Udfordringer og muligheder ved behandling af biometriske oplysninger i form af fingeraftryk i et persondataretligt perspektiv

Challenges and possibilities in relation to processing biometric data consisting of fingerprints in a data protection perspective

Foto: Shutterstock.com

Kandidatspeciale ved Juridisk Institut, Aalborg Universitet

Udarbejdet af:	Katrine Niebuhr Poulsen (20123624) Trine Aaen (20136129)
Retsområde:	Persondataret
Vejleder:	Charlotte Bagger Tranberg
Afleveringsdato:	20-05-2019
Antal anslag:	137915

Abstract

It has become a reality that biometrics is part of our daily lives. Biometrics has gradually evolved from being used in specific areas of public authorities (for example, the police and the Immigration Office for purposes of law enforcement and control) to a solution, that simplifies everyday action such as payment.
One of the primary reasons for using biometric solutions is *convenience*. Our community is designed to be easy and convenient. Passwords and pin codes can be hard to remember, so the use of biometric solutions will often be an easier way to access protected information. Therefore, it is no surprise that biometrics has become so widespread.

The Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) has been a breakthrough for biometric personal data. Within the frames of the Regulation, the data controller is now more than ever before bound and obliged to comply and demonstrate compliance with the Regulation. These requests to the data controller are also a part of the term *accountability,* which is the key stone of the Regulation.

The main focus in this thesis is to examine which challenges and possibilities that exist when processing biometric data consisting of fingerprints, when the data controller has to secure a legitimate legal basis.

This thesis uses the legal dogmatic method to describe and analyse the existing law. It will be the main method used in the following. The thesis also uses the legal method when analysing decisions by The Danish Data Protection Agency and related Swedish case law. The thesis does not include Danish case law for the simple reason that there is no case law in the area.

In continuation of above, the thesis will account for general rules in the Regulation, including key provisions in article 5 and the legal basis for processing in article 6 and article 9. The Danish Data Protection Agency and its decisions paralleled to the Regulation will illustrate the consequence of processing biometric data for the purpose of uniquely identifying a natural person. In interaction with Swedish case law, it will also illustrate the proportionality assessment whether the intended purpose of processing biometric data could be achieved in a less intrusive way.

The conclusion of the thesis is, central parameters are absolutely essential in the assessment of whether processing biometric data is in compliance with the key provisions in article 5. For example, these parameters are storage in centralised or decentralized databases, whether a template or the like is stored, or the raw form of biometric data is stored. In addition, the analyse may indicate that the purpose of the processing has a certain significance for whether the processing can be considered to be proportional or not.

In closing, it is first known to us in the year of 2018 in Denmark that biometrics is used with focus on necessity in everyday life such as payment. An example of a current biometric

solution, *Fingopay by Nets Denmark A/S,* shows the prevalence of biometrics. It may be an expression that proportionality assessment has moved in such a way, that the storage location (central or decentralized) is not given the same weight in 2019. In any case, *Fingopay* is an excellent example of the fact that biometric solutions have become a reality in the future and a natural part of our daily lives.

Fremstillingens indhold

Kap. 1 Introduktion

1.1. Indledning

Det er for alvor blevet en realitet, at biometri er en del af vores dagligdag. Biometrien har gradvist udviklet sig fra at blive anvendt på specifikke områder af offentlige myndigheder (eksempelvis ved politiet og udlændingestyrelsen med behandlingsformål som retshåndhævelse og kontrol[1]) til en løsning, der simplificerer en hverdagshandling som eksempelvis betaling.
Fakta er, at anvendelsen af biometriske oplysninger tidligere var en omkostningskrævende teknologi modsat i dag, hvor teknologien er økonomisk overkommelig for de fleste. Eksempelvis er en fingeraftrykslæser billig at anskaffe.[2]
En af de primære begrundelser for at benytte biometriske løsninger er *bekvemmelighed*, også kaldet "convenience".[3] Vores samfund er indrettet sådan, at det skal være nemt og bekvemt. Passwords og pin-koder kan være svære at huske, hvorfor brug af biometriske løsninger ofte vil være en nemmere løsning til at få adgang til beskyttede oplysninger.

Det interessante ved anvendelse af biometri er netop, at det skaber et stort potentiale for samfundsudviklingen. Brug af biometri kan medvirke til at højne sikkerhedsniveauet - især, hvis biometriske oplysninger kombineres med passwords, pin-koder, ID kort eller lignende. Der er tale om et sikkert middel, fordi det er nøjagtige oplysninger. Men omvendt er det også et meget skrøbeligt middel, fordi de biometriske rådata netop ikke kan ændres igen som eksempelvis et password kan. Det kan derfor få fatale konsekvenser, hvis de biometriske oplysninger misbruges eller i det hele taget falder i de forkerte hænder. Derfor er det også væsentligt, at den dataansvarlige iagttager relevante regler og krav på området, når vedkommende ønsker at benytte en biometrisk løsning.

Der er med den gældende lovgivning, Europa-parlamentets og Rådets forordning (EU) nr. 2016/679 af 27. april 2016 strammet op for konsekvensen af at have overtrådt databeskyttelseslovgivningen, da databeskyttelse i højeste grad tages alvorligt. Som illustrerende eksempel kan det nævnes, at en bøde er gået fra at være et femcifret beløb til nu at være et ottecifret beløb ifølge forordningens art. 83.[4]

Anvendelsesområdet inden for biometrien ses at udvikle sig i en hastig fart, hvorfor det stiller strenge krav til reguleringen af behandling af biometriske personoplysninger.
I forordningen er kernen den dataansvarliges ansvarlighed (accountability), hvilket medfører, at den dataansvarlige må og skal demonstrere sin vilje gennem en række tiltag til at ville overholde og imødekomme forordningens regler. Den dataansvarlige er således forpligtet til at efterleve og påvise denne efterlevelse af reglerne.

[1] Kofod Olsen, Birgitte, Identifikationsteknologi og individbeskyttelse, 1998, side 122 ff.
[2] Artikel 29-gruppen, WP 193, 2012, side 2 og side 16.
[3] Teknologirådets anbefalinger om biometri, side 14.
[4] Blume, Peter, Persondataret årgang 2018, artikel nr. RR.8.2016.30.

Heri ligger også en forpligtelse for den dataansvarlige til at sikre sig, at der foreligger et legitimt behandlingsgrundlag. Det legitime behandlingsgrundlag omfatter iagttagelsen af, at behandlingen har et lovligt grundlag samt overholdelse af de grundlæggende principper i forordningens art. 5.

I fremstillingen vil læseren blive præsenteret for en uddybende og analyserende gennemgang af muligheder og udfordringer ved anvendelse af biometriske løsninger med fokus på fingeraftryk. Det er særligt interessant, fordi behandling af biometriske oplysninger med henblik på entydig identifikation af den registrerede nu er omfattet af art. 9 om de særlige kategorier af oplysninger med forordningens ikrafttræden.

1.2. Afgrænsning

Fokus i fremstillingen er biometriske oplysninger med udgangspunkt i brug af fingeraftryk. Brug af fingeraftryk som biometrisk løsning er den ældste og mest anvendte metode på nuværende tidspunkt.[5] Vi er bevidste om, at biometri er meget mere end det. Denne fremstilling ville blive for omfangsrig, såfremt alle biometriske løsninger ville skulle inddrages, herunder eventuelt i kombination med andre teknologiske løsninger såsom videoovervågning.

Fremstillingen vil tage udgangspunkt i forordningen og de relevante bestemmelser heri. I forbindelse med forordningens ikrafttræden, er der i 2018 kommet en dansk supplerende lov, lov nr. 502 af 23. maj 2018 (databeskyttelsesloven). Når den omtales supplerende, har det også den betydning for specialet, at den ikke anvendes, medmindre det i loven fremgår supplerende bestemmelser til behandling af biometriske oplysninger.

I fremstillingen tages udgangspunkt i de generelle regler i forordningen, herunder de grundlæggende principper i art. 5 og de mulige behandlingshjemler ved behandling af biometriske oplysninger i art. 6 og art. 9. I forlængelse heraf skal det nævnes, at ved beskrivelse af de grundlæggende principper i art. 5 kan det ikke undgås, at andre supplerende relevante bestemmelser inddrages. Disse inddrages blot kort og behandles ikke yderligere i specialet.

Derudover inddrages kravene for et gyldigt samtykke i art. 7 samt de indledende relevante bestemmelser om, hvad en personoplysning er, og hvornår der er tale om en behandling i forordningens forstand. Øvrige bestemmelser, såsom bestemmelser om de registreredes rettigheder, er altid relevante, når der behandles personoplysninger, og dermed også, når der behandles biometriske oplysninger. De vil dog ikke blive inddraget yderligere i fremstillingen, idet denne i så fald ville blive for omfangsrig.

I analysen inddrages udvalgte afgørelser fra Datatilsynet. Vi er bevidste om, at der foreligger flere afgørelser fra Datatilsynet, som omhandler behandling af biometriske oplysninger. De er dog ikke inddraget i analysen, fordi de ikke vil kunne bringe nyt ind i forhold til allerede inddraget afgørelser.

I fremstillingen inddrages ikke dansk retspraksis af den simple årsag, at der ikke findes retspraksis på området. Vi har i stedet valgt at inddrage svensk retspraksis som supplement til analysen. Vi er også her bevidste om, at der findes yderligere svensk retspraksis på området, men af samme årsag som ovenfor inddrages dette ikke.

[5] Artikel 29-gruppen, WP 193, 2012, side 20.

1.3. Problemformulering

Læseren af fremstillingen vil finde en gennemgang af udfordringerne og mulighederne ved anvendelse af biometriske løsninger herunder særligt med udgangspunkt i følgende problemformulering:

- Hvilke udfordringer og muligheder findes ved behandling af biometriske oplysninger i form af fingeraftryk, når den dataansvarlige skal sikre et legitimt behandlingsgrundlag?

1.4. Metode og retskilder

For at besvare specialets problemformulering er det nødvendigt at redegøre for de centrale bestemmelser i forordningen, herunder i lyset af behandling af biometriske personoplysninger. Til dette anvendes den retsdogmatiske metode, *de lege lata*. Med denne metode beskrives og analyseres gældende ret med formålet om at opnå ny viden gennem en metodisk, gennemsigtig og systematisk proces.[6]

Metodisk vil fremstillingen gå til værks ved at analysere den gældende retstilstand samt konsekvenserne af forordningens ikrafttræden for biometrien. Dette vil blive foretaget ved inddragelse af relevante retskilder, først og fremmest forordningen, idet den er primær retskilde, men også ved inddragelse af afgørelser fra Datatilsynet og relevant svensk retspraksis. Supplerende vil der, især i det indledende afsnit og i beskrivelsen af gældende ret, blive inddraget relevant faglitteratur samt vejledninger fra Artikel 29-gruppen.
Ved gennemgang af afgørelserne i fremstillingen vil den juridiske metode blive anvendt. Den juridiske metode kendes bedst fra den praktiske sammenhæng, hvor formålet er at nå frem til en afgørelse, når der tages stilling til et konkret retligt problem. Metoden kan bedst beskrives som en afvejning og efterfølgende sammenlægning af fakta og jus, der ender med at give et resultat.[7]
Slutteligt konkluderes på ovenstående, og dermed vil problemformulering blive forsøgt besvaret.

Da vægten i fremstillingen er at beskrive og analysere gældende ret ud fra gældende databeskyttelsesforordning og de relevante afgørelser fra praksis, fastslås det, at den retsdogmatiske metode danner grundlaget, hvortil den suppleres af den juridiske metode i kap. 4, hvor afgørelserne analyseres.

[6] Munk-Hansen, Carsten, Retsvidenskabsteori, 2018, side 204.
[7] Munk-Hansen, Carsten, Retsvidenskabsteori, 2018, side 193.

1.4.1. De anvendte kilder i fremstillingen

1.4.1.1. Databeskyttelsesforordningen

Forordning nr. 2016/679, der internationalt betegnes General Data Protection Regulation (deraf GDPR, som herefter referes til som forordningen), udgør størstedelen af en ny databeskyttelsespakke, som EU-kommissionen fremsatte forslag om tilbage den 1. januar 2012. Den blev vedtaget den 14. juni 2016, og trådte endeligt i kraft den 25. maj 2018. Hermed afløses det tidligere gældende databeskyttelsesdirektiv 95/46/EF.

Forordningen har til formål at beskytte personoplysninger, da den fastslår særligt gennem EU's Charter om grundlæggende rettigheder og traktaten om Den Europæiske Unions funktionsmåde, at databeskyttelse er en grundlæggende rettighed. I chartret og traktaten fastsættes det, at enhver har ret til beskyttelse af personoplysninger, som vedrører den pågældende person.[8]
Dette beskyttelsesbehov anses kun for større og i tiden mere efterspurgt, da den hastige teknologiske udvikling og globalisering har skabt flere nye udfordringer, når det angår beskyttelse af personoplysninger.[9]

Det følger af art. 288 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF), at der er forskel på, om et område reguleres ved et direktiv eller en forordning. En forordning er *"almengyldig"* og er direkte bindende og gælder umiddelbart i hver medlemsstat.
Det betyder, at forordningen er på niveau med andre nationale love i Danmark, hvorfor den må betragtes som værende en primær retskilde. I den forbindelse skal det også fastlægges, at forordningen danner rammen for denne fremstilling, hvorfor der ikke umiddelbart tages udgangspunkt i andre supplerende love hertil.

1.4.1.2. Artikel 29-gruppen

Artikel 29-gruppen var et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Gruppen blev nedsat ved art. 29 i direktiv 95/46/EF. Gruppen har bidraget til en vis harmonisering i mellem medlemsstaterne, men har ikke haft nogen kompetence i forhold til afgørelser.
Gruppen har siden 1997 bidraget med udtalelser og vejledninger, der rent metodisk ikke er bindende. Vejledninger er blot forslag og rådgivende ord, men langt hen ad vejen er de normerende, da disse følges.

Gruppen er efter forordningens ikrafttræden erstattet af Det Europæiske Databeskyttelsesråd, hvis formål er at sikre en ensartet anvendelse af forordningen.[10] Det betyder, at gruppen lever videre gennem dette råd, hvorfor gruppens vejledninger og retningslinjer stadig anses for at være et vigtigt fortolkningsbidrag til databeskyttelseslovgivningen.[11]

[8] Forordning 2016/679, præambel nr. 1.
[9] Forordning 2016/679, præambel nr. 6.
[10] Forordning 2016/679 art. 70, stk. 1.
[11] Blume, Peter, Den nye persondataret, 2018, side 16.

1.4.1.3. Teknologirådet

Ifølge lov nr. 375 af 14. juni 1995 om Teknologirådet var rådet en selvejende institution, hvis opgaver blandt andet var at følge den teknologiske udvikling, udarbejde helhedsvurderinger af teknologiens muligheder og konsekvenser for samfundet, og formidle resultatet til Folketinget, samfundets øvrige politiske beslutningstagere og den danske befolkning med formålet om at støtte og fremme en teknologisk debat.[12]

Teknologirådet blev ophævet som offentligt råd ved lov nr. 79 af 2011/1 om ophævelse af lov om Teknologirådet og ændring af lov om Det Etiske Råd. Herefter har rådet fungeret *som en privat, almennyttig fond, som fortsat skal kunne arbejde for og i samspil med beslutningstagere på alle niveauer i samfundet, herunder Folketinget.*[13]

Inddragelse af Teknologirådets anbefaling sker på baggrund af, at formålet med udarbejdelsen af omtalte har været at vurdere, hvilke fordele og ulemper udbredelsen af biometriske løsninger skaber, hvilket ses at være i overensstemmelse med denne fremstillings problemformulering.[14]

1.4.1.4. Retspraksis

Der er tradition for at betragte retspraksis som en egentlig retskilde, hvorfor det er naturligt at overveje i nærværende fremstilling, hvorvidt retspraksis kan inddrages ved besvarelse af opgavens problemfelt.
Det har dog vist sig i søgningen efter relevant dansk retspraksis, at der endnu ikke foreligger dansk retspraksis, som har relevans for nærværende fremstilling. Det er i fremstillingen derfor valgt at inddrage svensk retspraksis, idet dagældende direktiv 95/46/EF og ligeledes forordningen naturligvis finder anvendelse i andre nordiske lande på lige fod med Danmark.

Fremmed ret findes ikke at have direkte betydning på dansk retsudøvelse. Ingen udenlandsk dom er direkte anvendelig som kilde i dansk ret. Svensk retspraksis inddrages derfor kun som supplement til illustration af retstilstanden for biometriske løsninger i persondataretlig forstand.[15]

1.4.1.5. Afgørelser fra Datatilsynet

Datatilsynet er et uafhængigt tilsynsorgan, som fører tilsyn med alle former for behandling omfattet af databeskyttelseslovgivningen. Tilsynets virke og sammensætning er hjemlet i databeskyttelseslovens § 27 i overensstemmelse med forordningens art. 51 og art. 52.

