Biometri og GDPR

Innsamling av biometriske opplysninger med fokus på samtykke som behandlingsgrunnlag

Kandidatnummer: 11

Antall ord: 14 976

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

08.06.2020

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Den teknologiske utviklingen har de siste årene medført økt bruk av biometri for å fastslå eller bekrefte en persons identitet. Biometri er et system for automatisert måling av en persons kroppslige kjennetegn, som for eksempel fingeravtrykk, ansiktsform, irismønster og stemme.[1] Utviklingen i biometrisk teknologi har gjort det mulig for bedrifter og offentlige myndigheter å ta i bruk mer effektive, sikrere og økonomisk gunstige løsninger for identifikasjon. Fingeravtrykksgjenkjenning, ansiktsgjenkjenning og irisgjenkjenning brukes blant annet i dag til å åpne smarttelefoner og som ledd i adgangskontroll. Ansiktsgjenkjenningsteknologien kan videre implementeres i kameraovervåkningssystemer og en persons stemme kan brukes til å bekrefte hvorvidt en person er den han gir seg ut for å være. Fordelene med slike systemer er mange og bruken øker i omfang.

Til tross for en rekke fordeler med biometrisk identifikasjon, kan dens spesielle karakter ved å være knyttet uløselig til en persons kroppslige kjennetegn også være problematisk for den enkeltes personopplysningsvern.[2] Ettersom opplysningene er permanente, kan de ikke endres om de skulle komme på avveie. Dette skiller biometri fra andre identifikasjonsmetoder som passord og andre innloggingsformer, og gjør at de kan bli spesielt utsatt for misbruk. [3] Bekymring rundt utviklingen av denne typen teknologi har dermed særlig vært knyttet til automatisering av kroppslige kjennetegn med mulighet for videre bruk, innføring av systemer for sosial kontroll og risikoen for feilaktige resultater.[4] Disse utfordringene adresseres nå ytterligere i EUs personvernforordning (General Data Protection Regulation - heretter «GDPR», «forordningen» eller «personvernforordningen»)[5]. Det er nå inntatt en egen definisjon av biometriske opplysninger i art. 4 nr. 14 og biometriske opplysninger med det

[1] Nancy Yue Liu, *Bio-privacy: Legal Challenges for Privacy Regulations of Biometric Identification and Authentication,* Det juridiske fakultet, Universitetet i Oslo 2010, s. 31.
[2] Datatilsynet, «Biometri», 17. juli 2019, https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (lest 19. mars 2020).
[3] CNIL, «Facial recognition for a debate living up to the challenges», 15. november 2019, https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf (lest 11. februar 2020) s. 6.
[4] Christopher Kuner, Lee A. Bygrave og Christopher Docksey, *The General Data Protection Regulation: a commentary,* Oxford 2020 s. 209.
[5] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (GDPR).

«formål å entydig identifisere en fysisk person» er inntatt som en særlig kategori av personopplysninger etter art. 9 nr. 1.

Mer konkret er masteroppgaven en rettslig analyse av kravene til innsamling av biometriske opplysninger med fokus på samtykke som behandlingsgrunnlag etter GDPR. Innsamling er en form for «behandling» som er definert i art. 4 nr. 2 som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger». Fra det tidspunkt en person har gitt fra seg biometriske opplysninger, har vedkommende gitt fra seg kontrollen over opplysninger om seg selv som kan utsettes for misbruk og behandling uten den registrertes kunnskap. Det vil derfor vurderes hva som skal anses som biometriske opplysninger etter definisjonen i art. 4 nr. 14 og når biometriske opplysninger skal anses som en særlig kategori av personopplysninger etter art. 9 nr. 1.

Det er et sentralt personvernrettslig hensyn at den enkelte skal kunne ha kontroll over egne personopplysninger.[6] Samtykke som grunnlag for lovlig behandling av personopplysninger vil i denne forbindelse kunne ivareta hensynet til den enkeltes selvbestemmelsesrett og kontroll over egne personopplysninger. Dette forutsetter imidlertid at samtykket er gyldig for å unngå at kontrollen blir illusorisk.[7] Kravene til samtykke har både i tiden før og etter GDPR reist en rekke spørsmål og usikkerhet rundt hva som skal til for at et samtykke kan anses gyldig.

Ved bruk av biometrisk identifikasjon vil det i mange tilfeller være aktuelt å bygge på samtykke som behandlingsgrunnlag. Biometrisk identifikasjon med samtykke som behandlingsgrunnlag blir i større grad tatt i bruk av banker for verifisering av kundene, på arbeidsplasser og av andre offentlige myndigheter. Det er derfor sentralt å analysere hvilke krav som stilles til samtykke og hvilke begrensninger som foreligger ved å bygge på dette behandlingsgrunnlaget ved innsamling av biometriske opplysninger.

[6] Jf. fortalepunkt 7.
[7] EDPB (Personvernrådet), Guidelines 05/20 on consent under Regulation 2016/679*,* s. 5, avsnitt 3. Retningslinjene om samtykke ble adoptert 4. mai 2020 og er en videreføring av Artikkel 29-gruppen, Guidelines on consent under Regulation 2016/679*,* WP259, 2018. Enhver henvisning til Artikkel 29-gruppens retningslinjer om samtykke fra 2018 anses nå som en henvisning til Personvernrådets oppdaterte versjon. Den oppdaterte versjonen inneholder videre spesifisering av lovligheten av samtykke knyttet til såkalte «cookie-walls» og eksempel 16 om skrolling og samtykke. Resten av dokumentet er i stor grad det samme med unntak av noen språklige endringer. Se EDPB, 05/20 s. 4.

