måde. Såfremt alle kravene efter artikel 13 er opfyldt og informationen vises på en måde, hvor den registrerede modtager dem, må det anses for at være en rimelig og gennemsigtig behandling. Det er dog i realiteten en umulighed, at give denne information til alle kunder.

[202] Betænkning nr. 1565 om forordningen, side 244

Kapitel 5 – Konklusion og perspektivering

5.1 Konklusion

De persondataretlige udfordringer ved anvendelse af biometri i tv-overvågning er et endnu uafklaret område, og der er endnu ikke fastlagt praksis. Ved hjælp af casen "TechX" er problemformuleringen forsøgt besvaret.

Formålet i casen "TechX" er, at forebygge tyveri i forretningerne. Parterne er omfattet af et fælles dataansvar, idet de begge har fastlagt formålet, og at tv-overvågningen skal anvendes som hjælpemiddel for behandlingen og opnåelse af formålet.

TechX og forretningerne har behandlingshjemmel til at behandle og videregive de almindelige overvågningsoptagelser jf. tv-overvågningslovens henholdsvis §§ 2, nr. 3 og 4c, stk. 2. Behandling af lovovertrædelser i almindelighed vil ikke kunne foretages af TechX og forretningerne, da det alene er offentlige myndigheder, der kan behandle disse oplysninger.

I analysen kunne det afvises, at TechX og forretningerne kunne behandle oplysningerne på baggrund af et retskrav, idet de skal bevise, at behandlingen er nødvendig. Det vurderes ikke, at bevisbyrden kan løftes, idet almindelig tv-overvågning i dag anvendes sammenholdt med, at biometrisk overvågning er meget indgribende.

Samtykke kan derimod i teorien opnås, hvilket dog kræver, at hver enkelt kunde i forretningen ved indsamlingen skal oplyses om de i forordningens artikel 13 oplistede informationer, og at derudover skal foreligge *udtrykkeligt* samtykke. I praksis vil det ikke være muligt at opnå samtykke fra samtlige kunder. Personer der påtænker at begå tyveri, vil ikke give deres samtykke, mens andre kunder ikke vil give deres samtykke grundet det uforholdsmæssige tidsforbrug på at registrere ansigtsbiometrien og på gennemlæse en privatlivspolitik. Derudover må det antages, at der i Danmark stadig er en meget tilbageholdende holdning til biometri, idet danskerne ikke er vant til at disse oplysninger registreres hos private. Oplysninger om lovovertrædelser kan ikke behandles af private, hvorfor disse oplysninger ikke må sammenkobles med de biometriske data. Der kan i en vis grad være mulighed for at behandle disse oplysninger jf. tv-overvågningsloven, idet videregivelsen af overvågningsmateriale med gerningspersoner automatisk vil være

behandling af disse oplysninger. Allerede på disse to grundlag kan TechX og forretningerne ikke anvende denne teknologi i forretningerne.

Lovlighed, som er et af de grundlæggende behandlingsprincipper, kan ikke opfyldes, idet der principielt set ikke er behandlingshjemmel for behandling af de biometriske data, da samtykke i praksis ikke kan opnås. En anden sondring er, om en sådan overvågning er proportional. Biometrisk overvågning er en meget indgribende metode, og der vil være mulighed for at forebygge tyveri eller fastlægge, forsvare eller gøre et retskrav gældende ved en mindre indgribende metode, f.eks. almindelige tv-overvågning og opsætning af tyveridetektorer.