Datatilsynets afgørelser inddrages som fundamentet for fremstillingens analyse. Valget er begrundet i, som nævnt tidligere, at der ikke foreligger dansk retspraksis på området, hvorfor det ikke har været en mulighed at inddrage dette i analysen. Det findes dog også, på baggrund

[12] Lov nr. 375 af 14. juni 1995, § 1 om formålsbestemmelse.
[13] Betænkning til lovforslag nr. 79 2011/1 over Forslag til lov om ophævelse af lov om Teknologirådet [...], pkt. 2.
[14] Teknologirådets anbefaling om biometri, 2010, side 5.
[15] Munk-Hansen, Carsten, Retsvidenskabsteori, 2018, side 273.

af tilsynets virke og sammensætning, at afgørelserne kan tillægges en betydelig værdi i analysen af retstilstanden. Især, når det tages i betragtning, at der endnu ikke er forelagt lignende sager for domstolene.
Datatilsynets afgørelser kan dog ikke betragtes som værende egentlige retskilder. Med det i mente skal det også her anføres, at såfremt der fremlægges sager ved domstolene omhandlende brug af biometriske løsninger, så vil det trumfe Datatilsynets afgørelser og dermed måske også ændre retstilstanden.

I forlængelse hermed skal det også bemærkes, at de anvendte afgørelser er fra hhv. 2003, 2004, 2006 og 2017. Med blot den enkelte afgørelse fra 2017 er det vigtigt at gøre læseren af fremstillingen opmærksom på, at der skal tages højde for, at opfattelsen kan være anderledes i dag vedrørende specifikke forhold, da teknologien skrider hurtigt frem. En vurdering vil i dag måske vægte mindre end andet, hvorfor læseren må tage sine forbehold.

1.4.1.6. Retslitteratur

Der er generelt enighed om, at retslitteratur ikke kan anses for at være en selvstændig retskilde. Det betyder dog ikke, at retslitteraturen skal undervurderes. Forfatteren savner måske nok legitimitet til at fastsætte gældende ret, men forfatterens resultater vil kunne indgå med betydelig vægt i argumentationen.[16]

Retslitteraturen inddrages for at opnå, og dermed også give læseren en bredere forståelse for gældende ret, og for hvilken betydning gældende ret har for den dataansvarlige, som ønsker at anvende biometriske løsninger.

1.5. Fremstillingens disposition

Nærværende fremstilling består af følgende fem kapitler fordelt således:

Kapitel 1 introducerer fremstillingens emne, afgrænsning af emnet, og hvilken problemstilling, der forsøges at blive klarlagt. Dertil vil metode, kilder samt relevante begreber anvendt i fremstillingen blive forklaret.

Kapitel 2 redegør for hvad biometri er, de biometriske løsninger som verifikation og identifikation, og de biometriske processer.

Kapitel 3 beskriver de centrale bestemmelser i forordningen, herunder de grundlæggende principper i art. 5, med fokus på at analysere reglerne i den specifikke biometriske sammenhæng.

Kapitel 4 udgør fremstillingens primære analyse ved gennemgang af både dansk og svensk praksis med særlig fokus på mulige behandlingshjemler og de grundlæggende principper i art. 5.

[16] Munk-Hansen, Carsten, Retsvidenskabsteori, 2018, side 372 ff.

Kapitel 5 udgør en opsamling på fremstillingen med en konklusion.

Kapitel 6 følger op med en perspektivering om et eksempel på, hvordan biometrien kan benyttes i dag.

Kapitel 7 indeholder en fortegnelse over relevante kilder og litteratur.

1.6. Begreber

I det kommende afsnit redegøres for to centrale aktører i henhold til en generel persondataretlig behandling. Der er bevidsthed om, at der findes andre aktører i behandlingen af personoplysninger, men disse findes ikke at være relevante for fremstillingens analyse.

1.6.1. Den registrerede

Begrebet *den registrerede* dækker over en identificeret eller identificerbar fysisk person, hvorfor det er *fysiske* personer, der nyder beskyttelse af forordningens bestemmelser. Af definitionsbestemmelsen i forordningens art. 4, nr. 1, fremgår det, at "ved en identificerbar fysisk person [skal] forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, [...], der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet."

Terminologien *den registrerede* findes ikke særligt dækkende, da persondataretten ikke kun alene tager sigte på selve registreringen af fysiske personer, men på al behandling af persondata.[17]

1.6.2. Den dataansvarlige

Ifølge definitionen i art. 4, nr. 7 kan enhver fysisk eller juridisk person være dataansvarlig, idet betingelsen er, at vedkommende alene eller i forening afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger. Rådighedsretten ligger hos den dataansvarlige, og det er i den dataansvarliges interesse, at behandlingen af personoplysninger sker.
Forordningen er orienteret mod den, der råder over samt behandler de personlige oplysninger, hvilket er den dataansvarlige. Det er således afgørende at identificere den dataansvarlige ved al behandling af persondata, idet det er den dataansvarliges ansvar at leve op til forordningens regler og påvise det.
I litteraturen er det anført, at forordningen ikke tager stilling til hvem, som ejer de omhandlende personoplysninger, da det både er gældende for den dataansvarlige og den registrerede. Yderligere er det bemærket, at den dataansvarlige som begreb måske er defineret for bredt under hensyntagen til, at en dataansvarlig, som en enkelt person, måske ikke kan magte opgaven med forordningens krav til den dataansvarlige.[18]

[17] Blume, Peter, Den nye persondataret, 2018, side 69.
[18] Forordning 2016/679 art. 4, nr. 7, samt Blume, Peter, Den nye persondataret, 2018, side 73.

Kap. 2 Biometri

2.1. Biometri - Hvad er det?

Betydningen af selve ordet "biometri" skal findes i de græske ord "bios", som betyder liv, og "metron", som betyder mål. Når det sættes i sammenhæng, giver det resultatet at måle liv.[19]
Biometri går i sin helhed ud på at måle en fysisk eller biologisk egenskab hos en fysisk person, hvorved det gør en biometri som oplysning til en beskrivende, nærmere nøgen oplysning om et menneske. Det gør også den biometriske oplysning særligt skrøbelig, netop fordi grundlaget for den biometriske oplysning ikke kan erstattes.

Biometrien kan beskrives med tre nøgleord:

1) Universel, fordi biometrien er en egenskab, der eksisterer hos alle fysiske personer,
2) entydig, fordi den hos hver enkelt person er særegen, og
3) bestandig, fordi den som egenskab ikke ændrer sig gennem den fysiske persons liv.

Dette er præcis med til at forklare, hvorfor biometrien findes særlig anvendelig til verifikation og identifikation af en fysisk person.

I forordningens art. 4, nr. 14 defineres biometrisk data som:
"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."

Den biometriske data forudsætter, at de fysiske karakteristika og egenskaber ved en bestemt person er målbare. Målbarheden udgør baggrunden for de biometriske teknologier, da der ved eksempelvis en fingertryksaflæsning måles forskellige punkter i aftrykkets udseende.
Her kan der være tale om en måling af kun 19 målepunkter i aftrykket, hvilket siger noget om, hvor lidt der skal til for at kunne verificere en person ved eksempelvis en adgangskontrol i en virksomhed.

Kilden til de biometriske oplysninger kan inddeles i tre hovedområder:

1) fysiologiske,
2) adfærdsmæssige, og
3) psykologiske teknikker.

Der er tale om en bred tilgang til en biometrisk oplysning, men det er vigtigt at bemærke, at kilden i sig selv ikke kan betragtes som den biometriske oplysning, men derimod kun kan anvendes til indsamling af en biometrisk oplysning (eksempelvis template) gennem et udtræk af mere specifikke informationer (fx målinger) fra de tekniske prøver. Fingeraftryk vil høre under kategorien fysiologiske.

[19] Bagger Tranberg, Charlotte, 2007, ET.2007.105.

2.1.1. Verifikation og identifikation

Der skelnes mellem verifikation og identifikation ved behandling af biometriske oplysninger.

Verifikation er en proces, hvor den registreredes biometriske data kun matches med én bestemt profil. Det kan eksempelvis være tilfældet, når der skal gives adgang til en bygning med et personligt ID-kort. Systemet vil i en database matche dataene fra kortet med data, der kræves for at opnå adgang med det specifikke kort. Det hedder én-til-én matchproces (1:1). Det kan yderligere forklares ved, at denne måde begrænser matchprocessen til kun at matche dét fingeraftryk, der afgives, med det ene fingeraftryk, der tidligere er registreret i forbindelse med oprettelsen af det personlige ID-kort. Der sammenlignes således kun med én bestemt profil med de præsenterede data ved adgangskontrollen.[20]

Ved *identifikation* sammenlignes den registreredes biometriske oplysninger med en stor mængde lagrede oplysninger fra andre registrerede. Det vil sige, at der sker én til flere matchprocesser, da systemet netop sammenligner én profil med mange profiler (1:n).[21]
En database, der anvendes til identifikation, kan gribes an ved at gruppere den i enten et positivt eller et negativt match. Begge måder giver adgang til bygningen. Dette har en særdeles vigtig betydning for, hvor mange oplysninger fra registrerede personer, systemet kræver for at kunne identificere.
Et system baseret på et negativt match er mest hensigtsmæssigt i tilfældet, hvor der skal identificeres få uønskede personer, hvor personer får adgang, hvis deres data ikke findes i databasen. Omvendt er et system baseret på et positivt match mest hensigtsmæssigt, når der ønskes, at en stor gruppe ikke skal have adgang til bygningen, mens en mindre gruppe skal.[22]

Helt overordnet kan identifikation siges at besvare spørgsmålet om *hvem jeg er*, hvorimod verifikation besvarer spørgsmålet om *jeg er den, som jeg udgiver mig for at være*.
Når det sondres mellem verifikation og identifikation, er det vigtigt at bemærke, at identifikation er en mere indgribende proces end verifikation. Ved identifikation sammenstilles de biometriske oplysninger med andre identifikationsoplysninger, hvor verifikation blot kræver et match med en lagret template eller lignende. Men selvom det kan få verifikation til at lyde tilforladelig i forhold til identifikation, så skal verifikation stadig betragtes som en indgribende foranstaltning.[23]

2.1.2. Templates

Ved definitionen af en template er der ikke tale om en fuldstændig udførlig kopi af et fingeraftryk. Årsagen hertil er processens kompleksitet og den enorme mængde data, der ville skulle lagres. Derimod er der tale om et udtræk af forskellige punkter og værdier af de rå biometriske data, hvor en matematisk værdi genereres ud fra. Dette udgør en skabelon, der på

[20] Artikel 29-gruppen, WP 193, 2012, side 5-6, og Teknologirådets anbefaling om biometri, 2010, side 13.
[21] Teknologirådets anbefaling om biometri, 2010, side 13.
[22] Teknologirådets anbefaling om biometri, 2010, side 13.
[23] Bagger Tranberg, Charlotte, 2007, ET.2007.105.

engelsk kaldes en *template*. Det er derfor typisk alene template, der lagres til senere behandling frem for de rå biometriske data (se nedenfor under registreringsfasen).

En template består af et bestemt antal målepunkter, hvor det er vigtigt at tage højde for størrelsen af den mængde oplysninger, som template skal indeholde. Her er det væsentligt, at der er tilstrækkelige med oplysninger (f.eks. målepunkter fra et fingeraftryk) til at forvalte sikkerheden, så der ikke sker overlapning mellem forskellige biometriske oplysninger samt at erstatning af identiteter undgås.
Samtidig må størrelsen på template ikke være for omfattende, da det ikke må være muligt at kunne foretage rekonstruktion af de biometriske oplysninger. Med sidstnævnte stiller det derfor krav til, at genereringen af template skal være en envejsproces, så det umuliggør at regenerere de rå biometriske data ud fra template.

Generelt kan det siges, at template forsimpler selve processen i at matche en ny måling med template grundet færre målepunkter end et billede af et komplet fingeraftryk. Dette er blandt andet med til at gøre den biometriske teknologi til en effektiv, nem og hurtig løsning.

2.2. Behandling af de biometriske data (processen)

Behandlingen af biometriske oplysninger sker i biometriske systemer, der er teknologiske biometriapplikationer. Disse biometriapplikationer gør det muligt at foretage automatisk verifikation og identifikation som ovenfor nævnt (ved verifikation: Er jeg den, jeg udgiver mig for at være? Og ved identifikation: Hvem er jeg?).
Ved verifikation vil systemet bekræfte en given persons identitet ved at behandle personens biometriske data, og bekræfte forespørgslen med et ja eller nej. Ved identifikation vil systemet genkende personen ved at skelne vedkommende fra andre personer, hvis biometrisk data også er lagret i systemet, og svare at spørgeren er X.[24]

Af sikkerhedsmæssige årsager kan et biometrisk system kombinere flere forskellige biometriske målinger med andre identifikations- og verifikationsteknologier. I visse systemer kan der anvendes både ansigtsgenkendelse og stemmeregistrering. Der kan anvendes tre metoder samtidig; teknologierne er typisk baseret på en bestemt viden ved hjælp af et password eller en pin-kode, en bestemt ting gennem en nøgle eller et smartkort, og et bestemt personkarakteristik.[25]
En behandling af biometriske oplysninger i et biometrisk system vil typisk indeholde forskellige processer som registrering og indsamling, lagring og opbevaring, og match.

2.2.1. Registreringsfasen

Registreringsfasen kan siges at være den første kontakt mellem det biometriske system og den registrerede. Der er tale om en etablering af en forbindelse mellem den registrerede og de biometriske oplysninger. En registrering af den pågældende person vil typisk kræve en personlig involvering, når de biometriske rådata skal indsamles. Dette vil give en god anledning

[24] Artikel 29-gruppen, WP 80, 2003, side 3, fodnote 4.
[25] Artikel 29-gruppen, WP 80, 2003, side 4.

til at formidle information og oplysning f.eks. i henhold til forordningens art. 13 om oplysningspligt.
Det er dog ikke altid tilfældet, at der sker en personlig involvering fra den registrerede, da det også er muligt at indsamle biometrisk data og registrere vedkommende uden samtykke eller vedkommendes viden. Dette kan blandt andet lade sig gøre med CCTV-systemer, hvor ansigtsgenkendelse vil ske uden videre.

Processer, der har til formål at udtrække biometriske oplysninger fra en biometrisk kilde samt anvende disse oplysninger ved at kæde dem sammen med en person, udgør registreringsfasen. De biometriske rådata indsamles ved hjælp af specifikke sensorer, der er forskellige afhængig af, hvilken metode der udnyttes. Derefter uddrager det biometriske system alle brugerspecifikke data ud af det biometriske rådata, som derefter opbygges til en template (forklaret ovenfor).

Nøjagtigheden og sikkerheden i registreringsprocessen er altafgørende for hele det biometriske systems funktion.[26]

2.2.2. Lagringsfasen

Størrelsen af de biometriske oplysninger har en betydningsfuld rolle for hvordan oplysningerne skal lagres. Generelt er der tre forskellige måder:

1) lagring i en biometrisk anordnings hukommelse,
2) lagring i en central database, og
3) lagring på et smart card.[27]

En biometrisk anordning vil typisk være placeret lokalt, hvor registreringen finder sted. Det kan være en aflæser, scanner eller lignende. En central database vil derimod være placeret et andet sted, hvortil de biometriske data fremsendes og lagres i. Her vil de biometriske data ofte være tilgængelige for et eller flere biometriske systemer. Et smart card vil typisk være i den registreredes besiddelse, hvorfor den registrerede har de bedste muligheder for at føre kontrol med sine oplysninger.[28]

Når der er tale om verifikation er det i princippet ikke nødvendigt at lagre referencedata, der skal bruges, i en central database, men derimod findes det tilstrækkeligt kun at lagre dem decentralt.
Omvendt vil det være nødvendigt i tilfældet af identifikation at lagre referencedata i en central database, da det biometriske system skal kunne fastslå identiteten på den registrerede ud fra en sammenligning af oplysningerne med andre personers tilsvarende oplysninger.

[26] Artikel 29-gruppen, WP 193, 2012, side 5.
[27] Artikel 29-gruppen, WP 80, 2003, side 4. Sidstnævnte lagring kaldes også "match on card-teknologi" ifølge Teknologirådets anbefaling om biometri, 2010.
[28] Datatilsynets afgørelse 2004-219-0208.

2.2.3. Matchfasen

Match finder sted, når biometriske oplysninger (eksempelvis template) fra registreringen skal sammenlignes med de oplysninger, der indsamles, når behovet for identificering og verifikation opstår.
Der er tale om den matchproces, der eksempelvis udføres i den biometriske anordning (én-til-én match) eller i den centrale database (én eller flere matchprocesser). Udtrykket *matchværdier* kommer her i spil, da match i eksemplet om brug af template skal måle værdier mod hinanden. Matcher værdierne, gives der "grønt lys".

I forståelsen af, hvorvidt et system afgør om et match er gyldigt eller ej, følger forklaringen af en række udtryk for risici. Det kan være vanskeligt at opnå 100% fejlfrie resultater i selve matchningen, da forskelle i miljø ved registreringen og forskelle i udstyr, der anvendes til indsamlingen, spiller en rolle for nøjagtigheden af resultatet.