1.2 Metode og rettskildebilde

EUs personvernforordning trådte i kraft 25. mai 2018, og er fortsatt et relativt nytt regelverk. Norge er bundet av forordningen gjennom EØS-avtalen vedlegg XI nr. 5 bokstav e og har inkorporert forordningen gjennom Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven). I fortolkningen av EU-retten må det tas utgangspunkt i EU-rettslig metode. I dette ligger at man skal tilstrebe en ensartet og autonom fortolkning som sikrer lik forståelse av regelverket i alle medlemsstatene.[8] I fortolkningen av EU-retten skal det dermed legges vekt på en kontekstuell og formålsrettet fortolkning av bestemmelsene.[9] Dette innebærer blant annet at forordningens fortale, forordningens øvrige bestemmelser og dens systematikk må ses i sammenheng.[10] Fortalen inneholder mer utfyllende forklaring på hvordan bestemmelsene skal forstås, og vil derfor være et viktig tolkningsbidrag. EU-domstolen har imidlertid påpekt at den ikke er rettslig bindende og at den ikke kan medføre en fortolkning i strid med en ellers klar ordlyd.[11]

Videre er det EU-domstolen som har i oppgave å tolke EU-retten, og deres avgjørelser anses for å ha prejudikatvirkning.[12] Det skal dermed foreligge gode grunner for å fravike dens avgjørelser.[13] Når det kommer til behandling av biometriske opplysninger har EU-domstolen foreløpig kun behandlet saker som gjelder politiets innsamling og oppbevaring av fingeravtrykk.[14] Manglende rettspraksis innebærer dermed et økt fokus på fortolkning av forordningen. Det er imidlertid relevante saker om biometriske opplysninger etter GDPR fra datatilsyn i Sverige, Storbritannia, Danmark, Polen og Frankrike.[15] Det vil også vises til saker

[8] Se for eksempel de forente sakene i dom av 21. desember 2011 [GC], C-424/10 og C-425/10, *Ziolkowski og Szeja mfl.,* ECLI:EU:C:2011:866, avsnitt 32.
[9] *Ziolkowski og Szeja mfl.* [GC] C-424/10 og C-425/10, avsnitt 33.
[10] Se for eksempel drøftelsen i *Ziolkowski og Szeja mfl.* [GC], C-424/10 og C-425/10, avsnitt 35-51.
[11] Dom av 19. juni 2014 [A5], C-345/13 *Karen Millen Fashions,* ECLI:EU:C:2014:2013, avsnitt 31.
[12] Halvard Haukeland Fredriksen og Gjermund Mathisen, *EØS-rett*, 3 utg. Fagbokforlaget 2018 s. 315.
[13] Fredriksen og Mathisen (2018) s. 315.
[14] Se for eksempel dom av 17. oktober 2013 [C5], *Schwarz,* C-291/12, ECLI:EU:C:2013:670 og dom av 16. april 2015 [C5], *Willems mfl.,* C-446/12 og C-449/12, ECLI:EU:C:2015:238.
[15] Sak fra det britiske datatilsynet, Information Commissioner's Office (ICO), Enforcement Notice to Her Majesty's Revenue and Customs, 9. mai 2019, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf
Sak fra det svenske datatilsynet, Datainspektionen, Tillsyn enlight EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever, sak DI-2019-2221, 20. august 2019, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf
Sak fra det franske datatilsynet, Commission nationale de l'informatique et des libertés (CNIL), Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position, 29. oktober 2019 https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

fra den norske klageinstansen Personvernnemnda fra tiden før forordningen, der sakene fortsatt er av relevans.[16] Saker fra nasjonale tilsynsmyndigheter gir en viss veiledning i hvordan forordningen bør forstås, og vil særlig være aktuelle i analysen av samtykkekravet.

Videre ble European Data Protection Board (heretter «EDPB» eller «Personvernrådet») opprettet som et nytt organ med forordningens ikrafttreden.[17] Personvernrådet erstatter den tidligere Artikkel 29-gruppen, som var det rådgivende organet i tiden før GDPR.[18] Personvernrådet har som formål å sikre en ensartet anvendelse av forordningen.[19] Personvernrådet består av EUs datatilsyn (European Data Protection Supervisor) og representanter for medlemsstatenes nasjonale tilsynsmyndighet.[20] Fra Norge er det en representant fra Datatilsynet, men i lys av at Personvernrådet er et EU-organ har ikke EØS/EFTA-landene stemmerett.[21] Personvernrådets uttalelser og retningslinjer er i utgangspunktet ikke rettslig bindende, men det antas at dens uttalelser vil tillegges vesentlig vekt i fortolkningen av forordningen.[22]

Personvernrådet har videre uttalt at den gir sin tilslutning til en rekke opplistede retningslinjer om GDPR fra Artikkel 29-gruppen før forordningens ikrafttreden.[23] Personvernrådet kom videre i juli 2019 med retningslinjer knyttet til behandling av personopplysninger gjennom videoovervåkning der behandling av biometriske opplysninger i denne forbindelse vurderes.[24] Det er imidlertid ikke utarbeidet nye retningslinjer om biometriske opplysninger generelt. Artikkel 29-gruppens tidligere uttalelser vil dermed være av relevans for oppgaven. Også