5.2 Perspektivering

The Social Credit System

The Social Credit System eller på dansk det kinesiske pointsystem er et system, der profilerer personer ud fra deres handlinger, omgangskreds, livsstil og mange andre faktorer. Hver enkelt borgere har et antal point, som gennem livet kan stige og falde alt efter deres opførsel og gerninger. Hver gang der foretages en god gerning, opnår borgeren point, mens pointene bliver fratrukket, hvis denne eksempelvis udfører en kriminel handling, eller omgås de forkerte personer. Hver eneste handling registreres ved hjælp af de snart 626 millioner overvågningskameraer der forventes at være i 2020, der anvender ansigtsgenkendelse. Den kinesiske befolkning har gennem tiden vænnet sig til, at dette er en normal livsstil, da de længe har været vant til at blive overvåget. Hvorvidt lignende tilstande kan opstå i Danmark er endnu uvist, men teknologien og anvendelsen af denne kunne pege i retningen af en udvikling, der kan muliggøre en lignende tilstand. Forordningens artikel 22 indeholder et forbud mod automatiske afgørelser. På nuværende tidspunkt vil det ikke være muligt at skabe lignende situationer som det kinesiske.[203]

[203] http://nyheder.tv2.dk/udland/2018-04-15-ekstrem-overvaagning-i-kina-alle-faar-point-for-deres-opfoersel, besøgt d. 22/11-2018

Litteraturliste

Afgørelser og domme:

- EU-Domstolen, sag: C-210/16
- Datatilsynet, Journalnummer: 2003-212-0143

Artikler:

- Tranberg, Charlotte Bagger: Biometriske personoplysninger. I: *Aalborg Universitet*, 1.1.2007.

Bøger:

- Blume, Peter: *Den nye persondataret Persondataforordningen*. 1. udg. Jurist- og Økonomforbundets Forlag, 2016.
- Munk-Hansen, Carsten: *Retsvidenskabsteori.* 1. udg. Jurist- og Økonomforbundets Forlag, 2014.
- Rienecker, Lotte og Peter Stray Jørgensen: *Den gode opgave.* 4. udg. Samfundslitteratur, 2012.
- Waaben, Henrik og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer.* 3. Udgave, 2. Oplag, 2017. Jurist- og Økonomforbundets Forlag, 2015.

Hjemmesider:

- https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1/, besøgt d. 5/12-2018
- https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/, besøgt d. 5/12-2018
- https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvornaar-behandler-du-personoplysninger/, besøgt d. 21/11-2018
- https://europa.eu/european-union/eu-law/legal-acts_da, besøgt d. 5/12-2018

- https://www.google.dk/search?biw=1432&bih=699&tbm=isch&sa=1&ei=TmsHXMSvLYP4wQKEtKXgAg&q=biometrical+data&oq=biometrical+data&gs_l=img.3..0i24.10335.14353..14748...0.0..0.162.1351.13j3.....0....1..gws-wiz-img.....0j0i67j0i30j0i19j0i5i30i19j0i30i19.NjxSVpT0JMU#imgrc=xlRGx9PrC9RZrM:, besøgt d. 5/12-2018
- http://nyheder.tv2.dk/udland/2018-04-15-ekstrem-overvaagning-i-kina-alle-faar-point-for-deres-opfoersel, besøgt d. 5/12-2018
- https://videnskab.dk/sporg-videnskaben/har-enaeggede-tvillinger-identiske-fingeraftryk, besøgt d. 5/12-2018

Love, bekendtgørelser, direktiver og forordninger:

- Europa-Parlamentet og Rådets direktiv af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (95/46/EF) (databeskyttelsesdirektivet).
- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679/EU)
- L 205 Forslag til lov om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger.
- Lovbekendtgørelse nr. 1190 af 11. oktober 2007 om tv-overvågning (tv-overvågningsloven)
- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer (persondataloven – *historisk*)
- Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

Vejledninger:

- Artikel 29-gruppen, *Retningslinjer vedrørende retten til dataportabilitet*, WP 242 rev. 01

- Teknologi-rådet, *Biometri – brug af biometriske teknologier i det danske samfund*, Teknologirådets rapport 2010/2
- Vejledning, Databeskyttelsesforordningen, 2017
- Vejledning om dataansvarlige og databehandlere, 2017