De vigtigste er FAR (false accept rate) og FRR (false reject rate).
FAR er en betegnelse for sandsynligheden om, at et system fejlagtigt vil identificere og matche en persons template, som ikke er berettiget til eksempelvis adgang. Det kan også forklares ved, at systemet vil undlade at afvise en person, der ikke skal have adgang. FAR er et udtryk for procentdelen af falske positive match.
FRR betegner sandsynligheden for, at et system fejlagtigt vil opfatte en persons template til ikke at matche med den tidligere registrerede template, som rent faktisk er brugerens. Derfor omfatter FRR procentdelen af falske negative match, når en person ikke matches til sin egen registrerede skabelon.

Det skal iagttages, at FAR og FRR anvendes som redskaber i fællesskab, da de er afhængige af hinanden. Reduceres den ene, forøges den anden, og omvendt. Jo mere nøjagtigt et biometrisk system er, desto større risiko vil der være for, at FRR tenderer til en høj procentdel. Det er vigtigt i fastlæggelsen af en acceptabel nøjagtighed at vurdere behandlingens formål både ift. FAR og FFR, men også ift. størrelsen af den befolkningsgruppe, som systemet skal administrere.[29] Jo større gruppe af registrerede, desto højere tolerance for satserne er der.

[29] Artikel 29-gruppen, WP 193, 2012, side 6, samt Teknologirådets anbefaling om biometri, 2010, side 14.

Kap. 3 Den retlige ramme for legitim behandling

3.1. Oplysningskategorierne

Der skelnes nu mellem almindelige og særlige kategorier af personoplysninger (følsomme oplysninger) i henholdsvis art. 6 og art. 9. Dertil behandling af personoplysninger vedrørende straffedomme og lovovertrædelser i art. 10.
Forordningens art. 9 udgør en udtømmende liste over hvilke oplysninger, som kan kategoriseres som særlige kategorier af personoplysninger. Det betyder også, at almindelige oplysninger omfatter alle de oplysninger, som ikke er nævnt i art. 9.
Der er desuden i udgangspunktet forbud mod behandling af de særlige kategorier af personoplysninger i art. 9, hvorfor behandling af de nævnte oplysninger kun kan ske med hjemmel i art. 9, stk. 2.

3.1.1. Særlige kategorier af personoplysninger (følsomme oplysninger)

Særlige kategorier af personoplysninger er reguleret i forordningens art. 9. Disse særlige kategorier er "oplysninger 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."[30]

Dog skal art. 9(2) iagttages, hvor det bestemmes under hvilke betingelser behandling trods forbuddet kan ske. Det kan siges at være en to-leddet proces, da det umiddelbart skal undersøges, om der foreligger et samtykke til behandling af personoplysningen. Hvis ikke samtykke foreligger, kan det trods forbud og manglende samtykke findes nødvendigt at behandle personoplysningen efter en række nødvendighedshensyn. Disse nødvendighedshensyn er oplistet i art. 9, stk. 2, litra b)-j).
Art. 9, stk. 2 kan betragtes på to forskellige måder, enten som undtagelser eller behandlingsmuligheder. Forskellen på disse er, hvor strengt bestemmelserne skal fortolkes. En opfattelse kan være, at databeskyttelseslovgivningen tolker bestemmelserne som behandlingsmuligheder.[31]

3.1.2. Almindelige personoplysninger

De almindelige oplysninger er reguleret i forordningens art. 6. Særligt for denne bestemmelse er, at enhver personoplysning, selv den mest trivielle oplysning, kun må behandles med hjemmel i lov. Bestemmelsen har derfor en vigtig funktion for den generelle opfattelse af behandling af personoplysninger.[32]

[30] Forordning 2016/679 art. 9(1).
[31] Blume, Peter, Den nye persondataret, 2018, side 103.
[32] Blume, Peter, Den nye persondataret, 2018, side 95.

Betegnelsen og oplysningskategorien *semi-følsomme oplysninger* findes ikke i forordningen, hvorfor disse falder ind under kategorien almindelige oplysninger. Visse oplysninger er dog særskilt reguleret i forordningens art. 10.

For art. 6 om almindelige oplysninger gør det sig gældende, at behandling af personoplysninger må ske, hvis mindst én af betingelserne i artikel 6, stk. 1, litra a)-f) er opfyldt af den dataansvarlige.
Her er der også, som ved de særlige kategorier af oplysninger, tale om en række nødvendighedshensyn, der kan begrunde behandling, når der ikke foreligger samtykke fra den registrerede.

Ud af nødvendighedshensynene i art. 6 er interesseafvejningsreglen i art. 6, stk. 1, litra f, værd at bemærke. Denne adskiller sig fra art. 9, hvor der ikke findes lignende bestemmelse om interesseafvejning. Det har ikke været formålet med forordningen at begrænse brugen af almindelige oplysninger, hvorfor denne interesseafvejningsregel har fået sin plads her.
Efter art. 6, stk. 1, litra f, er det muligt for den dataansvarlige at behandle almindelige oplysninger, såfremt det er begrundet i den dataansvarliges saglige interesse, og hvor denne interesse vejer tungere end den registreredes interesser, eller hensynet til den registreredes grundlæggende rettigheder og frihedsrettigheder overstiger den dataansvarliges interesser.

Som noget nyt er der i interesseafvejningsreglen nævnt et hensyn til den registrerede, hvis vedkommende er barn. Dette er udtryk for, og stemmer overens med forordningens øvrige systematik om, at der skal tages særligt hensyn til børn.
Når hensynet til børn fremhæves i art. 6, stk. 1, litra f, stiller det yderligere krav til, at den dataansvarliges interesse skal oplyses særlig klart. Det skal tillægges en vis betydning, at børn op til en vis alder, formentlig 15 år, ikke er i stand til at overskue konsekvenserne af et samtykke, hvorfor interesseafvejningen her kan være eneste behandlingsbetingelse.[33]

3.1.3. Samspillet mellem biometrisk data og oplysningskategorierne

Behandling af biometriske oplysninger med det formål entydigt at identificere en fysisk person er nu omfattet af de særlige kategorier af oplysninger i forordningens art. 9. Hvis der *ikke* er tale om en identifikationsløsning, vil det være en almindelig oplysning omfattet af forordningens art. 6.
Denne funktionelle afgrænsning er speciel, fordi der ikke findes andre typer af oplysninger, hvor denne indfaldsvinkel benyttes. Formålet og teknologien afgør, om det er en følsom oplysning. Men rene rådata i sig selv, eksempelvis en finger, er ikke en følsom oplysning.[34]
Et finger- eller håndaftryk kan ikke i sig selv frembringe oplysninger til identifikation af en person. Det kræver et match eller sammenstilling med andre identifikationsoplysninger.

[33] Blume, Peter, Den nye persondataret, 2018, side 100.
[34] Blume, Peter, Den nye persondataret, 2018, side 105.

3.2. Samtykke

Samtykket skal ses som en behandlingshjemmel, der bruges i vidt omfang, *som én blandt flere mulige ligestillede behandlingshjemler*.[35] Rækkefølgen, som blandt andet oplistes i forordningens art. 9, hvor samtykke nævnes som første behandlingsgrundlag, findes meget relevant, men det er ikke nødvendigvis altid samtykke, der egner sig bedst til grundlag for en legitim behandling.[36] Dette bliver illustreret i fremstillingens analyse af Datatilsynets afgørelser.

Det medfører, at den dataansvarlige ikke nødvendigvis først skal undersøge, om den registrerede vil give sit samtykke til behandlingen, men derimod må den dataansvarlige gerne undersøge andre mulige behandlingsgrundlag. Dog betragtes det som værende god skik, hvis den dataansvarlige forsøger at opnå samtykke.

I forlængelse heraf kan det siges, at samtykke som mulig behandlingshjemmel ikke udelukker, at den dataansvarlige, efter forgæves forsøg på indhentelse af samtykke, vælger at finde hjemmel i en af de andre mulige behandlingshjemler.
Det kan dog tænkes at kollidere med tanken om afvejning til ugunst for den registrerede, hvis den dataansvarlige vælger denne løsning i forbindelse med interesseafvejningsreglen i art. 6, stk. 1, litra f. Det faktum, at den registrerede ikke frivilligt vil give sit samtykke, kan så tvivl, om det rent faktisk falder ud til fordel for den dataansvarlige, og om det rent faktisk vil være en behandling i overensstemmelse med princippet om god skik i art. 5, litra a.[37] Dette generelle princip behandles nærmere senere i fremstillingen.

Indhentelse af samtykke fra den registrerede har ikke den effekt, at den dataansvarliges forpligtelser til at overholde forordningens øvrige regler, herunder de grundlæggende principper i art. 5, ophører.
Selvom den dataansvarlige kan legitimere sin behandling af biometriske oplysninger ved den registreredes samtykke, så berettiger det eksempelvis ikke en indsamling og behandling af oplysninger, der står i misforhold til formålet.[38]

Med forordningen er der, modsat tidligere lovgivning, indsat en bestemmelse i art. 7, der præciserer betingelserne for samtykke nærmere. Ifølge bestemmelsens stk. 1 er det den dataansvarlige, der skal kunne påvise, hvis en behandling er baseret på et samtykke. Det er dermed den dataansvarlige, som har bevisbyrden.
Da der ikke gælder nogen formkrav til samtykke efter lovgivningen, kan der være tale om et mundtligt eller skriftligt samtykke. Det er dog klogt og mest hensigtsmæssigt, at den dataansvarlige kræver skriftligt samtykke så vidt det er muligt. Især ved behandling af

[35] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 170.
[36] Artikel 29-gruppen, WP 187, 2011, side 8.
[37] Blume, Peter, Den nye persondataret, 2018, side 97.
[38] Artikel 29-gruppen, WP 187, 2011, side 8.

oplysninger af følsom karakter, eller hvis samtykket har stor betydning for mindst én af parterne.[39]
Af præambelbetragtning nr. 32 til forordningen fremgår det, at samtykke bør gives separat til alle behandlingsformål, hvis der foreligger flere. Omvendt dækker samtykket alle de behandlingsaktiviteter, der udføres under ét formål.

3.2.1. Krav til samtykket

Databeskyttelsesforordningens art. 4, nr. 11 definerer samtykket som *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.*

3.2.1.1. Frivilligt samtykke

At samtykket skal være *frivilligt* betyder, at den registrerede reelt har en bestemmelsesret og kontrol over sit samtykke. Hvis samtykket er knyttet til betingelser og vilkår, og ikke kan forhandles, så er samtykket ikke afgivet frivilligt.[40]
Ligeledes fremgår det af forordningens art. 7, stk. 4, at såfremt opfyldelsen af en kontrakt er gjort betinget af et samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelsen, er der ikke tale om et frivilligt afgivet samtykke.

Hvis en behandling af biometriske oplysninger er baseret på et samtykke fra den registrerede, stilles der krav om, at der foreligger et gyldigt alternativ til den biometriske løsning. Det kan eksempelvis være et kodeord eller et magnetkort. Det er ikke tilstrækkeligt, at der stilles et system til rådighed, hvis systemet er for kompliceret eller for tidskrævende, og derfor afholder den registrerede fra at anvende det.[41]
Såfremt den registrerede kun kan vælge imellem at afgive sine biometriske oplysninger eller ikke at anvende en tjeneste overhovedet, vil det tale kraftigt for, at der ikke er afgivet et frivilligt samtykke. Dette understøttes af præambelbetragtning nr. 42 til forordningen, hvor det anføres, at samtykket kun kan anses for at være afgivet frivilligt, når den registrerede har et reelt valg og kan afvise at give sit samtykke uden det kommer vedkommende til skade.

3.2.1.2. Specifikt samtykke

Når der stilles krav om, at samtykket skal være *specifikt*, betyder det, at et generelt samtykke uden nærmere angivelse af et specificeret formål ikke accepteres. Der er strenge krav til, at det skal være forståeligt for den registrerede om, hvad denne samtykker til. Den dataansvarlige skal klart og præcist forklare omfanget og konsekvenserne af behandlingen af den registreredes data.[42]

[39] Præambelbetragtning nr. 32 til forordning 2016/679.
[40] Artikel 29-gruppen, WP 259, 2017, side 6.
[41] Artikel 29-gruppen, WP 193, 2012, side 11.
[42] Artikel 29-gruppen, WP 187, 2011, side 19.

3.2.1.3. Informeret samtykke

At samtykket skal være *informeret* betyder, at der skal gives tilstrækkelig information om, hvordan de biometriske oplysninger påtænkes at blive anvendt. Når biometriske oplysninger har egenskaber som værende unik og universel, så stiller det yderst store krav til formidlingen om, hvordan oplysningerne lagres er klar og lettilgængelig. Dette er helt afgørende for, at et samtykke kan anses for at være gyldigt.[43]

3.2.2. Tilbagekaldelse

Samtykket *skal* til enhver tid kunne tilbagekaldes og ophæves af den registrerede. Det har den betydning for den dataansvarlige, at der stilles krav til implementering af tekniske midler, der har funktionen at tilbagekalde evt. anvendelse af biometriske oplysninger i anvendte systemer. Det biometriske system skal effektivt kunne fjerne alle oprettede identitetsforbindelser, hvis samtykke tilbagekaldes.[44]

3.3. Persondataretlige krav til biometriske løsninger

3.3.1. Hvad er en personoplysning?

Ifølge forordningens art. 4, nr. 1, fastlægges det, at en personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person.

Med fokus på begrebet "identificeret" er der tale om en situation, når en person kan *skelnes* - og dermed skille sig ud - fra andre personer. Ses der på begrebet "identificerbar", er der tale om en situation, når det blot er *muligt* at identificere en person, men hvor identificeringen endnu ikke er sket.
Forskellen på endelsen -bar betyder, at dette begreb kan kaldes en grænsebetingelse, der afgør, hvornår oplysningen ligger inden for forordningens anvendelsesområde.
Ved vurderingen af, om en person er identificerbar, fremgår det af præambelbetragtning nr. 26 til forordningen, at alle hjælpemidler bør tages i betragtning, der med rimelig kan tænkes at bringes i anvendelse af den dataansvarlige eller en anden person.

En personoplysning kan bl.a. være et navn, et identifikationsnummer, eller elementer om en persons ydre træk eller en egenskab, som man ikke umiddelbart kan se med det blotte øje. I forordningens art. 4, nr. 1, betegnes det som "en persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet". Disse særlige oplysninger kaldes også identifikatorer. Disse oplysninger har "en særligt privilegeret og tæt forbindelse med den pågældende person".[45]

[43] Artikel 29-gruppen, WP 193, 2012, side 11.
[44] Artikel 29-gruppen, WP 193, 2012, side 12.
[45] Artikel 29-gruppen, WP 136, 2007, side 12.

3.3.2. Er en biometrisk oplysning en personoplysning?

Det er konstateret i teorien, at de biometriske identifikationsmålinger eller template uddraget heraf anses for at være personoplysninger i de fleste tilfælde.[46]
De biometriske rådata, som indsamles i registreringsfasen, er en personoplysning omfattet af forordningen, netop fordi de kan henføres til en bestemt fysisk person. Det må derfor også gælde for templates eller lignende, som er genereret ud fra de samme data.[47]

Det fremgår nu direkte af ordlyden i forordningens art. 9, at behandling af biometrisk data med det formål entydigt at identificere en fysisk person, er en følsom oplysning.

Datatilsynet har desuden flere gange konstateret, at en biometrisk oplysning er en personoplysning i persondataretlig forstand, jf. afgørelserne nedenfor i fremstillingens kap. 4.

3.3.3. Hvornår behandles biometriske oplysninger?

Det fremgår nærmere i forordningens art. 4, nr. 2, hvornår der er tale om en behandling af personoplysninger i forordningens forstand. Det fremgår af bestemmelsen, at der er tale om en behandling ved enhver aktivitet eller række af aktiviteter - med eller uden brug af automatisk behandling, hvor personoplysninger gøres til genstand for *"indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse…"*
Forordningen gælder altså for stort set enhver form for behandling af personoplysninger.

Datatilsynet har flere gange konstateret, at lagring af fingeraftryk på chippen ved udstedelse af smartcard, aflæsning af fingeraftryk og smartcard ved indcheckning, scanning af fingeraftryk, udregning af matchværdier og sammenligning i forhold til central database, er en behandling i persondataretlig forstand.[48]

3.4. De grundlæggende persondataretlige principper

Forordningens art. 5 danner rammen for den dataansvarliges virksomhed. Bestemmelsen fastlægger de generelle principper for al behandling af persondata. De gælder således for enhver information om en identificeret eller identificerbar fysisk person.

Det følger af art. 5, stk. 2, at det er den dataansvarlige, der er ansvarlig for at reglerne overholdes og endvidere at dette påvises. *Ansvarlighed* er generelt et gennemgående hovedprincip i forordningen, og det skal være synligt, at den dataansvarlige overholder dette krav. Art. 5 kan karakteriseres "som en art "grundlov" for persondatabehandling."[49]

[46] Artikel 29-gruppen, WP 80, 2003, side 5.
[47] Bagger Tranberg, Charlotte, ET.2007.105, side 2.
[48] Bagger Tranberg, Charlotte, ET.2007.105, note 24.
[49] Blume, Peter, Den nye persondataret, 2018, side 85.