Dom fra den franske administrative domstolen i Marseilles, Tribunal Administratif de Marseilles, 27. februar 2020, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf
Veiledende uttalelse fra det danske datatilsynet, Vejledende udtalelse om anvendelsen af fingeraftryk til brug for registrering af ansattes komme-/gå-tider, 29. mai 2019, https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/maj/vejledende-udtalelse-om-anvendelsen-af-fingeraftryk-til-brug-for-registrering-af-ansattes-komme-gaa-tider/
Sak fra det polske datatilsynet Urząd Ochrony Danych Osobowych (UODO), Prezes urzędu ochrony danych osobowych, 4. mars 2020, https://uodo.gov.pl/en/553/1102

[16] Saker fra Personvernnemnda under personverndirektivet som det vises til i oppgaven: PVN-2006-10 (Esso) og PVN-2011-11 (Visma Retail).
[17] Jf. GDPR art. 68 (1).
[18] Working Party on the Protection of Individuals with regard to the Processing of Personal Data (heretter «Artikkel 29-gruppen» eller «A29WP»).
[19] Jf. GDPR art. 70 og art. 71.
[20] Jf. GDPR art. 68 (3).
[21] Se Utkast til EØS-komiteens beslutning med tilpasninger i Prop.56 LS (2017–2018), s. 198.
[22] Prop.56 LS (2017–2018), s. 168.
[23] Se EDPB, https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (lest 29. februar 2020). Personvernrådet uttaler her: «During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines». De aktuelle retningslinjene som er videreført er listet opp.
[24] EDPB, Guidelines 3/2019 on the processing of personal data through video devices, 10. juli 2019.

andre uttalelser fra Artikkel 29-gruppen vil være av betydning der bestemmelser i personverndirektivet 1995[25] er videreført i GDPR og Personvernrådet ikke har kommet med nye uttalelser.

I lys av mangelen på autoritative kilder, vil litteratur på området for biometri, herunder særlig dens tekniske spesifikasjoner, være relevant for oppgaven. De tekniske spesifikasjonene vil forklares rent deskriptivt. Det er også publisert internasjonale artikler med ulike synspunkter på hvordan biometriske opplysninger skal forstås etter forordningen. I mangel av andre autoritative kilder vil det vises til ulike forfatteres ståsted. Artiklene utgjør imidlertid ingen tungtveiende rettskilde.

Det presiseres avslutningsvis at det tas utgangspunkt i oversettelsen av GDPR i personopplysningsloven av hensyn til oppgavens leservennlighet. Ved terminologiske forskjeller mellom oversettelsen og den offisielle versjonen, er det likevel den offisielle versjonen som legges til grunn.

1.3 Avgrensning

Oppgaven vil ta for seg innsamling av biometriske opplysninger etter GDPR. Mange vil kunne relatere behandling av biometriske opplysninger til politi- og kriminalitetsformål, men behandling av slike opplysninger er regulert av direktiv 2016/680.[26] Dette er dermed utenfor denne oppgavens rammer. Ulike nasjonale særregler på området for biometri, herunder blant annet personopplysningsloven § 12 om ytterligere regulering av biometriske opplysninger, vil heller ikke behandles inngående.

Oppgaven tar for seg innsamling som en form for behandling av biometriske opplysninger. Det er også ytterligere problemstillinger innen andre former for behandling av slike opplysninger, særlig problemstillinger knyttet til den registrertes rettigheter som retting og sletting. Dette vil være utenfor denne oppgavens tema. Videre er det også en rekke utfordringer knyttet til lagring av biometriske opplysninger. Hvordan biometriske

[25] Europaparlaments og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (heretter «personverndirektivet»).
[26] Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS (på engelsk forkortet «Law Enforcement Directive» (LED)).

opplysninger skal lagres i databaser er imidlertid ikke regulert av GDPR. Utfordringer knyttet til informasjonssikkerhet vil dermed ikke tas opp i denne oppgaven.

Jeg har videre valgt å analysere samtykke som grunnlag for innsamling av biometriske opplysninger. En rekke offentlige myndigheter og andre private virksomheter som ønsker å samle inn biometriske opplysninger vil ofte måtte bygge på samtykke som et mulig lovlig behandlingsgrunnlag. Avgrensningen åpner også for en mer dyptgående analyse av dette behandlingsgrunnlaget. Det avgrenses mot reglene for samtykke der den registrerte er barn under 16 år etter art. 8.

Enhver form for behandling av biometriske opplysninger vil kunne reise flere menneskerettslige og etiske problemstillinger. Disse utfordringene vil imidlertid være utenfor denne oppgavens rammer å behandle nærmere.

Oppgavens tema er avslutningsvis innenfor et område under stadig utvikling. Det avgrenses derfor mot lovendringer, rettspraksis, avgjørelser fra nasjonale tilsynsmyndigheter, retningslinjer fra Personvernrådet og øvrige relevante kilder offentliggjort etter 20. mai 2020.

1.4 Videre fremstilling

Oppgaven vil i det videre i kap. 2 gi en introduksjon av GDPR, reguleringen av biometriske opplysninger etter forordningen, og sentrale prinsipper som gjør seg gjeldende på området. I kap. 3 vil jeg forklare sentrale begreper knyttet til forordningen og biometri som anses nødvendig for oppgaven. Jeg vil videre i oppgavens hoveddel, kap. 4 og 5, gå dypere inn i definisjonen av biometriske opplysninger, forbudet mot behandling av slike opplysninger etter art. 9 nr. 1 og analyse av kravene til samtykke som behandlingsgrunnlag ved innsamling av biometriske opplysninger. I kap. 6 vil jeg gi noen avsluttende bemerkninger.

2 General Data Protection Regulation (GDPR)

2.1 Forsterket vern med ny forordning

GDPR har introdusert et betydelig større fokus på personopplysningsvern i EU. Det tidligere personverndirektivet var blitt utdatert og det var et stort behov for fornyelse som følge av den teknologiske utviklingen og de medfølgende personvernrettslige utfordringene. Reglene i det tidligere direktivet var også svært ulikt praktisert i medlemsstatene, noe som bidro til en usikker rettstilstand og en for lav grad av beskyttelse i tråd med samfunnsutviklingen.[27] De sentrale prinsippene fra direktivet er likevel i stor grad videreført i den nye forordningen. At reglene om behandling av personopplysninger nå er inntatt i en forordning fremfor et direktiv innebærer i seg selv et forsterket vern, i lys av forordningsformens bindende karakter med direkte virkning for EUs medlemsstater fra det tidspunkt den trer i kraft.[28] Norge er tilsvarende forpliktet gjennom EØS-avtalen art. 7 bokstav a til å inkorporere forordninger i norsk lov.[29]

Formålet med forordningen er at den skal fortsette å fremme fri flyt av personopplysninger på tvers av landegrenser, samtidig som den skal sørge for et høyt vern av disse personopplysningene.[30] Den skal i denne forbindelse bidra til å sikre et likt vern i alle EU- og EØS-landene. Forordningen er videre gjort teknologinøytral for å hindre omgåelser og misbruk av regelverket.[31] Det er dermed et regelverk som søker å balansere det store behovet for behandling av personopplysninger, og det tilsvarende behovet for vern av slike opplysninger for enkeltpersoner.

---

[27] Se fortalepunkt 9.
[28] Det påpekes også i forarbeidene til GDPR at forordningsformen ble ansett som den beste lovgivningsformen for å sikre økt harmonisering av grunnleggende regler, og dermed økt beskyttelse av personopplysninger for den enkelte, samt et effektivt indre marked. Se European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25. januar 2012 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT (lest 2. april 2020) s. 5.
[29] EØS-avtalen art. 7 bokstav a: «Rettsakter som er omhandlet i eller inntatt i vedlegg til denne avtale eller i EØS-komiteens vedtak, skal være bindende for avtalepartene og skal være eller gjøres til del av deres interne rettsorden som følger: en rettsakt som tilsvarer en EØF-forordning skal som sådan gjøres til del av avtalepartenes interne rettsorden».
[30] Jf. GDPR art. 1 nr. 1 og fortalepunkt 6.
[31] Se fortalepunkt 15.

Forordningen får hovedsakelig anvendelse på «helt eller delvis automatisert behandling av personopplysninger» og på «ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register», jf. GDPR art. 2 nr. 1. Behandling av biometriske opplysninger er i all hovedsak automatisert og faller klart innenfor forordningens saklige virkeområde.

2.2 Nytt om biometriske opplysninger og samtykke i GDPR

Etter det tidligere personverndirektivet var biometriske opplysninger ansett som alminnelige personopplysninger etter art. 2 bokstav a så langt vilkårene var oppfylt. Det var dermed ingen særskilt regulering av slike opplysninger og behandling av biometriske opplysninger var lite adressert i et personvernrettslig perspektiv på tidspunktet for direktivets ikrafttreden i 1995. Artikkel 29-gruppen publiserte imidlertid i 2003 et dokument der de viste til de personvernrettslige utfordringene biometrisk teknologi kan medføre.[32] Med utviklingen av denne teknologien ble dokumentet fra 2003 senere fulgt opp i 2012 med ytterligere retningslinjer om hvordan biometriske opplysninger skal behandles etter direktivet.[33] Den raske teknologiske utviklingen på dette området og den økte behandlingen av biometriske opplysninger medførte dermed gradvis et større fokus på behovet for vern ved behandling av denne typen opplysninger.

Den ovennevnte utviklingen er ytterligere adressert i GDPR der det er inntatt en egen definisjon av biometriske opplysninger i art. 4 nr. 14. Biometriske opplysninger med det «formål å identifisere en fysisk person» er videre ansett for å ha et ytterligere behov for vern, og er dermed inntatt som en særlig kategori av personopplysninger i art. 9 nr. 1 (også kalt «sensitive personopplysninger»).

Før forordningens ikrafttreden kunne biometriske opplysninger anses som sensitive etter personverndirektivet art. 8 dersom de avslørte opplysninger om blant annet etnisk opprinnelse, religiøs tro eller helseopplysninger.[34] For eksempel kunne bruk av ansiktsgjenkjenning avsløre opplysninger om en persons etniske opprinnelse.[35] Slike opplysninger var dermed inntatt i forbudet i art. 8 nr. 1. Biometriske opplysninger med

[32] Artikkel 29-gruppen, Working document on biometrics, 2003, WP80.
[33] Artikkel 29-gruppen, Opinion 3/2012 on developments in biometric technologies, WP193.
[34] Artikkel 29-gruppen, 2003 s. 10.
[35] Artikkel 29-gruppen, 2003 s. 10.

identifikasjonsformål var imidlertid ikke ansett som sensitive.[36] Dette er dermed en viktig endring med forordningen.