3.4.1. Lovlighed, rimelighed og gennemsigtighed

Forordningens art. 5, stk. 1, litra a, viderefører det hidtil gældende princip om "god databehandlingsskik". For at kunne behandle personoplysninger er det et krav, at behandlingen er lovlig. Det betyder også, at en behandling ikke anses for at være lovlig, hvis den strider imod andre præceptive lovregler.
En behandling betragtes som værende lovlig, når personoplysninger behandles på grundlag af den registreredes samtykke eller et andet legitimt grundlag. Dette gælder i forhold til forordningen, men også i forhold til anden national lovgivning og EU lovgivning.

Behandlingen skal være *rimelig* for at kunne finde sted. Dette betyder, at behandlingen i øvrigt skal være overensstemmende med forordningens beskyttelsesinteresse. Dette har fungeret som en generalklausul, hvor en behandling har kunne afvises alene på baggrund af dette, selvom behandlingen ellers er anset for værende i overensstemmelse med forordningen.

Vedrørende dette princip er der med forordningen ikke tale om en ændring af gældende ret, og det må således fortsat være op til tilsynsmyndigheden at fastlægge regler for god databehandlingsskik.

Art. 5, stk. 1, litra a, fremhæver også, at behandlingen skal være *gennemsigtig,* hvilket er et centralt parameter. Den registrerede skal have mulighed for nemt at overskue behandling af sine personoplysninger, og hvorfor behandlingen finder sted.
I præambelbetragtning nr. 39 til forordningen anføres det, at kommunikationen skal foregå i *et klart og enkelt sprog*. Det er i overensstemmelse med forordningens øvrige systematik, da det er et gennemgående træk, at sproget skal være forståeligt og let tilgængelig for en almindelig person. Dette udmønter sig blandt andet i forordningens art. 12.

Det kan være svært præcist at angive, hvilke krav princippet om lovlighed, rimelighed og gennemsigtighed stiller til kommunikationen mellem dataansvarlig og den registrerede, så den lever op til forordningen. Det afhænger af den konkrete situation. Men det har betydning for, hvordan den dataansvarliges oplysningspligt udformer sig efter art. 13 og art. 14 i forordningen om oplysningspligt ved indsamling.[50]

3.4.2. Formålsbegrænsning

Første led i forordningens art. 5, stk. 1, litra b, fastslår, at personoplysninger kun må indsamles til udtrykkeligt angivne og legitime formål. Der skal foreligge saglige formål med indsamlingen, og det skal være klart, hvorfor indsamlingen finder sted.[51]

[50] Blume, Peter, Den nye persondataret, 2018, side 86.
[51] Præambel nr. 39 til forordning 2016/679.

Andet led i bestemmelsen fastslår, at de indsamlede oplysninger ikke på et senere tidspunkt efter indsamling må viderebehandles til et andet formål, som ikke er foreneligt med det oprindelige formål.[52]
Som et eksempel skal forordningens art. 6, stk. 4 om almindelige oplysninger ses som et værktøj til den dataansvarlige, hvoraf en række supplerende forhold fremgår til vurderingen af, om der er tale om en nyt formål, der lovligt kan viderebehandles i henhold til art. 5, stk. 1, litra b. Bestemmelsen udpensler, at der kan ske behandling til et andet formål end det oprindelige formål, hvis den registrerede samtykker hertil, eller hvis der findes hjemmel til behandlingen på baggrund af EU-ret eller national ret.

Når biometriske oplysninger behandles, ligger der en klar forudsætning for, at formålet med behandlingen af disse oplysninger er defineret og udspecificeret under hensyntagen til de eventuelle risici, der er forbundet med den biometriske behandling. Særligt når det sættes i relation til personers grundlæggende rettigheder.
Risikoen for genbrug af biometriske oplysninger, og dermed viderebehandling til uforenelige formål, anses for at være relativ lav, såfremt de biometriske oplysninger ikke lagres i centrale databaser, hvor oplysningerne kan være tilgængelige for tredjemand. Ved central lagring af biometriske oplysninger øges risikoen for, at oplysningerne anvendes til at forbinde forskellige databaser, som vil give mulighed for, at der udarbejdes detaljerede profiler over enkeltpersoners vaner både i det offentlige og private rum.[53]

Ved behandling af biometriske oplysninger, så har det netop stor betydning, at formålet er specificeret, fordi biometriske oplysninger er stationære, og derfor ikke ændrer sig over tid.[54]

3.4.3. Dataminimering

Af forordningens art. 5, stk. 1, litra c, fremgår det, at personoplysninger skal være tilstrækkelige, relevante og begrænset til det, der findes nødvendigt i forhold til de formål, hvorunder de behandles.
Som bidrag til fortolkning af princippet kan det i præambel nr. 39 i forordningen læses, at det kræver, at perioden for opbevaring af personoplysningerne minimeres til det strengt nødvendige. Personoplysninger bør i øvrigt også kun behandles, hvis formålet med behandlingen ikke kan opfyldes på en anden rimelig måde end påtænkte. Med dette er der tale om et *centralt* proportionalitetsprincip.[55]

Ved behandling af biometriske oplysninger kan der opstå risiko for, at der indsamles flere oplysninger end nødvendigt for selve matchfunktionen. Ved anvendelsen af biometriske

[52] Det fastslås i bestemmelsen, at viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statiske formål ifølge artikel 89, stk. 1, ikke er uforeneligt med indsamlingsformålet.
[53] Artikel 29-gruppen, WP 80, 2003, side 7.
[54] Bagger Tranberg, Charlotte, ET.2007.105, side 2.
[55] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 97.

oplysninger er behovet, at spørgsmålet om proportionalitet rejses for hver enkelt kategori af behandlet data set i lyset af formålet med indsamlingen og behandlingen.[56]

Det er op til den dataansvarlige at sørge for, at der kun indsamles nødvendige oplysninger til opfyldelse af formålet med behandlingen. Det betyder, at det kun er de påkrævede oplysninger, og ikke alle frit tilgængelige oplysninger, der indsamles, behandles eller lagres. Det skal overvejes, om det påtænkte formål kan opnås på en mindre indgribende måde. Dernæst har det også betydning, hvordan den dataansvarlige opstiller en standardkonfiguration og indretter det biometriske system, således systemet optimalt fremmer denne databeskyttelse uden at den dataansvarlige skal håndhæve den.[57]

Når et foreslået biometrisk system skal underlægges en analyse af proportionaliteten skal det indledende vurderes, om systemet er nødvendigt for at opfylde det, som Artikel 29-gruppen kalder *et identificeret behov*. Der er tale om en 4 trins test, der senere anvendes i analysen i fremstillingens kap. 4.
Den første del består af en afvejning om, hvorvidt den valgte løsning er nødvendig for opfyldelsen af behovet, eller om systemet blot betragtes at være den billigste og nemmeste løsning til opfyldelse af formålet med behandlingen af personoplysningerne.

Dernæst skal der tages stilling til, om det biometriske system er effektivt i opfyldelsen af behovet sammenholdt med den anvendte biometriske teknologis karakteristika. Med dette menes, at en identifikator kan være hensigtsmæssig og teknisk velegnet i ét tilfælde, men ikke i et andet.
Her kan det blandt andet være relevant ved identifikationsløsninger, at det biometriske system karakteriseres af begrænset FRR. Hvis systemet fejlagtigt gentagne gange afviser den registrerede og dennes template, så findes det ikke effektivt til det ønskede formål.

Ved tredje trin i analysen skal det afvejes, om det resulterende tab af privatliv står i rimeligt forhold til det forventede resultat og identificerede behov. Spørgsmålet kan være om fordelene ved det biometriske system og de anvendte identifikatorer vægter mest. Det er konstateret af Artikel 29-gruppen, *at hvis fordelene er relativt begrænsede, [...] vil tabet af privatliv ikke være hensigtsmæssigt.*

På fjerde trin skal det afgøres, hvorvidt et mindre indgribende middel kan opfylde det identificerede behov med det biometriske system. Mindre indgribende løsninger kan eksempelvis være brug af smartcard eller andre metoder, der ikke medfører en centraliseret lagring af biometriske personoplysninger, når formålet blot er verifikation. Her tages hensyn til privatlivets fred.[58]

[56] Artikel 29-gruppen, WP 193, 2012, side 8.
[57] Artikel 29-gruppen, WP 193, 2012, side 10.
[58] Artikel 29-gruppen, WP 193, 2012, side 8.

Med 4 trins testen er der ikke tale om en vurdering af, hvorvidt biometriske løsninger skal benyttes eller ej. Derimod er der tale om en vurdering af, om der kan findes en mindre indgribende biometrisk løsning.

3.4.4. Rigtighed

Med art. 5, stk. 1, litra d, er der tale om en kvalitetsbestemmelse. Princippet om datakvalitet fastslår, at personoplysninger skal *være korrekte og om nødvendigt ajourførte*.[59] Når oplysningerne skal ajourføres, skal det måles op imod behandlingsformålet på ny.

Bestemmelsen medfører, at *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*.[60]
Der stilles store krav til, at urigtige oplysninger *straks* slettes.

Bestemmelsen omhandler kun sletning og berigtigelse rent ordlydsmæssigt, men det antages også at den dataansvarlige vil kunne blokere eller arkivere personoplysningen for at opfylde datakvalitetskravet. Disse to metoder har det til fælles, at de ikke aktivt behandler oplysningen.

Begrebet urigtige oplysninger kan siges at dække andre begreber som vildledende og ufuldstændige oplysninger, som tidligere er nævnt i persondataretlig lovgivning.[61] Det forudsættes, at den dataansvarlige selvfølgelig er bekendt med de omstændigheder, hvoraf det fremgår, at personoplysningerne er urigtige.
Det fremgår af praksis, at den dataansvarlige må indrette rutiner - alt afhængig af hvilken personoplysning, der er tale om - så det er muligt at efterse datakvaliteten med passende mellemrum. Det biometriske system skal gøre det muligt for den dataansvarlige at reagere hurtigt på urigtige oplysninger.[62]

For at et biometrisk system skal kunne opfylde de formål, der har været med indsamlingen, må de biometriske oplysninger være *nøjagtige* og relevante (læs rigtige). I vurderingen af datakvaliteten skal der tages stilling til hvilken oplysningskategori, der er tale om, og om behandlingen medfører en indgriben i integriteten. Jo mere følsom oplysningen er og indgribende behandlingen er, desto større krav til god datakvalitet og kontrol stilles der.[63]

Kravet om rigtighed stiller strenge krav til registreringsfasen, når de biometriske oplysninger indsamles hos den registrerede. Nøjagtig registrering af oplysninger er netop vigtigt for at undgå og forebygge identitetssvindel.[64] Manglende iagttagelse af nøjagtighed vil kunne medføre en falsk afvisning (tidligere betegnet FRR) og et falskt match (tidligere betegnet FAR).

[59] Forordning 2016/679 art. 5, stk. 1, litra d.
[60] Forordning 2016/679 art. 5, stk. 1, litra d.
[61] Se evt. forklaring i Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 99.
[62] Blume, Peter, Den nye persondataret, 2018, side 93.
[63] Blume, Peter, Den nye persondataret, 2018, side 93.
[64] Artikel 29-gruppen, WP 193, 2012, side 9.

Det bemærkes endnu engang, at det med anvendelse af biometriske systemer følger en vanskelighed ved at opnå 100 % fejlfrie resultater, hvorved FRR og FAR undgås helt.[65]
Nøjagtighed er derfor generelt afgørende for det biometriske systems funktion, da det har betydning for alle led i den biometriske proces. De biometriske oplysninger er kun anvendelige, hvis de er nøjagtige og relevante i forhold til indsamlingens formål.

3.4.5. Opbevaringsbegrænsning

Tages der udgangspunkt i den moderne informationsteknologi og det faktum, at det ikke er særlig dyrt for den dataansvarlige at lagre oplysninger, så er det med forordningen fastlagt i art. 5, stk. 1, litra e, at perioden for opbevaring af identificerende oplysninger skal tidsbegrænses.
Det forhindrer lagring i tilfælde, hvor det er fristende at lagre oplysninger, selvom de ikke behandles med et formål, fordi de måske kan blive anvendelige i fremtiden. Med andre ord forhindrer det også dataophobninger, der kan true den personlige integritet.
Der er altså tale om en tidsbegrænsning under kravet til, at oplysninger ikke må lagres i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. Undtaget er personoplysninger omfattet af formålsbegrænsningsprincippet.

Ifølge præambelbetragtning nr. 39 til forordningen bør den dataansvarlige indføre tidsfrister for sletning eller periodisk gennemgang for at sikre, at personoplysninger ikke opbevares i længere tid end nødvendigt. Generelt stilles krav til, at den dataansvarlige indfører politikker på området samt tidsfrister for sletning eller periodisk gennemgang, hvor disse skal kunne begrundes i forhold til behandlingens formål. Dette støttes i praksis.[66]
Ifølge senere praksis har det vist sig at være en mulighed for Datatilsynet i bestemte sammenhænge at fastsætte udfyldende tidsfrister, som også med forordningen betragtes at være en vejledende mulighed fremover. Det har været - og er stadig - antaget i dansk praksis, at der gælder en vejledende grænse på 5 år, som dog kan besluttes at være kortere eller længere.[67]

Der skal være tydelig forskel mellem generelle personoplysninger og biometriske oplysninger, når det skal afgøres, om oplysningerne anses for nødvendige til lagring eller ej. Generelle oplysninger kan måske være påkrævet i en længere periode end biometriske oplysninger, hvor de sidstnævnte typisk er bundet til et adgangsforhold, som den registrerede har i forbindelse med arbejde eller fritidsaktivitet fx adgang til et motionscenter. Når en medarbejder ikke længere er ansat i en virksomhed, hvor vedkommende havde adgang til et afgrænset område, så skal de biometriske oplysninger, der er brugt til adgangskontrol, slettes, da formålet med behandlingen ikke længere er aktivt.[68]

[65] Artikel 29-gruppen, WP 193, 2012, side 6.
[66] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565 side 100, samt Blume, Peter, Den nye persondataret, side 94.
[67] Blume, Peter, Den nye persondataret, side 94.
[68] Artikel 29-gruppen, WP 193, 2012, side 10.

3.4.6. Ansvarlighed

Det følger af forordningens art. 5, stk. 1, litra f, at personoplysninger skal behandles på en sådan måde, at der er sikret en tilstrækkelig sikkerhed for de pågældende personoplysninger. Forordningen præciserer nærmere kravene til behandlingssikkerheden i art. 32, hvorefter oplysningerne skal behandles sikkert ved at iagttage passende tekniske og organisatoriske foranstaltninger.
Der er tale om en nydannelse i lovgivningen i forhold til tidligere gældende direktiv nr. 95/46/EF, når sikkerhed er blevet et princip i forordningen. Det giver indtrykket af, at der har været et behov for, at sikkerheden skal fremhæves. Det kan ses som et signal til de dataansvarlige, at behandlingssikkerhed skal tillægges en stor vægt i forhold til behandling af personoplysninger efter forordningen.

3.4.6.1. Specifikke krav til den dataansvarlige

Tidligere databeskyttelseslovgivning stillede kun krav til den dataansvarlige om at sikre, at nævnte grundlæggende principper overholdes modsat forordningen, der nu kræver at den dataansvarlige kan *påvise* det. Det kan siges at være overensstemmende med den røde tråd om *ansvarlighed.*

Som led i det overordnede krav om ansvarlighed, der fremgår eksplicit af forordningens art. 5, stk. 2 og art. 24, er den dataansvarlige forpligtet til at træffe passende tekniske og organisatoriske foranstaltninger gennem design og standardindstillinger med henblik på efterlevelse af forordningen, herunder effektiv implementering af de grundlæggende principper i art. 5, og beskyttelse af de registreredes rettigheder. Dette fremgår eksplicit af forordningens art. 25.
Den dataansvarlige er dermed forpligtet til at overveje, hvordan forordningens bestemmelser kan efterleves med konkrete foranstaltninger i design af IT systemer samt ved indretningen af den dataansvarliges organisation.
Det fremgår af præambelbetragtning nr. 78, at sådanne foranstaltninger bl.a. kan bestå af dataminimering, pseudonymisering af oplysninger og gennemsigtighed. Dataminimering og gennemsigtighed er desuden nævnt i art. 5 under de grundlæggende principper, som den dataansvarlige altid er forpligtet til at overholde ved enhver behandling af personoplysninger.

3.4.6.2. Tekniske foranstaltninger

Når biometriske personoplysninger behandles, kan det få alvorlige konsekvenser for de registrerede i tilfælde, hvor der sker et brud på persondatasikkerheden, medmindre den dataansvarlige forholder sig til dette ved at træffe tekniske og organisatoriske foranstaltninger. De omtalte brud på persondatasikkerheden kan udmønte sig i, at en ulovlig adfærd skaber en uautoriseret aktivitet i form af at rekonstruere det biometriske træk fra skabelonen, hvorfor det kan konstateres, at brug af template i stedet for et billede af det fulde fingeraftryk kan være et godt eksempel på en sådan foranstaltning. Det mindsker risikoen for misbrug, hvis der lagres biometriske skabeloner frem for rådata i form af billeder af hele fingeraftryk.