Videre var kravene til samtykke etter direktivet regulert etter art. 2 bokstav h for alminnelige personopplysninger og etter art. 8 bokstav a for særlige kategorier av personopplysninger. Forordningens krav til samtykke som behandlingsgrunnlag er mer detaljerte, og stiller strengere krav til den behandlingsansvarlige. De alminnelige kravene til samtykke fremgår nå av GDPR art. 6 nr. 1 bokstav a, med tilhørende definisjon i art. 4 nr. 11, og for særlige kategorier av personopplysninger av GDPR art. 9 nr. 2 bokstav a. Det er i tillegg oppstilt en rekke nye krav i GDPR art. 7 og art. 8. Det antas dermed at mange samtykker gitt før forordningens ikrafttreden, ikke lenger er gyldige.[37] De strenge samtykkekravene kan i mange tilfeller gjøre det vanskelig å bygge på dette behandlingsgrunnlaget ved innsamling av biometriske opplysninger.

2.3 Sentrale prinsipper

Prinsippene som fremgår av GDPR art. 5 er i stor grad videreført fra det tidligere personverndirektivet art. 6. Disse prinsippene er helt sentrale for personvernlovgivningen, og setter den overordnede rammen for behandling av personopplysninger etter forordningen og annet personvernrettslig regelverk.[38] De ulike prinsippene er lovlighet, rettferdighet, åpenhet, formålsbegrensning, dataminimering, riktighet, lagringsbegrensning, og integritet og konfidensialitet. Jeg vil i det videre gå nærmere inn i prinsippet om lovlighet, formålsbegrensning og dataminimering. Dette fordi de er av særlig betydning for innsamling av biometriske opplysninger etter forordningen.

2.3.1 Prinsippet om lovlighet

Det fremgår av GDPR art. 5 nr. 1 bokstav a at personopplysninger skal behandles på en «lovlig (...) måte med hensyn til den registrerte». I prinsippet om lovlighet ligger at den

[36] Det ble under det tidligere direktivet diskutert når biometriske opplysninger var å anse som sensitive, og om de burde anses som sensitive i sin natur fremfor hva de kunne avsløre av andre sensitive opplysninger. Se nærmere om denne debatten i bl.a. Catherine Jasserand, «Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data», *European Data Protection Law Review,* vol. 2 (2016) nr. 3 s. 297–311 på s. 308-309 og Liu (2010) s. 145-150.
[37] Åste Marie Bergseng Skullerud mfl., *Personopplysningsloven og personvernforordningen: Kommentarutgave*, Universitetsforlaget, 2019 s. 489.
[38] Skullerud (2019) s. 172.

behandlingsansvarlige må ha et rettslig grunnlag for behandling av personopplysninger. Dette innebærer i forordningen et krav til behandlingsgrunnlag. Lovlig behandling forutsetter dermed et gyldig behandlingsgrunnlag i art. 6 nr. 1 og et eventuelt gyldig unntak i art. 9 nr. 2 for særlige kategorier av personopplysninger. Samtykke er et slikt lovlig behandlingsgrunnlag. Det ligger videre i prinsippet om lovlighet at behandlingsgrunnlaget, som et samtykke, må foreligge før selve innsamlingen av personopplysninger.[39]

Det fremgår videre av art. 9 nr. 4 at medlemsstatene kan «innføre ytterligere vilkår, herunder begrensninger, med hensyn til behandling av (...) biometriske opplysninger». Det er dermed opp til medlemsstatene om de ønsker en strengere regulering for behandling av slike personopplysninger. Illustrerende er Norge som stiller ytterligere krav til behandling av biometriske opplysninger til identifikasjonsformål i personopplysningsloven § 12.[40]

2.3.2 Prinsippet om formålsbegrensning

Det fremgår av art. 5 nr. 1 bokstav b at personopplysninger skal samles inn for «spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene». Dette prinsippet setter en svært viktig begrensning i hvilke personopplysninger som kan samles inn. Innsamling av biometriske opplysninger vil ofte være til ulike identifiserings- eller verifiseringsformål eller med det formål å kategorisere personer.[41] Det må nærmere spesifiseres hva formålet med innsamlingen er for å sikre at den behandlingsansvarlige ikke behandler opplysningene utover det som er angitt. Dette skal også sikre at opplysningene slettes når de ikke lenger er nødvendige for å oppnå formålet etter art. 17 nr. 2 bokstav a. For samtykke som grunnlag for innsamling av biometriske opplysninger etter art. 6 nr. 1 bokstav a og art. 9 nr. 2 bokstav a er det et krav om at samtykket gjelder for et eller flere nærmere spesifiserte formål. Prinsippet om formålsbegrensning er derfor viktig for å sikre den enkeltes kontroll med hva personopplysningene benyttes til.[42]

[39] EDPB, 05/20 s. 25, avsnitt 121.
[40] Personopplysningsloven § 12 (1): «Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.»
[41] Artikkel 29-gruppen, Opinion 02/2012 on facial recognition in online and mobile services, WP192, s. 4.
[42] Prop. 115 L (2017-2018) Endringer i personopplysningsloven (bekjempelse av arbeidslivskriminalitet) s. 9.

2.3.3 Prinsippet om dataminimering

Dataminimeringsprinsippet fremgår av art. 5 nr. 1 bokstav c der det heter at personopplysningene som samles inn skal være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for». Dette innebærer at man skal behandle så lite personopplysninger som mulig for å oppnå formålet med behandlingen.[43] I at opplysningene skal være «adekvate» og «relevante» ligger at de skal ha nærhet til formålet og være egnet til å oppnå det aktuelle formålet.[44]

Videre skal ikke personopplysningene «lagres lenger enn det som er strengt nødvendig» og personopplysninger bør kun behandles «dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte», jf. fortalepunkt 39. Dataminimeringsprinsippet vil derfor kunne sette ytterligere begrensninger på i hvilken grad biometriske opplysninger kan samles inn eller behandles på annen måte. Jeg vil i punkt 5.4 vurdere hvordan dataminimeringsprinsippet setter begrensninger på adgangen til å samtykke til behandling av biometriske opplysninger.