Manglende fortrolighed og integritet i forbindelse med brug af databaser, hvori de biometriske oplysninger lagres, vil være ødelæggende for ikke mindst fremtidige applikationer, der bygger på informationer fra disse databaser, men også for den registrerede, som tilføjes en uoprettelig skade. I allerværste tilfælde vil det betyde, at den registreredes fingeraftryk fremover vil fremstå utroværdigt og miste sin værdi.[69]

Yderligere er det centralt ved vurderingen, om behandling af biometriske oplysninger i øvrigt er i overensstemmelse med forordningen, at undgå lagring i en central database. I stedet må det anbefales, at oplysningerne lagres på medier, hvortil det udelukkende er den registrerede, som har adgang til f.eks. et smartcard.[70]

Det er også afgørende, at biometriske oplysninger lagres i krypteret form. De såkaldte krypteringsnøgler kan kun afkodes på basis af en ny indsamling af data fra den registrerede selv, hvorfor at det undgås at de biometriske oplysninger genbruges til andre formål end hvad der blev indsamlet til. Det er i øvrigt i overensstemmelse med princippet om formålsbegrænsning i art. 5, stk. 1, litra b.[71]

Endnu en foranstaltning kan være en automatisk mekanisme oprettet til sletning af data, således unødvendige data rettidig slettes, når de ikke længere findes nødvendige for formålet med det biometriske system.
En sådan mekanisme kan integreres på forskellige måder, eksempelvis ved anvendelse af flygtige lagre til lagring af oplysningerne, der automatisk slettes, når en fingeraftryksaflæser slukkes, sælges eller afinstalleres. Det medfører, at der ikke findes en biometrisk database ved ovennævnte handlinger, hvorfor oplysninger konstateres at være slettet permanent.[72]

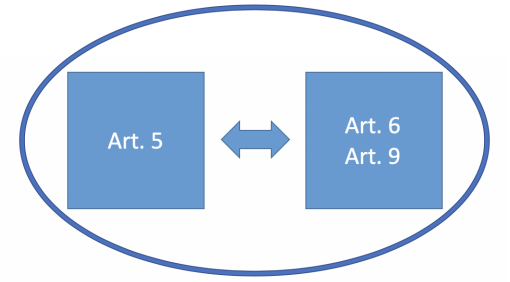
[69] Artikel 29-gruppen, WP 80, 2003, side 9.
[70] Artikel 29-gruppen, WP 193, 2012, side 33.
[71] Artikel 29-gruppen, WP 80, 2003, side 9.
[72] Artikel 29-gruppen, WP 193, 2012, side 35.

3.4.7. Sammenfatning

Helt overordnet kan det siges, at den dataansvarlige skal sikre sig, at den pågældende behandling har et lovligt grundlag. Finder den dataansvarlige behandlingshjemmel i forordningens art. 6 eller art. 9 ved behandling af biometriske personoplysninger, er det ikke alene tilstrækkeligt til at udgøre et legitimt behandlingsgrundlag.

Den dataansvarlige skal derudover også iagttage om de grundlæggende principper i forordningens art. 5 er opfyldt, der er gennemgået i nærværende afsnit. Med andre ord skal bestemmelserne være opfyldt i forening.

Dette illustreres ved nedenstående figur:



Kap. 4 Gennemgang af praksis

4.1. Indledende bemærkninger

Fremstillingen vil i det følgende forsøge at udlede, hvad Datatilsynet hidtil har tillagt vægt i vurderingen af, om en behandling er i overensstemmelse med de grundlæggende principper i forordningens art. 5.
Det ønskes desuden at illustrere, hvilke situationer en behandling går fra at være omfattet af de almindelige ikke-følsomme oplysninger til at være omfattet af følsomme oplysninger, og særligt i forlængelse af dette, hvilken konsekvens det får for den enkelte dataansvarlige i jagten på et legitimt behandlingsgrundlag.

I analysen tages udgangspunkt i Datatilsynets betragtninger suppleret af egne betragtninger og bidrag, herunder inddragelse af Artikel 29-gruppens 4 trins proportionalitetsvurdering. Denne må vurderes at være et nyttigt redskab for den dataansvarlige at inddrage i vurderingen af, hvorvidt en behandling er i overensstemmelse med proportionalitetsprincippet i forordningens art. 5, stk. 1, litra c.

Opsummerende bygger proportionalitetsvurderingen på følgende fire trin:

1. Det skal vurderes, hvorvidt det udvalgte system (teknologien) er nødvendigt for at opfylde det identificerede behov, eller om det biometriske system er udvalgt eksempelvis fordi der blot er tale om en nem og billig løsning.
2. Dernæst skal det vurderes, om det udvalgte system er effektivt i opfyldelsen af det pågældende krav med henblik på at vurdere, om systemets karakteristika er velegnet til formålet.
3. Dertil skal det vurderes, om tab af privatliv står i rimeligt forhold til det forventede udfald i form af fordele ved anvendelsen af det udvalgte system. Hvis der er tale om en praktisk fordel eller en mindre økonomisk besparelse, vil der ikke være tale om en hensigtsmæssig behandling.
4. Endeligt skal det vurderes, om der kan findes et middel, der er mindre indgribende i privatlivets fred til opfyldelsen af formålet.[73]

Ovennævnte vil i det følgende refereres til som Artikel 29-gruppens 4 trins test.

[73] Artikel 29-gruppen, WP 193, 2012, side 8.

Som et redskab til analysen er følgende analyseskema udarbejdet, som i forenklet udgave er indsat herunder. Formålet med skemaet er at danne et overblik på tværs af de i fremstillingen behandlede afgørelser til sammenligning og vurdering.

AFGØRELSE	PDL § 6	GDPR ART. 9	GDPR ART. 6	PROPORTIONELT?	
				Ja	Nej
BORNHOLMERKORTET (A)	X	X		X	
MOTIONSCENTRET (B)	X	X			X
SAS (C)	X		X	X	
BLODDONATION (D)	X	X			X
UDDEVALLA	X	X		(X)	(X)

Som det kan udledes af analyseskemaet ovenfor, så gælder det for mange af de inddragne afgørelser, at den pågældende behandling har skiftet oplysningskategori, således behandlingen, der før var omfattet af art. 6 om almindelige oplysninger, nu med forordningens ikrafttræden er omfattet af art. 9 om særlige kategorier af oplysninger.
Som tidligere nævnt i fremstillingen har det afgørende betydning for, hvorvidt der er tale om en identifikationsløsning eller en verifikationsløsning. Det er endvidere bestemmende for, hvor behandlingshjemlen skal findes.

Da afgørelserne fra Datatilsynet er truffet på baggrund af tidligere gældende lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven), sondres der mellem tidligere gældende ret og forordningen på følgende måde: Når fremstillingen i det følgende alene henviser til forordningen er det udtryk for, at der ikke er sket materielle ændringer med indførelsen af denne.

4.2. Biometrisk data skifter oplysningskategori

Tilbage i 2003 retter statsvirksomheden, Bornholmstrafikken, der transporterer passagerer, post og gods til og fra Bornholm, henvendelse til Datatilsynet[74] om, hvorvidt det er muligt inden for persondatalovens[75] rammer at behandle fingeraftryk med henblik på identifikation ved indførelsen af nyt pendler ID-kort. Sagen kaldes i afhandlingen *afgørelse A*.

Bornholmstrafikkens formål med ID-kortet er at tilbyde passagererne en rabat gennem et personligt chipkort, hvorpå kundens fingeraftryk opbevares som en matematisk værdi (en template) genereret ud fra 19 målepunkter. Det betyder, at værdien ikke forlader kortet, og udelukkende lagres på kundens eget kort - og ikke i en central database.

[74] Datatilsynets afgørelse 2003-212-0143.
[75] Lov 2000-05-31 nr. 429 om behandling af personoplysninger.

Den nævnte løsning udgør en identifikation af kunderne, som benytter ID-kortet. Når kunden rejser og vil benytte kortet, kræver det, at vedkommende checker sig ind ved en gate efter forudgående reservation, hvor kortet samt kundenummer aflæses og tjekkes i et bookingsystem. Hvis kundenummeret eksisterer, skal vedkommende scanne sin finger, hvor fingeraftrykket matches med værdien i chippen på det personlige kort.

Datatilsynet vurderer, at behandlingen er omfattet af persondatalovens § 6 om almindelige oplysninger. De vurderer også, at behandlingshjemlen vil kunne findes på baggrund af samtykke (stk. 1, nr. 1), nødvendighed i opfyldelsen af en aftale (stk. 1, nr. 2) og en interesseafvejning (stk. 2, nr. 7) - begrundet med, at Bornholmstrafikkens interesse i at sikre entydig identifikation af deres kunder (de registrerede) vejer tungere end kundens interesser.
Ifølge forordningen vil der være tale om en oplysning omfattet af art. 9 om særlige kategorier af oplysninger. Konsekvensen af, at behandlingen skifter oplysningskategori er, at behandlingen udelukkende kan bero på et samtykke fra den registrerede, jf. art. 9, stk. 2, litra a, modsat tidligere, hvor hjemlen kunne findes i hele tre behandlingsgrundlag.

I den forbindelse bør det bemærkes, at Datatilsynet lægger til grund, at kunderne, som indgår aftale med Bornholmstrafikken om erhvervelse af et Bornholmerkort, indgår denne aftale på baggrund af et frivilligt afgivet samtykke, samt de er bekendt med de vilkår, som gælder for aftalen.
Det bør tillægges en afgørende vægt i vurderingen, om der er tale om et frivilligt afgivet samtykke, hvorvidt der findes et alternativ til den biometriske behandling som fx et kodeord eller magnetkort.[76]
Tanken bag dette er at sondre mellem to faktorer; 1) om den registrerede reelt har mulighed for at fravælge den biometriske behandling frem for noget mindre indgribende, og 2) om det i den forbindelse så vil betyde, at den registrerede ikke har mulighed for at indgå aftale med Bornholmstrafikken om erhvervelse af et rabatkort.

Det tillægges vægt af Datatilsynet, at de biometriske oplysninger lagres på kundens eget kort, som er i kundens besiddelse. Der lagres således ikke biometriske oplysninger i en central database.

Drages paralleller til Artikel 29-gruppens 4 trins test, vil ovenstående understøtte, at tab af privatliv står i rimeligt forhold til fordelene ved anvendelsen af det pågældende system. Som det fremgår af afsnit 3.4.2 mindskes risikoen for genbrug af biometriske oplysninger og dermed viderebehandling til uforenelige formål, såfremt de biometriske oplysninger ikke lagres i centrale databaser, hvor oplysningerne er tilgængelige for tredjemand.

Det er svært at forestille sig, hvordan formålet vil kunne opnås med mindre indgribende midler, idet de biometriske oplysninger forbliver i den registreredes egen varetægt.
Man ville med fordel kunne overveje muligheden for at anvende en verifikationsløsning frem for, i tilfældet her, en identifikationsløsning. Det er dog tvivlsomt, hvorledes behandlingen vil

[76] Artikel 29-gruppen, WP 193, 2012, side 10.

kunne opfylde formålet ved en verifikationsløsning, da det jo netop er centralt, at Bornholmstrafikken skal kunne kontrollere, at det netop er X, der er i besiddelse af rabatkortet, som er berettiget til at bruge rabatordningen.

4.3. Motionscentret

Ovenstående understøttes af afgørelsen i det følgende om et motionscenter, som ønsker at etablere en biometrisk løsning med henblik på at kontrollere adgangen til centret. I fremstillingen refereres til sagen som *afgørelse B*.
Løsningen bygger, i tråd med ovenstående, også på identifikation af den registrerede, hvorfor der også her er tale om behandling af oplysninger omfattet af forordningens art. 9.[77]
Med adgangskontrolsystemet skal medlemmerne have aflæst deres fingeraftryk ved indgangen, hvor en scanner udregner en matchværdi, der holdes op mod motionscentrets centrale medlemsdatabase. De biometriske oplysninger behandles på baggrund af den registreredes samtykke, og slettes igen, når medlemskabet ophører.

Afgørelsen adskiller sig fra *afgørelse A* ved proportionalitetsvurderingen. Datatilsynet lægger i *afgørelse B* vægt på, at der er tale om en central lagring af oplysningerne, og at de biometriske oplysninger sammenstilles med andre identifikationsoplysninger. Det medfører, at den registrerede ikke er i besiddelse af de personlige oplysninger, som tilfældet er i *afgørelse A*, hvorfor den registrerede ikke har samme mulighed for at føre kontrol med oplysningerne.
Datatilsynet vurderer, at behandlingen i *afgørelse B* ikke er i overensstemmelse med de grundlæggende principper i art. 5, herunder proportionalitetsprincippet. Formålet vurderes at kunne opnås med mindre indgribende midler.

Ovenstående betyder også, at allerede fordi det vurderes, at formålet kan opnås med mindre indgribende midler, vil behandlingen ikke kunne leve op til de 4 krav i Artikel 29-gruppens 4 trins test.
Det bør overvejes, om motionscentret i stedet bør udstede et medlemskort, hvor værdierne, som lagres på kortet (i kundens egen besiddelse), matches med resultatet af en scanning af medlemmets fingeraftryk (verifikation), trods dette kan spås at være en merudgift for centret. Hertil skal der være tale om et system baseret på et frivilligt samtykke, der suppleres af et alternativ, som ikke stiller medlemmet dårligere, når den biometriske løsning (foreslået verifikation) fravælges.[78]

Sammenfattende kan det konstateres, at ovenstående afgørelser (*A og B*) illustrerer ændringen med indførelsen af forordningen, hvor behandling af biometriske oplysninger med henblik på entydig identifikation nu er omfattet af de særlige oplysningskategorier i forordningens art. 9. Det har den betydning, at behandlingshjemlen skal findes i art. 9 fremfor art. 6. Det medfører, at med de angivne formål vil det udelukkende være en mulighed at finde hjemlen på baggrund et samtykke fra den registrerede. Samtykket skal naturligvis leve op til de almindelige krav til et *frivilligt*, *specifikt*, *informeret* og *utvetydigt* samtykke.

[77] Datatilsynets afgørelse 2004-219-0208.
[78] Teknologirådets anbefaling om biometri, 2010, side 8.

Det kan endvidere konstateres, at ved vurderingen, om den pågældende behandling lever op til proportionalitetskravet i art. 5, stk. 1, litra c, skal det tillægges afgørende vægt, hvor de biometriske oplysninger lagres. Det er centralt, at den registrerede selv er i besiddelse af sine oplysninger fx på et kort eller andet medie, som er tilfældet i *afgørelse A*. Decentral lagring er altså at foretrække; også kaldet match on card teknologi.[79]

4.4. Verifikation

For at illustrere forskellen på verifikation og identifikation og konsekvensen heraf vil der i forlængelse af ovenstående gennemgås en afgørelse fra Datatilsynet om Scandinavian Airlines Danmark (SAS).[80]
Afgørelsen adskiller sig fra ovenstående afgørelser, fordi der er tale om en verifikationsløsning. I fremstillingen refereres til denne som *afgørelse C*.

Med denne afgørelse illustreres en situation, som kan siges at være mindre indgribende for den registrerede. Dog skal det holdes for øje, at alle former for behandling af biometrisk data er indgribende uanset verifikation eller identifikation.

Sagens faktiske omstændigheder er, at biometriske personoplysninger i form af fingeraftryk behandles i processen, når det skal kontrolleres om bagage og passager stemmer overens med baggrund i EU's sikkerhedskrav (i selvbetjeningsmiljø). Den biometriske oplysning, i form af en template, bliver midlertidigt lagret sammen med bagagenummer i en lokal database. Når passageren efterfølgende stiger ombord på flyet, skal vedkommende på ny have aflæst sit fingeraftryk, hvor det skal verificeres med fingeraftrykket fra indcheckning. SAS kan gennem sådan verificering fastslå, at passageren (den registrerede) hører sammen med indchecket bagage.

Ved en sammenligning af afgørelserne hhv. *afgørelse A* og *afgørelse B* er der, som nævnt ovenfor, her tale om en verifikationsløsning. Behandlingen er omfattet af forordningens art. 6 om almindelige oplysninger, hvorfor der ikke sker et skift i oplysningskategori, som er tilfældet i ovenstående afgørelser.

Datatilsynet vurderer, at behandlingen vil kunne ske på baggrund af et indhentet samtykke fra den registrerede. Samme hjemmel vil derfor kunne bruges til behandlingen efter forordningen. Det bør dog overvejes, om behandlingshjemlen vil kunne findes i interesseafvejningsreglen, jf. forordningens art. 6, stk. 1, litra f. Denne mulighed nævnes ikke i afgørelsen.

Ved den såkaldte interesseafvejningstest i forordningens art. 6, stk. 1, litra f, skal følgende vurderes; den dataansvarliges *legitime interesse*, indvirkningen på den registrerede ved den konkrete behandling, den foreløbige balance mellem den dataansvarliges legitime interesser og indvirkningen på den registrerede, og til sidst eventuelle yderligere garantier, som den

[79] Teknologirådets anbefaling om biometri.
[80] Datatilsynets afgørelse 2006-219-0370.

dataansvarlige kan anvende for at forhindre uhensigtsmæssig indvirkning på den registrerede ved den påtænkte behandling.[81]

På den ene side står hensynet til SAS om at overholde pålagte krav på EU-retligt plan. SAS pålægges at sikre, at vedkommende, som indleverer bagage til indcheckning på et fly, er samme person, som rejser med flyet. Dette er et krav efter EU forordning nr. 2320/2002 for alle flyselskaber. I tilknytning hertil har SAS til formål at gennemføre specifikke biometriske løsninger til at kontrollere bagage, som indcheckes.

På den anden side står indvirkningen på passageren (den registrerede) ved den konkrete behandling. Her er det centralt at bemærke, at behandling af biometriske oplysninger i sig selv er indgribende i den registreredes rettigheder og frihedsrettigheder, hvorfor det kan tale for, at interesseafvejningstesten vil falde ud til fordel for den registrerede.

Dog skal det sidste led inddrages, nemlig om eventuelle yderligere garantier, som den dataansvarlige kan anvende, vil kunne forhindre uhensigtsmæssig indvirkning på den registrerede. I den forbindelse er det vigtigt, at det er en verifikationsløsning, hvor der genereres en template ud fra den registreredes fingeraftryksaflæsning. Det er alene template, som lagres i den centrale database, og denne sammenstilles derfor ikke med andre identifikationsoplysninger om den registrerede.
Template lagres i relativ kort tid. Det oplyses, at den lagres typisk mellem 20 - 60 min. Dog højst et par timer, hvis der er tale om forsinkelser eller skift af fly med videre. Når passageren stiger ombord på flyet, og har verificeret, at bagagen tilhører den pågældende, slettes template fra systemet.[82]

Hvis behandlingen *ikke* vurderes at kunne rummes inden for ovenstående, må hjemlen bestå af et samtykke fra den registrerede, som allerede er tilfældet. Samtykket skal leve op til de specifikke krav til et gyldigt samtykke, og der skal være et alternativ til den biometriske behandling. Det fremgår, at der findes et alternativ i form af at passagerer, som ikke ønsker at få aflæst deres fingeraftryk, har mulighed for at benytte sig af en manuel ID kontrol.

Datatilsynet vurderer, at behandlingen er i overensstemmelse med de grundlæggende principper i art. 5, herunder proportionalitetsvurderingen. Datatilsynet lægger vægt på de samme elementer, som er behandlet ovenfor, at der alene er tale om lagring af en template, at denne template ikke sammenstilles med andre identifikationsoplysninger om den registrerede, og at lagringsperioden er relativ kort, hvorfor oplysninger slettes fra databasen relativt hurtigt igen.

Det er generelt helt afgørende, at der er tale om en verifikationsløsning. I den forbindelse er det relevant at inddrage fremstillingens tidligere beskrivelser af hhv. verifikation og identifikation.

[81] Artikel 29-gruppen, WP 217, 2014, side 35 nederst.
[82] På side 44 i Artikel 29-gruppen, WP 217, nævnes eksempler som begrænsning af oplysninger, der indsamles, eller krav om omgående sletning af personoplysningerne efter anvendelse.

Ved en verifikationsløsning er processen forenklet, forstået på den måde, at den kræver 1:1 matchproces, således skal der ikke registreres flere oplysninger på den registrerede end den biometriske oplysning i form af en template eller lignende.
Ved en identifikationsløsning stilles større krav til, at der indhentes flere identifikationsoplysninger om den registrerede, idet en template alene ikke er nok til at identificere en person. Behandlingen vil derfor alt andet lige være mere indgribende i den enkelte persons personlige rettigheder og frihedsrettigheder.
Ved brug af biometriske løsninger må det derfor vurderes, at verifikation er den mindst indgribende løsning. Det kan af naturlige årsager ikke undgås at påvirke proportionalitetsvurderingen i en positiv retning, hvilket også ses i Datatilsynets egne betragtninger.

Ovenstående betyder også, at ved inddragelse af Artikel 29-gruppens 4 trins test, må det vurderes, at kravene er opfyldt. Formålet vil ikke kunne opnås med mindre indgribende midler, da det er svært at forestille sig hvad det kan være. Ligesom tab af privatlivet må vurderes at stå i rimelig forhold til fordelene ved det anvendte system.
I forlængelse heraf kan det siges, at der rigtigt nok er tale om central lagring, men at lagringen er meget kortvarig, og det alene er lagring af en template, og at denne ikke sammenstilles med andre identifikationsoplysninger. Dette må også betyde, at de to første krav er opfyldt, idet effektiviteten af det pågældende system og nødvendigheden med henblik på formålet med behandlingen må vurderes at være opfyldt, allerede fordi den mindst indgribende metode er valgt.

Sammenfattende, hvis nærværende afgørelse sammenlignes med *afgørelse B* kan det konstateres, at lagringen af de biometriske oplysninger sker centralt frem for decentralt i begge afgørelser. I *afgørelse B* lagres ligeledes en template, men denne sammenstilles med øvrige identifikationsoplysninger om den registrerede.
Det er derfor ikke alene afgørende i forhold til proportionalitetsvurderingen, om oplysningerne lagres centralt eller decentralt, men også hvorvidt de biometriske oplysninger indsamles og behandles med det formål at identificere den registrerede eller der er tale om verifikationsløsning. Desuden tillægges det vægt, at der alene lagres en udregnet matematisk værdi i form af en template og *ikke* rene rådata såsom et billede af et komplet fingeraftryk.

4.5. Blodbanken på Rigshospitalet

Til yderligere illustration af, at det tillægges vægt, hvorvidt der lagres en template eller rene rådata, inddrages endnu en afgørelse fra Datatilsynet.[83]
Gennem borgerhenvendelser bliver Datatilsynet gjort opmærksom på, at Blodbanken på Rigshospitalet registrerer bloddonorers fingeraftryk, hvorfor tilsynet af egen drift tager sagen op i 2014. Denne afgørelse refereres i afhandlingen til *afgørelse D*.

[83] Datatilsynets afgørelse 2014-632-0081.

Formålet med anvendelsen af fingeraftrykket er at sikre, at bloddonoren ikke forveksles med en anden person, og rent faktisk er den bloddonor, som systemet forventer. Dette er vigtigt for Region Hovedstaden for at forebygge, at der sker forbytninger af blodportioner, hvilket potentielt kan være livsfarligt. Det er sjældent sket, men ifølge Region Hovedstaden er det et tilbagevendende problem.
Den tidligere anvendte metode gik ud på, at bloddonoren under blodtapning blev spurgt om sin identitet af to personalemedlemmer, hvorfor denne metode ved brug af fingeraftryk anses for mere sikkert.

Alle donorer skal afgive et komplet fingeraftryk fra præcis to af sine fingre. Det er valgfrit for den registrerede hvilke fingre, der anvendes. De biometriske oplysninger i form af rene rådata lagres derefter elektronisk i et system kaldet "Blodflödet" som billeder i bitmap-filer sammen med den registreredes cpr-nummer.
Når den registrerede skal identificeres, skal én af de to valgte fingre indlæses, og er der et match i Blodflödet, kan tappeproceduren fortsætte. Billederne af den registreredes fingeraftryk opbevares i 30 år med henblik på sporbarhed.

Til sammenligning med afgørelserne *A og B* er nærværende afgørelse også et eksempel på en behandling af biometriske oplysninger med henblik på identifikation. Datatilsynet vurderer, at forholdet er omfattet af persondatalovens § 6 om almindelige oplysninger. I det tilfælde, at fingeraftrykket afslører følsomme oplysninger om patienten, vil behandlingen være omfattet af persondatalovens § 7 om særlige kategorier af oplysninger. Det kan eksempelvis være etniske oplysninger om den registrerede, som billeder af fingeraftryk kan afsløre.[84]

Idet det er en identifikationsløsning, vil behandlingen efter gældende forordning være omfattet af art. 9 om de særlige kategorier af oplysninger. Der sker derfor også i denne afgørelse et skift af oplysningskategori.
Det betyder dog ikke i den konkrete situation, at behandlingshjemlen kun vil kunne findes på baggrund af et indhentet samtykke fra den registrerede, jf. art. 9, stk. 2, litra a.
En anden mulig behandlingshjemmel vil kunne findes i forordningens art. 9, stk. 2, litra h, hvoraf det følger, at fagpersoner, der er underlagt tavshedspligt, kan behandle følsomme oplysninger, hvis behandlingen er nødvendig med henblik på medicinsk diagnose, ydelse af sundhedsbehandling eller forvaltning af social- og sundhedsomsorg og -tjenester.

Det er værd at bemærke, at en behandling efter forordningens art. 9, stk. 2, litra h, forudsætter hjemmel i EU-retten eller medlemsstaternes nationale ret for, at forbuddet mod behandling af følsomme oplysninger i forordningens art. 9, stk. 1, kan fraviges. Det betyder, at der gives medlemsstaterne *et nationalt råderum* til at fastsætte supplerende specifikke bestemmelser om databeskyttelse under forudsætning af, at de øvrige bestemmelser i forordningen overholdes.[85]
Det betyder også, at art. 9, stk. 2, litra h, ikke vil kunne anvendes som direkte behandlingshjemmel.

[84] Artikel 29-gruppen, WP 193, 2012, side 22.
[85] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 209.

I den forbindelse skal databeskyttelsesloven inddrages. Forordningens art. 9, stk. 2, litra h, er ordret implementeret i databeskyttelseslovens § 7, stk. 3, hvorfor denne i stedet vil kunne anvendes som direkte behandlingshjemmel.[86]

Der henvises desuden til Bekendtgørelse nr. 1230 af 8. december 2005 om kvalitets- og sikkerhedskrav til bloddonorvirksomhed som supplerende national hjemmel til at behandle følsomme oplysninger i forbindelse med blodtapning.
Det følger af bekendtgørelsens § 8, at en bloddonorvirksomhed skal registrere og opbevare oplysninger om identifikation af bloddonor. Det er understreget i bilag 1 til bekendtgørelsen, at ansvaret for at sikre kontrol af bloddonors identitet ligger hos blodbanken. Det udpensles, at proceduren for blodtapning skal foregå således, at bloddonors identitet kan kontrolleres og registreres sikkert, og at forbindelsen klart skal fastslås mellem donor, blod, blodkomponenter og blodprøver.

Med ovennævnte skal det præciseres, at det ikke følger direkte af ordlyden, hverken i databeskyttelsesloven eller i bekendtgørelsen, at formålet lovligt vil kunne opnås ved hjælp af en biometrisk løsning. En biometrisk behandling ses dog at kunne opfylde de krav, der stilles til bloddonorvirksomheden, hvorfor man ikke afvisende kan sige, at biometrisk behandling ikke kan komme på tale.

I den forbindelse skal også inddrages det faktum, at forordningens art. 9, stk. 2, litra h, indeholder et krav om *nødvendighed.* Det er op til den dataansvarlige at vurdere, hvorvidt den pågældende behandling er nødvendig.[87]
Spørgsmålet er, om nødvendighedskravet indeholder et krav til den dataansvarlige at tage stilling til, om det er nødvendigt at behandle de pågældende personoplysninger ved hjælp af en biometrisk løsning? Det må formodes at skulle besvares bekræftende.

Når hensynet til forebyggelsen af personforveksling tages i betragtning, kan det i hvert fald vurderes, at brug af en biometrisk løsning i højere grad giver mulighed for sikker identifikation af den registrerede, hvilket netop vil minimere risikoen for personforveksling, som kan få fatale konsekvenser for en given patient.

Spørgsmålet er, om forordningen med det nationale råderum, tillader brug af biometriske løsninger, når det ikke fremgår direkte af den nationale lovs ordlyd? Eller er det nok, at der er hjemmel til den pågældende behandling af de, i tilfældet, følsomme oplysninger, hvor måden, hvorpå behandlingen skal ske, ikke er fastlagt i ordlyden?

Af bet. nr. 1565 fremgår det, at *det antages,* at offentlige myndigheder vil kunne anvende biometriske personoplysninger med hjemmel i forordningens art. 9, stk. 2, litra f.[88]

[86] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 223-224.
[87] Betænkning om databeskyttelsesforordning (2016/679) nr. 1565, side 195.
[88] Datatilsynets afgørelse 2010-323-0140.

Dette understøtter ovenstående overvejelser, og det kan derfor ikke afvises, at der kan ske behandling af biometriske oplysninger uden denne mulighed fremgår direkte af ordlyden.[89]

I vurderingen af om de grundlæggende principper overholdes skal lagringens længde også inddrages. Det oplyses, at de biometriske oplysninger lagres i 30 år. Den lange slettefrist begrundes med, at det følger af bekendtgørelse nr. 1230 af 8. december 2005 om kvalitets- og sikkerhedskrav til blodbankvirksomhed §§ 8 og 10.
Datatilsynet vurderer ikke på trods af, at der henvises til kravene i bekendtgørelsen, at der er holdepunkter for, at de biometriske oplysninger skal gemmes i 30 år. Med andre ord er de *biometriske* oplysninger ikke nødvendige for opbevaringen i 30 år. De oplysninger, der er tale om i bekendtgørelsen, handler om forbindelsen mellem donor, blod, blodkomponenter og blodprøver. At Region Hovedstaden forklarer i forlængelse heraf, at donor kan få slettet sine oplysninger på anmodning retfærdiggør ikke den lange slettefrist.

Endeligt er det centralt i nærværende afgørelse, at der ikke genereres en template ud fra den registreredes fingeraftryk - tværtimod lagres et billede af den registreredes komplette fingeraftryk. Dette er også tidligere i fremstillingen beskrevet som rådata, som er de data, der indhentes i registreringsfasen, hvor der typisk efterfølgende genereres en template eller lignende ud fra disse.
Datatilsynet vurderer, at behandlingen vil kunne udføres med mindre indgribende midler. Her henvises til de øvrige omtalte afgørelser i nærværende fremstilling, hvor der alene lagres templates og altså ikke et billede af et komplet fingeraftryk.

I forlængelse af ovenstående er det vigtigt at have for øje, at både Datatilsynet i nærværende afgørelse og Artikel 29-gruppen i deres arbejdsdokument fra 2003[90] forholder sig til det faktum, at brug af template er den sikreste metode frem for lagring af et komplet fingeraftryk. Når der anvendes forskellige algoritmer i forskellige systemer, vil den matematiske værdi ikke være den samme hos én dataansvarlig som hos en anden dataansvarlig. Når forskellige algoritmer anvendes, vil muligheden for at samkøre to databaser være begrænset. Derved afskæres oplysningerne fra at blive anvendt uretmæssigt eller til uforenelige formål.
Et komplet billede af et fingeraftryk vil også kunne medføre, at aftrykket kan reproduceres og anvendes i andre sammenhænge. Det er derfor Datatilsynets opfattelse, at risikoen for misbrug er væsentligt højere, når billeder lagres sammen med den registreredes cpr-nummer, som det er tilfældet i denne sag.

Allerede fordi det vurderes, at formålet kan opnås med mindre indgribende midler og i særdeleshed, at tab af privatliv ikke står i rimelig forhold til fordelene ved anvendelsen af det pågældende system, vil kravene i Artikel 29-gruppens 4 trins test ikke være opfyldt.
Det er oplagt at overveje, om brug af en genereret template vil kunne imødekomme formålet med behandlingen.

[89] Betænkning om databeskyttelsesforordning (2916/679) nr. 1565, side 216.
[90] Artikel 29-gruppen, WP 80, 2003, side 33.

Derudover skal det også bemærkes, at der her er tale om central lagring frem for decentral lagring. Det bør derfor overvejes, om et mindre indgribende middel kunne være, at oplysningerne lagres decentralt. Datatilsynet nævner dog ikke dette forhold i afgørelsen, hvilket kan tyde på, at det ikke tillægges vægt.
Det kan dog ud fra gennemgang af de øvrige afgørelser vurderes, at det vil være muligt med en decentral lagring til opfyldelsen af dette formål. Det beskrives i afgørelsen, at der er valgt lagring af et komplet fingeraftryk frem for en genereret template på baggrund af økonomisk besparelser, hvorfor det må antages, at en decentral løsning også vil være for dyrt i denne sammenhæng. Det er dog netop ikke en legitim begrundelse for at anvende det pågældende system, hvilket kommer til udtryk i både trin 1 og 2.

Ved sammenligning af de øvrige gennemgået afgørelser ovenfor har Datatilsynet nærmest konsekvent lagt vægt på, at registreringen af biometriske oplysninger alene omfatter biometriske skabeloner - templates - og ikke et billede af et komplet fingeraftryk. Det er derfor afgørende for, at behandlingen ikke er i overensstemmelse med de grundlæggende principper, herunder proportionalitetsprincippet, i denne afgørelse, at der lagres et komplet fingeraftryk frem for blot en template.