[43] EDPB (Personvernrådet), Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, s. 5.
[44] Skullerud mfl. (2019) s. 174.

3 Terminologi

3.1 Personopplysninger og særlige kategorier av personopplysninger

For at de aktuelle opplysningene skal falle inn under forordningens saklige virkeområde må det være snakk om behandling av personopplysninger.[45] En «personopplysning» er definert i art. 4 nr. 1 som

> «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet».

Definisjonen er langt på vei en videreføring av definisjonen av personopplysninger i personverndirektivet art. 2 bokstav a. Definisjonen er svært vid da den omfatter «enhver opplysning» som kan knyttes til en «identifisert eller identifiserbar fysisk person», jf. art. 4 nr. 1. EU-domstolen uttalte i Peter Nowak-dommen at definisjonen er ment å omfatte alle opplysninger som kan knyttes til en person, uavhengig av om de anses som sensitive eller private.[46] Det er videre tilstrekkelig for at en person skal anses «identifisert» at vedkommende kan skilles ut fra andre, og at vedkommende er «identifiserbar» der slik utskillelse er mulig.[47] Denne koblingen kan både være direkte og indirekte. Biometriske opplysninger er først og fremst personopplysninger, og må dermed også være omfattet av art. 4 nr. 1. Jeg vil gå nærmere inn på i hvilken grad biometriske opplysninger er personopplysninger i kap. 4.3.

For at man skal kunne behandle personopplysninger, må et av de alminnelige behandlingsgrunnlagene i art. 6 nr. 1 være oppfylt. Et mulig behandlingsgrunnlag følger av

[45] Jf. GDPR art. 2 nr. 1.
[46] Dom av 20. desember 2017 [C5], C-434/16, *Peter Nowak,* ECLI:EU:C:2017:994 avsnitt 34.
[47] Artikkel 29-gruppen, Opinion 4/2007 on the concept of personal data, WP136 s. 12. Det er ikke kommet nye retningslinjer om hvordan personopplysningsbegrepet skal forstås etter GDPR. Det legges dermed til grunn at det forstås på samme måte som under personverndirektivet.

art. 6 nr. 1 bokstav a der behandlingen er lovlig dersom den registrerte har «samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål».

Videre reguleres særlige kategorier av personopplysninger av art. 9. Det fremgår av art. 9 nr. 1 at

> «behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, er forbudt».

Særlige kategorier av personopplysninger er dermed i utgangspunktet forbudt å behandle. Opplysningene er underlagt et særskilt vern på grunn av deres sensitive natur og den risiko de utgjør mot den enkeltes rettigheter og friheter.[48] Det er videre antatt at det er snakk om opplysninger som den enkelte har et ønske om å verne om i større grad enn andre opplysninger.[49] Hva som er å regne som biometriske opplysninger og i hvilke tilfeller disse er å regne som en særlig kategori av personopplysninger i art. 9 nr. 1, vil vurderes nærmere i kap. 4.

Det følger videre en rekke unntak fra forbudet mot behandling i art. 9 nr. 2. Et av disse unntakene fremgår av art. 9 nr. 2 bokstav a der slike opplysninger kan behandles dersom den registrerte har gitt

> «uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.»

Samtykke som behandlingsgrunnlag for biometriske opplysninger etter art. 6 og art. 9 vil vurderes i kap. 5.

[48] Jf. fortalepunkt 51.
[49] Schartum og Bygrave, *Personvern i Informasjonssamfunnet*, Fagbokforlaget 2016, s. 144.

3.2 Behandlingsansvarlig, databehandler og den registrerte

De ulike rollene som innehas ved behandling av personopplysninger er legaldefinert i art. 4. Viktige begreper som «behandlingsansvarlig», «databehandler» og «den registrerte» vil bli omtalt i oppgaven. Den «behandlingsansvarlige» er i art. 4 nr. 7 definert som

> «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes».

Det fremgår videre av art. 24 nr. 1 at den behandlingsansvarlige må gjennomføre «egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning». Det er dermed den behandlingsansvarlige som har det overordnede ansvaret for å sikre at det foreligger et gyldig behandlingsgrunnlag for behandling av personopplysningene og at personvernforordningen etterleves. Den behandlingsansvarlige kan være ulike private selskaper eller offentlige virksomheter. En arbeidsgiver vil for eksempel ofte være behandlingsansvarlig ved behandling av personopplysninger om ansatte.[50]

Videre er «databehandler» definert i art. 4 nr. 8 som

> «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige».

Databehandleren må dermed være et separat rettssubjekt og må behandle personopplysninger på vegne av den behandlingsansvarlige.[51] Dette vil ofte være IT-selskaper.[52]

Avslutningsvis, er «den registrerte» definert i art. 4 nr. 1 som en «identifisert eller identifiserbar fysisk person». Dette er dermed en person som får sine personopplysninger behandlet. Der for eksempel ansiktsgjenkjenningsteknologi blir brukt som adgangskontroll til en virksomhets kontorer vil den registrerte være den ansatte som får ansiktet avlest,

[50] Jon Wessel-Aas, *Personvern - publisering og behandling av personopplysninger*, Gyldendal 2018 s. 100.
[51] Artikkel 29-gruppen, Opinion 1/2010 on the concepts of "controller" and "processor", WP169, s. 25. Definisjonen av "behandlingsansvarlig" og "databehandler» er videreført fra personverndirektivet, og veiledningen fra før GDPR har dermed fortsatt betydning for forståelsen av innholdet i begrepene.
[52] Wessel-Aas (2018) s. 100.

virksomheten vil være behandlingsansvarlig og IT-selskapet vil være databehandler. Nærmere vurdering av begrepene anses ikke nødvendig for oppgaven.

3.3 Biometri, biometriske kjennetegn og biometriske systemer

Biometriske systemer for identifikasjon av individer er svært tekniske og det er derfor nødvendig med en avklaring av de viktigste begrepene som er sentrale for oppgaven. Det er videre sentralt å kjenne til den biometriske prosessen for å forstå reguleringen av behandlingen av denne typen opplysninger etter GDPR. Denne avhandlingen er imidlertid juridisk, og de tekniske begrepene vil derfor kun forklares så langt det anses nødvendig for oppgaven og i lys av oppgavens størrelse. I forklaringen av de tekniske begrepene har jeg i stor grad valgt å bygge på doktorgradsavhandlingen til Nancy Yue Liu og Artikkel 29-gruppens tidligere nevnte uttalelser fra 2003 og 2012.

Biometri er en teknikk som måler biometriske kjennetegn for å identifisere eller verifisere en person.[53] Det må skilles mellom biometriske kjennetegn og biometriske systemer. *Biometriske kjennetegn* er unike og permanente kroppslige kjennetegn ved en fysisk person som kan benyttes til identifikasjon.[54] Dette kan være fysiske, fysiologiske og atferdsmessige egenskaper ved en person som et fingeravtrykksmønster, ansiktsform, irismønster, stemme, håndskrift og ganglag.[55] Ettersom kjennetegnene i stor grad knyttes uløselig til en fysisk person, er de ansett som godt egnet for identifikasjonsformål. For at de biometriske kjennetegnene skal kunne brukes til identifikasjon må de gjennom et biometrisk system.

Biometriske systemer kan defineres som anvendelse av biometrisk teknologi i en automatisert prosess som tillater identifisering og verifisering av en person.[56] Det er nå også adgang til å kategorisere mennesker gjennom anvendelse av biometriske systemer og det er derfor foreslått en utvidet definisjon der et biometrisk system er et system som trekker ut og behandler biometriske opplysninger.[57]

[53] Liu (2010), s. 31.
[54] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/
[55] Artikkel 29-gruppen, 3/2012, s. 4.
[56] Artikkel 29-gruppen, 2003 s. 4 og videre fulgt opp i 3/2012 s. 5.
[57] Artikkel 29-gruppen, 3/2012 s. 5.

Det biometriske system er beskrevet som en tredelt prosess som inkluderer innrullering, oppbevaring og sammenligning.[58] I den første innrulleringsfasen blir biometriske kjennetegn, som et fingeravtrykk eller et ansikt, registrert i et elektronisk system som en *biometrisk prøve* (fra engelsk: «sample»).[59] Dette kan være gjennom en fingeravtrykkssensor, avlesning av et ansikt, irisavlesning eller et lydopptak. Kjennetegnet lagres dermed som et bilde eller et opptak. Deretter blir den sentrale informasjonen fra den biometriske prøven trukket ut og omdannet til en matematisk kodet mal ved hjelp av algoritmer (fra engelsk: «feature extraction»).[60] Den digitale representasjonen av den biometriske prøven, *den biometriske malen* (fra engelsk: «template»), blir så oppbevart i en database for senere sammenligning.[61] Den biometriske malen må være så nøyaktig kodet at den kun knyttes til den aktuelle biometriske prøven. Samtidig må den ikke inneholde en overdreven mengde informasjon, ettersom det øker risikoen for at den biometriske prøven kan regenereres.[62] Den biometriske prøven blir derfor ofte slettet fra databasen, slik at det kun er malen som lagres og blir brukt til senere sammenligning.[63] Formålet med den biometriske malen er å beskytte personopplysningene.[64]

I den avsluttende sammenligningsfasen blir en biometrisk mal som er innsamlet fra en ny biometrisk prøve, for eksempel fra et fingeravtrykk, sammenlignet med malen som er oppbevart i en database eller lignende.[65] Resultatet av sammenligningsprosessen vil avhenge av hvor stor sannsynligheten er for at de to malene stammer fra samme person, og vil i utgangspunktet generere et ja/nei-svar ut fra en satt grense.[66] Denne sannsynligheten vil vanligvis vurderes ut fra variablene om falsk positiv (False Acceptance Rate (FAR)) og falsk negativ (False Rejection Rate (FRR)).[67] Disse variablene vil angi hvor stor sannsynligheten er for at systemet feilaktig gjenkjenner en person som ikke er registrert, og hvor stor sannsynligheten er for at en registrert person vil bli avvist av systemet.[68] Målet er å finne et

[58] Artikkel 29-gruppen, 3/2012 s. 5.
[59] Yue Liu (2010) s. 36.
[60] Yue Liu (2010) s. 36.
[61] Artikkel 29-gruppen, 2003 s. 4.
[62] Se Artikkel 29-gruppen, 3/2012 s. 4. Malen må heller ikke inneholde en overdreven mengde informasjon av hensyn til dataminimeringsprinsippet og risikoen for videre behandling uten den registrertes kunnskap, se EDPB, 3/2019, s. 18 avsnitt 86.
[63] Artikkel 29-gruppen, 2003 s. 4.
[64] Artikkel 29-gruppen 3/2012 s. 20.
[65] Artikkel 29-gruppen, 2003 s. 5.
[66] Yue Liu (2010) s. 37.
[67] Artikkel 29-gruppen, 2003 s. 6.
[68] Artikkel 29-gruppen, 2003 s. 6.