4.6. Sammenfatning på Datatilsynets afgørelser

Ud fra gennemgang af ovenstående afgørelser fra Datatilsynet kan det konstateres, at forordningens ikrafttræden har medført, at flere af de biometriske løsninger med henblik på *identifikation* nu er omfattet af særlige kategorier af oplysninger. Det betyder, at den dataansvarlige skal finde behandlingshjemmel i forordningens art. 9 om de særlige kategorier af oplysninger frem for i art. 6 om almindelige oplysninger.
Som det ses i *afgørelse A* om Bornholmerkortet, får det den konsekvens, at mulige behandlingshjemler begrænses til indhentelse af samtykke fra den registrerede, idet behandlingen ikke kan rummes inden for de andre undtagelsers anvendelsesområde i forordningens art. 9, stk. 2.
I den forbindelse skal det bemærkes, at den dataansvarlige har pligt til at opfylde forordningens opstillede krav til et gyldigt samtykke. I forlængelse af dette er det væsentligt, at den registrerede reelt har mulighed for at fravælge den biometriske løsning - altså at der findes et alternativ.

For *afgørelse D* ses det dog ikke at have samme konsekvenser som for *afgørelse A*, forstået på den måde, at *afgørelse D* ses at have flere mulige behandlingshjemler i forordningens art. 9, stk. 2. Hvis betragtningerne i betænkningen følges, må det *antages,* at offentlige myndigheder vil kunne anvende biometriske oplysninger med hjemmel i forordningens art. 9, stk. 2, litra f.

Såfremt der er tale om en behandling med henblik på *verifikation,* som er tilfældet i *afgørelse C* om SAS, sker der ingen ændringer i forhold til forordningens ikrafttræden. Sagt med andre ord; der sker ikke skift af oplysningskategori. En verifikationsløsning vil efter forordningens ikrafttræden stadig være omfattet af forordningens art. 6 om behandling af almindelige oplysninger. Det betyder også, at en verifikationsløsning vil kunne ske på baggrund af

interesseafvejningsreglen i art. 6, stk. 1, litra f, til forskel fra en behandling efter art. 9, stk. 2, som ikke indeholder samme mulighed. Den dataansvarlige er dog forpligtet til at foretage en såkaldt "interesseafvejningstest" forud for behandlingen. Behandlingen vil i øvrigt også kunne ske på baggrund af indhentet samtykke fra den registrerede, jf. forordningens art. 6, stk. 1, litra a.

I vurderingen, om behandlingen er i overensstemmelse med de grundlæggende principper i art. 5, ses det, at Datatilsynet lægger særlig vægt på, hvorvidt behandlingen er proportionel. I denne forbindelse tillægges det afgørende vægt, om der er tale om central eller decentral lagring, samt hvorvidt der lagres en template eller et billede af et komplet fingeraftryk.

I den forbindelse er Artikel 29-gruppens 4 trins test er et nyttigt redskab, når den dataansvarlige skal vurdere, hvorvidt en behandling er i overensstemmelse med de grundlæggende principper, herunder særligt proportionalitetsprincippet. Om ikke andet kan det i hvert fald siges at være et nyttigt redskab ved inddragelse i vurderingen, om hvilke tiltag der kan gøres for at mindske den pågældende behandlings indgriben i den registreredes rettigheder og frihedsrettigheder.
Hvis der er tale om central lagring af biometriske oplysninger, vil Datatilsynet være tilbøjelig til at vurdere, at der findes et mindre indgribende middel til opfyldelse af formålet, eksempelvis muligheden for decentral lagring, hvorfor behandlingen ikke vil opfylde kravene i 4 trins testen. Sådan vil det dog ikke være i alle tilfælde. Afgørelsen om SAS (*afgørelse C*) er et eksempel på central lagring, hvor Datatilsynet vurderer, trods ovenstående betragtninger, at behandlingen er i overensstemmelse med de grundlæggende principper. Her er det afgørende, at den dataansvarlige sikrer den registrerede andre garantier såsom; at der lagres en template i stedet for et komplet fingeraftryk, at der er tale om en verifikationsløsning samt afgræsning af tidsrummet, hvori oplysningerne lagres. I så fald vil kravene i 4 trins testen umiddelbart også være opfyldt. Den dataansvarlige vil dog skulle overveje, hvorvidt der findes et middel, som er mindre indgribende, som for eksempel decentral lagring.
En verifikationsløsning vil være at foretrække, idet det er det mindst indgribende middel.

Omvendt kan det konstateres, at såfremt der lagres et billede af et komplet fingeraftryk, vil det ikke kunne opfylde kravene, idet der definitivt findes et middel, som er mindre indgribende; nemlig at der lagres en template, samt at den registreredes tab af privatliv ikke står i rimelig forhold til fordelene ved anvendelsen af det pågældende system.
Konsekvensen af at anvende et billede af et komplet fingeraftryk er, at det kan skabe rammer for misbrug. Lagres et komplet fingeraftryk og sker der brud på datasikkerheden, kan det medføre, at den biometriske rådata falder i forkerte hænder og kan bruges til eksempelvis at give uberettiget adgang. Hertil kommer andre fatale konsekvenser for den personlige integritet.

Det skal tilføjes i forlængelse af ovenstående, at ved gennemgang af relevante afgørelser fra Datatilsynet kan det tyde på, at formålet med behandlingen er ret så afgørende for, hvorvidt en behandling er proportionel eller ej.
Dette illustreres ved sammenligning af afgørelserne, hvor særligt *afgørelse B* og *afgørelse D* er interessante. Der er i begge tilfælde tale om central lagring af biometriske oplysninger, men i *afgørelse B* er formålet med behandlingen knap så tungtvejende, forstået på den måde, at

formålet med behandlingen er at sikre, at motionscentret kan kontrollere, at det kun er de medlemmer, som har adgang til motionscentret, der opholder sig i centret.
Til sammenligning er formålet med behandlingen i *afgørelse D* at forhindre, at der ikke sker forbytninger af blodportioner, hvilket potentielt kan være livsfarligt. Hensynene bag de to behandlinger er således vidt forskellige. I *afgørelse B* er der tale om økonomiske hensyn og i *afgørelse D* er der tale om hensynet til at sikre sundhed og undgå potentiel livsfare for en given patient. Som det ses af gennemgangen vurderer Datatilsynet, at behandlingen ikke er proportionel med formålet i *afgørelse B*, hvor det ikke er tilfældet i *afgørelse D*, men nærmere at det er problematisk, at der lagres et komplet fingeraftryk i en central database frem for en template eller lignende.
Ovenstående betragtninger understøttes af analysen af *afgørelse C*. Formålet med behandlingen tager her afsæt i sikkerhedsmæssige hensyn.

Det understøttes også af afsnit 3.4.2, hvori det anføres ved behandling af biometriske oplysninger, at der er en klar forudsætning for, at formålet med behandlingen er defineret og udspecificeret. Især fordi at behandling af biometriske oplysninger i sig selv er særlig indgribende i personers grundlæggende rettigheder og frihedsrettigheder.

4.7. Tallriksautomater i Uddevalla

Der findes endnu ikke eksempler i dansk retspraksis på, hvor domstolene har taget stilling til brugen af biometriske løsninger i forhold til databeskyttelseslovgivningen. Der findes dog eksempler på dette i vores naboland, Sverige. I fremstillingen inddrages derfor relevant svensk retspraksis som et supplement til analysen af Datatilsynets afgørelser. Sagen skiller sig ud på følgende måde, at det svenske datatilsyns beslutning behandles ved domstolene i tre instanser.

I følgende analyse af Datainspektionens beslutning og domstolenes afgørelser vil indgå henvisning til disses betragtninger suppleret af egne betragtninger. Hvor egne betragtninger inddrages, henvises kun til forordningen, idet svensk ret anses for værende i overensstemmelse hermed.

4.7.1. Resumé

Et gymnasium i Uddevalla anvender "tallerken-automater" med fingeraftrykslæsning. Formålet med systemet er at identificere de elever, som spiser i madsalene på gymnasiet. Der serveres mad i fire sale og i tre af salene benyttes det biometriske system.
Det foregår således, at eleverne skal indtaste deres egen firecifret kode og lade deres fingeraftryk aflæse for at få udleveret en tallerken i madsalen. Det er ca. 30 målepunkter fra en elevs finger, som lagres i systemet. Der lagres således ikke et komplet fingeraftryk, men en template. De 30 målepunkter lagres sammen med en personlig kode i én database. I en anden separat database lagres elevernes efternavn, klasse og den personlige kode. I samme database lagres oplysninger om, hvor mange måltider eleverne må spise pr. termin, og hvor mange måltider de allerede har "forbrugt".

Alle elever registreres i systemet på første ud af tre år. Oplysningerne er derfor lagret i systemet i 3 år i alt. De elever, som ikke ønsker at spise mad i madsalene, deaktiveres fra systemet. Hertil oplyses det, at det er nemmest at registrere alle elever efter klasselister, idet de fleste elever spiser i madsalene. Hvis en elev afslutter sit skoleforløb eller ikke betaler for skolemaden, deaktiveres elevens konto. Hvert år i august slettes elever, som har afsluttet skoleforløbet og nye registreres.

Elever og forældre informeres *ikke* om den biometriske løsning. Der indhentes heller *ikke* samtykke til indsamling og behandling af personoplysningerne. De elever, som ikke ønsker at benytte sig af systemet, er henvist til at købe madkuponer, som er en dyrere løsning.

4.7.2. Datainspektionens bemærkninger[91]

Det svenske datatilsyn, *Datainspektionen,* henviser til de grundlæggende principper i personuppgiftslagens § 9.[92] Som det ses, er disse principper stort set identiske med forordningens grundlæggende principper.

Personuppgiftslagen 9 §: *Den personuppgiftsansvarige skall se till att* *A. personuppgifter behandlas bara om det är lagligt,* *B. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,* *C. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,* *D. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,* *E. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,* *F. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,* *G. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,* *H. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och* *I. personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. [...]*	***Personuppgiftslagen 10 §:*** *Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att* *A. ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,* *B. den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,* *C. vitala intressen för den registrerade skall kunna skyddas,* *D. en arbetsuppgift av allmänt intresse skall kunna utföras,* *E. den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller* *F. ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.*

Datainspektionen vurderer, at behandlingen skal betragtes som en behandling af almindelige oplysninger. Da der er tale om en identifikationsløsning, vil behandlingen efter forordningen

[91] Datainspektionens beslutning 1601-2004.
[92] Personuppgiftslag, SFS nr.: 1998:204.

være omfattet af art. 9. Der vil derfor også her ske et skift i oplysningskategori som set i tidligere afgørelser i fremstillingen.

Det tillægges vægt, at registreringen trods det, at der ikke er registreret et billede af et komplet fingeraftryk, og oplysningerne ikke er følsomme oplysninger efter loven, betragtes som en indtrængen i den personlige integritet.
Datainspektionen finder, at formålet bør opnås med mindre indgribende midler. Det vurderes, at behandlingen strider imod de grundlæggende principper i personuppgiftslagens § 9, herunder at behandlingen ikke er adækvat og relevant i forhold til formålet med behandlingen samt at der behandles flere oplysninger end nødvendigt. Med andre ord vurderer Datainspektionen, at behandlingen ikke opfylder proportionalitetsprincippet.

Der henvises desuden til Artikel 29-gruppens arbejdsdokument om biometri fra 2003, hvor det bl.a. udtales, at behandling af biometriske oplysninger udgør en potentiel risiko for, at samfundet bliver mindre bevidst om, hvordan behandling af deres oplysninger kan påvirke deres hverdag.

4.7.3. Ländsrättens bemærkninger[93]

Det samme standpunkt indtager Ländsrätten i Stockholm. De er enige med Datainspektionen om, at formålet bør opnås med mindre indgribende midler.
Retten tilslutter sig synspunktet om, at de behandlede oplysninger ikke kan anses for at adækvate, relevante eller nødvendige i forhold til formålet med behandlingen.

4.7.4. Kammarrättens bemærkninger[94]

Kammarrätten er dog *ikke* enig i ovenstående betragtninger. De vurderer, at behandlingen *er* i overensstemmelse med de grundlæggende principper i personuppgiftslagens § 9.
Retten afviser desuden Datainspektionens henvisning til Artikel 29-gruppens udtalelse om, at behandling af biometrisk data kan medføre, at et barn gøres mindre opmærksom på de risici, som kan opstå senere i livet i forbindelse med denne behandling af personoplysninger. Der henvises til, at eleverne på gymnasiet i Uddevalla er 15 år og og ældre.

Kammarrätten behandler, som den første instans, spørgsmålet om, hvorvidt behandlingen kræver samtykke fra de registrerede (eleverne), eller om behandlingen kan rummes inden for en anden behandlingshjemmel. I den forbindelse henvises der til personuppgiftslagens § 10 (indsat ovenfor), som regulerer, hvornår der er hjemmel til at behandle personoplysninger efter loven. Udover, at det kan ske på baggrund af et samtykke fra den registrerede, kan det også ske ud fra en interesseafvejning.

Det skal herefter vurderes, hvorvidt behandlingen er nødvendig for at forfølge et formål, som tilgodeser den dataansvarlige, og om denne interesse vejer tungere end den registreredes interesse i beskyttelse mod krænkelse af den personliges integritet.

[93] Länsrättens afgørelse 2458-05.
[94] Kammarrättens afgørelse 1982-05.

Kammarrätten vurderer, at gymnasiets behov for at have et smidigt og enkelt system til at kontrollere, at det kun er de elever, som har betalt for skolemaden, der spiser det, vejer tungere end de registreredes interesse i beskyttelse af deres personlige integritet. Kammarrätten vurderer derfor, at behandlingen kan finde sted uden at der indhentes samtykke fra de registrerede.

I den forbindelse skal det bemærkes, at som konsekvens af at den pågældende behandling ikke længere vil være omfattet af kategorien for almindelige oplysninger, vil hjemlen kun kunne findes på baggrund af et indhentet samtykke fra de registrerede. Som det tidligere er omtalt, findes der ingen interesseafvejningsregel i forordningens art. 9.

Der henvises her til tidligere bemærkninger vedrørende kravene til et gyldigt samtykke. Samtykket kan kun anses for at være afgivet frivilligt, såfremt den registrerede har et reelt valg. Den registrerede skal derfor kunne afvise at afgive sit samtykke uden det kommer vedkommende til skade. Det er beskrevet, at de registrerede har mulighed for at fravælge den biometriske løsning, men i så fald er henvist til at købe madkuponer, som findes at være en dyrere løsning for den enkelte. Det vil kunne afholde elever fra at vælge den alternative løsning, idet det er den dyreste. Køb af madkuponer vil derfor ikke udgøre et gyldigt alternativ, hvilket vil resultere i at de registreres samtykke til behandlingen ikke vil udgøre et gyldigt samtykke.[95]

4.7.5. Regeringsrättens bemærkninger[96]

Regeringsrätten er til dels enig med Kammarrätten. Retten vurderer, at der ikke foreligger andre oplysninger i sagen end at de indhentede oplysninger, er nødvendige for at formålet med behandlingen kan opnås. De bemærker til dette, at det ikke ændrer på vurderingen, om behandlingen af oplysningerne er adækvat og relevant, at det er biometriske oplysninger som indhentes og behandles. De vurderer, at behandlingen ikke strider imod de grundlæggende principper i personuppgiftslagens § 9.

Regeringsrätten konstaterer herefter, at gymnasiet ikke har indhentet samtykke i forbindelse med indsamling og behandling af oplysningerne.
De anfører i den forbindelse, at behandling af biometrisk data med henblik på identifikation kan opfattes af mange som følsomme oplysninger. Oplysningerne findes i databaser, som er tilgængelige for gymnasiet, og oplysningerne lagres i længere tid. De vurderer derfor, at der bør tages særlige hensyn til de registreredes personlige integritet.

De tillægger også vægt, at der alene lagres et partielt fingeraftryk (en template) og ikke et billede af et komplet fingeraftryk.

Regeringsrätten konkluderer på baggrund af ovenstående - og på baggrund af det faktum, at gymnasiets interesse i at identificere eleverne vil kunne ske ved andre metoder - at behandlingen *er* tilladt under forudsætning af, at der indhentes samtykke fra de registrerede.

[95] Præambelbetragtning nr. 42 til forordning 2016/679.
[96] Regeringsrättens afgørelse 6588-05.

4.8. Sammenfatning på svensk retspraksis

Sagen vidner om, at vurderingen, om en behandling af biometriske oplysninger er i overensstemmelse med databeskyttelseslovgivningen, ikke er let.

Datainspektionen og Landsrätten har begge vurderet, at behandlingen ikke er overensstemmelse med de grundlæggende principper, og at formålet bør opnås med mindre indgribende midler. Kammarrätten og Regeringsrätten kommer frem til det modsatte resultat; de vurderer ikke, at behandlingen strider imod de grundlæggende principper, herunder proportionalitetsprincippet.
Der gives ikke megen information om, hvad der specifikt tillægges vægt. Det kan dog tyde på, at domstolene giver den dataansvarlige videre adgang til at behandle biometriske oplysninger.
I forlængelse heraf skal bemærkes, at Kammarrätten sågar også vurderer, at behandlingshjemmel kan findes i interesseafvejningsreglen, idet Kammarrätten vurderer, at gymnasiets interesse i at behandle oplysningerne vejer tungere end interessen i beskyttelse af de registreredes integritet.
Dette modificeres dog i Regeringsrätten, da de vurderer, at behandlingen kan betragtes som værende følsom for de registrerede, samt at der skal tages særlige hensyn til elevernes integritet, hvorfor behandlingen kun vil kunne finde sted ved indhentelse af samtykke.

Det skal bemærkes, at det ikke længere vil være muligt at finde hjemmel i interesseafvejningsreglen. Dette er en konsekvens af, at forholdet ikke længere vil være omfattet af art. 6 om behandling af almindelige oplysninger, men i stedet omfattes af art. 9 om følsomme oplysninger. Der findes ingen interesseafvejningsregel i art. 9, stk. 2.
Når den pågældende behandling kun vil kunne ske på baggrund af et indhentet samtykke, skal forordningens krav til et gyldigt samtykke naturligvis iagttages.

Datainspektionen bemærker, at selvom det ikke er tilfældet, at der er tale om lagring af et billede af et komplet fingeraftryk, så finder Datainspektionen, at behandlingen strider imod de grundlæggende principper.
Ovenstående kan tyde på, at lagring af template frem for et billede af et komplet fingeraftryk ifølge Datainspektionen ikke legitimerer en behandling, selvom det må vurderes at være det mindst indgribende. Regeringsrätten lader det dog indgå i deres vurdering som et argument for, at behandlingen *ikke* strider imod de grundlæggende principper.

Det faktum, at Datainspektionen og Regeringsrätten inddrager brug af template, bevidner, at lagring af template kontra lagring af et billede af et komplet fingeraftryk er en faktor i vurderingen, om en biometrisk løsning findes overensstemmende eller ej. Det kan dog konstateres, at Datainspektionen ikke tillægger det samme vægt som det danske Datatilsyn. Det vides dog ikke, hvorvidt Datainspektionen i stedet har tillagt andre momenter afgørende vægt, som er faldet ud til fordel for de registrerede.

Afslutningsvist kan det undre, at decentral og central lagring ikke nævnes eller behandles, da det bemærkes, at Datainspektionen inddrager Artikel 29-gruppens vejledninger. Dermed

foreligger der ikke tvivl om eksistensen heraf. Dog er det svært at konkludere på dette, da det ikke er klart om det er tillagt vægt, men ikke nedskrevet.

Kap. 5 Konklusion

Det er en forudsætning for at behandle personoplysninger omfattet af forordningen, at den dataansvarlige sikrer et legitimt behandlingsgrundlag. Princippet er lovfæstet i art. 5, stk. 1, litra a, hvor der stilles et generelt krav om lovlighed. Det betyder, at vedkommende skal sikre et lovligt behandlingsgrundlag, samt at de grundlæggende principper i forordningens art. 5 overholdes.

Det er med denne fremstilling forsøgt at give læseren en bredere forståelse for, hvad den dataansvarlige skal være særligt opmærksom på med henblik på efterlevelsen af dette.

Først og fremmest kan det konkluderes ud fra analysen af Datatilsynets afgørelser og svensk retspraksis, at mange biometriske løsninger nu vil være omfattet af forordningens art. 9 om særlige kategorier af oplysninger, hvor behandlingen, inden indførelsen af forordningen, var omfattet af almindelige oplysninger i art. 6. Det er her afgørende, om der er tale om verifikation eller identifikation. Dette vil i nogle tilfælde betyde, at mulige behandlingshjemler indskrænkes, således at behandlingen kun vil kunne finde sted på baggrund af et indhentet samtykke fra den registrerede.

Der kan af analysen udledes helt centrale parametre i vurderingen, om en behandling er i overensstemmelse med de grundlæggende principper i forordningens art. 5. Datatilsynet er særligt opmærksom på proportionalitetsprincippet, men også blandt andet hvor længe de pågældende oplysninger lagres. I vurderingen, hvorvidt behandlingen er i overensstemmelse med proportionalitetsprincippet, er følgende parametre centrale; hvorvidt der er tale om central eller decentral lagring, og hvorvidt der lagres en template eller lignende eller der lagres rene rådata.
I den forbindelse vil det være nyttigt for den dataansvarlige at inddrage Artikel 29-gruppens 4 trins test.
Hvis der er tale om central lagring af biometriske oplysninger, vil Datatilsynet være tilbøjelig til at vurdere, at der findes et mindre indgribende middel til opfyldelse af formålet, eksempelvis muligheden for decentral lagring, hvorfor behandlingen ikke vil opfylde kravene i 4 trins testen. Sådan vil det dog ikke være i alle tilfælde. Såfremt den dataansvarlige anvender en verifikationsløsning, vil oplysningerne kunne lagres centralt. Det forudsætter dog, at den dataansvarlige sikrer den registrerede andre garantier såsom; at der lagres en template frem for rene rådata samt afgrænsning af tidsrummet hvori oplysningerne lagres. Den dataansvarlige bør dog altid overveje mulighederne for decentral lagring, da det er mindst indgribende i den registreredes rettigheder og frihedsrettigheder.

Det kan desuden konstateres, at såfremt der lagres et billede af et komplet fingeraftryk, vil det ikke kunne opfylde kravene, idet der definitivt findes et middel, som er mindre indgribende; nemlig at der lagres en template, samt at den registreredes tab af privatliv ikke står i rimelig forhold til fordelene ved anvendelsen af det pågældende system.
Det kan få fatale konsekvenser for den registrerede, såfremt der lagres et komplet fingeraftryk frem for en template.

Det skal endvidere tilføjes, at selvom Datatilsynet ikke inddrager det i afgørelserne, så kan det tyde på, at formålet med behandlingen har en vis betydning for, hvorvidt en behandling kan anses for at være proportionel eller ej. Det har bl.a. den betydning, at en central lagring kan vurderes at være proportionel, netop fordi formålet med behandlingen er særligt tungtvejende og ikke blot hensynet til en privat virksomheds økonomiske interesse. Det understreger også vigtigheden af, at den dataansvarlige er omhyggelig i den indledende fase, hvor formålet med behandlingen skal angives og præciseres, som det følger af forordningens art. 5, litra b.

Det må også vurderes at være i overensstemmelse med det faktum, at behandling af biometriske oplysninger altid er særligt indgribende i den personliges rettigheder og frihedsrettigheder, uanset om der er tale om en verifikation eller identifikationsløsning.

I forlængelse heraf må det dog konkluderes, som følge af forordningens ikrafttræden, at der vil være en videre adgang for verifikationsløsninger, fordi identifikationsløsninger nu er omfattet af forordningens art. 9 om de særlige kategorier af oplysninger.

Der findes ingen dansk retspraksis på området, hvorfor det er Datatilsynets afgørelser, som er endeligt normerende i forhold til, hvornår en behandling af biometriske oplysninger er proportionel. Det bliver en anelse mere mudret ved analysen af svensk retspraksis, idet domstolene ikke ses at forholde sig til central eller decentral lagring. Udover dette er de forskellige instanser ikke enige, om den pågældende behandling er i overensstemmelse med de grundlæggende principper. Særligt skal det nævnes, at både Kammarrätten og Regeringsrätten er uenig med Datainspektionens afgørelse. Datainspektionen får kun medhold ved Landsrätten. I mangel på flere nyere afgørelser fra Datatilsynet, som har behandlet spørgsmålet om behandling af biometrisk data efter forordningen, er det således svært at sige, hvorvidt der rent faktisk er sket ændringer i proportionalitetsvurderingen.

Hvorvidt udfaldet af afgørelserne vil være det samme med forordningens ikrafttræden og dermed ovenstående ændringer til følge, kan vi kun gisne om. Allerede af den grund, at hjemlen til behandlingen skal findes i art. 9 om følsomme oplysninger, skærpes kravene til behandlingen på alle fronter.

Det kan i hvert fald konkluderes, at det ganske ofte er proportionalitetsvurderingen, som spænder ben for opfyldelsen af kravet om et legitimt behandlingsgrundlag. Det kan tyde på, særligt ved inddragelse af svensk retspraksis, at de nationale tilsynsmyndigheder og domstole ikke er enige om denne vurdering, herunder hvad der skal tillægges vægt og hvem det skal komme til gode. Det stiller krav til den dataansvarlige om at være omhyggelig i denne vurdering, i hvert fald så længe de danske domstole ikke har taget stilling til spørgsmålet.

Kap. 6 Perspektivering

Kendetegnet ved Datatilsynets afgørelser og svensk retspraksis, som behandles i fremstillingen, er for dem alle, at der er tale om situationer, hvor formålet med disse er at *kontrollere*. Begrebet *kontrol* kan vurderes at være en mere seriøs fællesnævner, hvor der skal føres tilsyn med et bestemt forhold til fordel for den dataansvarlige. Biometrien er et passende led i denne ligning.

Med afsæt i fremstillingen er det oplagt at illustrere, hvor udbredte biometriske løsninger efterhånden er blevet i takt med, at teknologien buldrer frem. Biometrien anvendes nu også i en udgave, der kan betegnes at være en *luksus* til fordel for den registrerede, der med andre ord giver forbrugeren en nemmere løsning i dagligdagen. Forbrugeren kan i dag betale alene ved at benytte sin finger i en scanner, hvor genkendelse af venestrukturen udgør det biometriske element. Det særlige ved denne situation er, at det er til fordel for forbrugeren modsat tilfældene i fremstillingen, hvor biometrien eksempelvis benyttes til at tjekke om den registrerede nu har adgang, om det nu er den registreredes bagage, der med ombord på et fly, eller om det nu er den registrerede, der kan opnå en vis rabat.[97]

Artikel 29-gruppen beskriver og forudser allerede i deres udtale fra 2012[98], at nye teknologier som eksempelvis genkendelse af blodåremønster *er* færdigudviklet, hvorfor næste skridt blot er at implementere og anvende det i hverdagssammenhænge.
Det antages, at denne teknologi er *et bæredygtigt alternativ til fingeraftryk,* som er fokus i denne fremstilling.[99] Genkendelse af venestrukturen er anvendt bredt og på tidspunktet for Artikel 29-gruppens udtale anvendtes den mest i Japan, men anvendes nu verden over. Det er os først bekendt i 2018 her i Danmark, at biometri anvendes med fokus på en nødvendighed i hverdagen som eksempelvis betaling.

Nævnte eksempel benytter teknologien, *Hitachi VeinID*, der muliggør løsningen Fingopay, som bruges i kantinerne på Copenhagen Business School. Den nordiske udbyder af informations-, kort- og betalingsservices, Nets Denmark A/S, påbegyndte en testperiode i foråret 2018 i samarbejde med det engelske firma, Sthaler, med formålet at se, hvorvidt danskerne var klar til biometrisk betaling. Spisestuerne A/S, der står for alle kantinerne på Copenhagen Business School, får nu ordningen permanent installeret til en fremtidig, nemmere betaling, da forsøgsordningen er gået langt over forventet.

Ved indsamlingstidspunktet skal den registrerede oprette en profil på udbyderens hjemmeside, hvor oplysninger som navn, e-mail og kortnummer registreres sammen med en personlig kode som sikkerhedsforanstaltning. Næste skridt er at koble biometriske oplysninger til profilen, hvor den registrerede på betalingsadressen skal have aflæst sin venestruktur i fingeren gennem en indrulleringsstation.
Målingen af venestrukturen omdannes til en unik token på 19 cifre, og lagres med de resterende oplysninger på profilen. Da den registreredes betalingskort er koblet op på denne profil, er

[97] Datatilsynets afgørelser om motionscentret, SAS og Bornholmerkortet.
[98] Artikel 29-gruppen, WP 193, 2012.
[99] Artikel 29-gruppen, WP 193, 2012, side 19.

kortet derfor også tilknyttet denne token. Når venestrukturen aflæses ved betaling, vil denne token lede efter et match i en database hos udbyderen.

Fingopay er et meget godt eksempel på, hvor udbredt biometriske behandlinger er i dag. Særligt for dette eksempel er, at biometrien udelukkende bruges til at tilbyde de forbrugere, som ønsker det, en tjeneste for at forenkle en almen kendt proces som betaling. Det er en service til kantinens gæster, hvor formålet er, at det skal kunne gå lidt hurtigere, og samtidig være nemt og bekvemt.
Det er oplyst, at der er tale om en verifikationsløsning, hvorfor forholdet vil være omfattet af GDPR art. 6. Det er åbenlyst, at behandlingen sker på baggrund af et indhentet samtykke fra den registrerede. Det er netop et tilbud til den enkelte om at benytte en forenklet betalingsmetode. Alternativet til at benytte biometrien er, at brugeren kører sit betalingskort gennem terminalen og taster pin-koden.

Drages der paralleller til fremstillingen, hvor det er konkluderet, at proportionalitetsprincippet er særlig vigtig i vurderingen af, om behandling er i overensstemmelse med GDPR, vil det være relevant at diskutere, hvorvidt vurderingen af proportionaliteten har udviklet sig. Det vil derfor også være relevant her at inddrage Artikel 29-gruppens 4 trins test.

Særligt skal det sidste led i 4 trins testen fremhæves om, hvorvidt der findes et mindre indgribende middel. Det er her væsentligt at bemærke, at der er tale om central lagring frem for decentral lagring. Det har vist sig at være afgørende i vurderingen af, om behandlingen er proportionel.
Det er dog svært at sige, om det pågældende formål vil kunne forfølges ved en decentral lagring. Hvis blikket kastes tilbage på *afgørelse A* om Bornholmstrafikken i analysen ses et eksempel på decentral lagring, hvor den genererede template lagres på et personligt smartcard, som er i kundens egen besiddelse. Man kunne overveje, om det ville være en mulighed i denne situation. Det vil dog betyde, at den registrerede alligevel ville skulle finde et kort frem fra lommen eller tasken, hvorfor vedkommende lige så godt ville kunne finde dankortet frem. Hele ideen med den biometriske løsning er jo netop, at det skal være nemt og bekvemt!

Måske Fingopay er et udtryk for, at proportionalitetsvurderingen har flyttet sig på den måde, at det ikke tillægges samme vægt i år 2019, hvor oplysningerne lagres (centralt eller decentralt). Ovenstående er i hvert fald et glimrende eksempel på, at det for alvor er blevet en realitet, at biometriske løsninger er og bliver nok i videre omfang i fremtiden, en naturlig del af vores dagligdag.

Kap. 7 Litteratur- og kildefortegnelse

7.1. Forordninger, love og forarbejder

Forordning nr. 2016/679 af 27. april 2016, "Databeskyttelsesforordningen"

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger, "Persondataloven"

Lov nr. 375 af 14. juni 1995 om Teknologirådet

Betænkning nr. 1565 af 2017 om databeskyttelsesforordningen - og de retlige rammer for dansk lovgivning.

Betænkning til lovforslag nr. 79 2011/1 over Forslag til lov om ophævelse af lov om Teknologirådet og om ændring af lov om Det Etiske Råd

7.2. Litteratur

Munk-Hansen, Carsten, Retsvidenskabsteori, Djøf Forlag, 2018, 2. udgave.

Blume, Peter, Den nye persondataret, Jurist- og Økonomforbundets Forlag, 2018, 2. udgave.

Kofoed Olsen, Birgitte, Identifikationsteknologi og individbeskyttelse - en øvelse i juridisk teknologivurdering, Jurist- og Økonomforbundets Forlag, 1998, 1. udgave.

7.3. Udtalelser og vejledninger

Artikel 29-gruppen, WP 80: Arbejdsdokument om biometri, 2003.

Artikel 29-gruppen, WP 136: Udtalelse nr. 4/2007 om begrebet personoplysninger, 2007.

Teknologirådet, "Biometri - brug af biometriske teknologier i det danske samfund", 2010.

Artikel 29-gruppen, WP 187: Udtalelse 15/2011 om definitionen af samtykke, 2011.

Artikel 29-gruppen, WP 193: Udtalelse 3/2012 om udviklingen inden for biometriske teknologier, 2012.

Artikel 29-gruppen, WP 217: Udtalelse 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF, 2014.

7.4. Artikler

Tranberg, Charlotte B., Biometriske personoplysninger, ET.2007.105.

7.5. Praksis fra datatilsyn

7.5.1. Datatilsynet (j.nr.)

2003-212-0143, Fingeraftryk på Bornholmerkort

2004-219-0208, Adgangssystem til motionscenter baseret på fingeraftryk

2006-219-0370, Anvendelsen af biometri ved indcheckning af bagage

2014-632-0081, Brug af fingeraftryk ved bloddonation

7.5.2. Datainspektionen (d.nr.)

1601-2004, Tallriksautomat Uddevalla.

7.6. Fremmed ret

Personuppgiftslagen SFS 1998:204.

7.7. Svensk retspraksis

Länsrätten i Stockholm Län. Dom af 2. marts 2005 i 2458-05, Tallriksautomat Uddevalla.

Kammarrätten i Stockholm. Dom af 1. november 2005 i 1982-05, Tallriksautomat Uddevalla.

Regeringsrätten i Stockholm. Dom af 16. december 2008 i 6588-05, Tallriksautomat Uddevalla.


Ordoptælling
Statistik:
Sider 57
Ord 20.016
Tegn (uden mellemrum) 118.081
Tegn (med mellemrum) 137.915
Afsnit 688
Linjer 2.263
Medtag fodnoter og slutnoter
Luk