nivå der FAR og FRR er forsvarlig justert ut fra hvor stor grad av sikkerhet som er påkrevd i det aktuelle systemet.[69] For eksempel vil det være større behov for en lavere FAR (og dermed en høyere FRR) ved adgangskontroll til taushetsbelagte dokumenter for å hindre at noen feilaktig får tilgang til systemet, og tilsvarende en høyere FAR (og dermed lavere FRR) ved tilgang til en kino for å unngå at noen med billett avvises av systemet. Sammenligningsfasen er dermed sannsynlighetsbasert med en viss risiko for feilaktige resultater.

[69] Yue Liu (2010) s. 39.

4 Innsamling av biometriske opplysninger

4.1 Hva er biometriske opplysninger? En analyse av GDPR art. 4 nr. 14

4.1.1 Innledende om definisjonen

Det fremgår av art. 4 nr. 14 at «biometriske opplysninger»[70] er

> «personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger».

Definisjonen er langt på vei en videreføring av Artikkel 29-gruppens definisjon som før forordningens ikrafttreden var ansett som gjeldende rett. Artikkel 29-gruppen definerte biometriske opplysninger som «biologiske egenskaper, atferdsmessige aspekter, fysiologiske kjennetegn, levende trekk eller gjentakende handlinger hvor disse kjennetegnene og/eller handlingene både er unike for individet og målbare, selv om mønsteret som er brukt i praksis for teknisk måling innebærer en viss grad av sannsynlighet for at mønsteret kun tilhører det aktuelle individet» (min oversettelse). [71]

Det nye med definisjonen i forordningen er dermed at de biometriske kjennetegnene må gjennom en «særskilt teknisk behandling» der formålet må være «å muliggjør[e] eller bekreft[e] en entydig identifikasjon», jf. art. 4. nr. 14. Dette kan sies å være en presisering av den tidligere definisjonen. Dette tilsier også at Artikkel 29-gruppens uttalelser fra 2003 og 2012 fortsatt kan tillegges vekt ved fortolkningen av definisjonen.

For at biometriske opplysninger skal være underlagt forbudet mot behandling av slike opplysninger i art. 9 nr. 1, må opplysningene først og fremst være omfattet av definisjonen i art. 4 nr. 14. Hvorvidt de aktuelle personopplysningene er å regne som særlige kategorier av

[70] Betegnelsen «biometriske opplysninger» er oversatt fra det engelske «biometric data». Mange vil også på norsk omtale dette som «biometrisk data». Jeg vil i oppgaven holde meg til den norske oversettelsen i personopplysningsloven 2018.
[71] Artikkel 29-gruppen, 3/2012 s. 4.

personopplysninger, har betydning for hvorvidt de skal være underlagt strengere krav ved behandling. Det stilles blant annet strengere krav til viderebehandling til andre formål enn det opplysningene først ble innsamlet for etter art. 6 nr. 4 og det stilles strengere krav til hvorvidt den registrerte kan være gjenstand for avgjørelser utelukkende basert på automatisk behandling etter art. 22.

Det må også utarbeides en vurdering av personvernkonsekvenser, Data Protection Impact Assessment (heretter «DPIA»). Det skal «særlig være nødvendig» med en DPIA ved behandling av særlige kategorier av personopplysninger, jf. art. 35 nr. 3 bokstav b. En DPIA er imidlertid også påkrevd for øvrige personopplysninger der behandlingen innebærer «bruk av ny teknologi» og vil medføre «høy risiko» for den enkeltes rettigheter og friheter, jf. art. 35 nr. 1. Behandling av biometriske opplysninger vil derfor ofte kreve en DPIA uavhengig av om opplysningene anses som en særlig kategori av personopplysninger etter art. 9.

Jeg vil i det videre gå nærmere inn i definisjonens vilkår og hvordan vilkårene skal forstås etter gjeldende rett, før jeg vurderer hvilke opplysninger som faller inn under forbudet mot behandling i art. 9.

4.1.2 Vilkår om at opplysningene «stammer fra en særskilt teknisk behandling»

Som nevnt i kapittelet over må personopplysningene «stamm[e] fra en særskilt teknisk behandling» for å være omfattet av definisjonen i art. 4 nr. 14. En naturlig forståelse av «særskilt teknisk behandling» er at personopplysningene må gjennom en spesiell teknologisk prosess. Dette synes å sikte til det biometriske systemet der en biometrisk prøve blir omdannet til en biometrisk mal.[72] Ettersom den biometriske malen klart «stammer fra en særskilt teknisk behandling» etter å ha gjennomgått en automatisert omdannelse til en matematisk kodet mal, er det klart at denne er omfattet av definisjonen.

Det vises videre til «ansiktsbilder» og «fingeravtrykksopplysninger» som eksempler på hva som faller innunder definisjonen i art. 4 nr. 14. De biometriske prøvene, som danner

[72] Els J. Kindt, «Having yes, using no? About the new legal regime for biometric data», *Computer Law and Science Review,* vol. 34, issue 3 (2017) s. 523–538 på s. 531.

grunnlaget for dannelsen av den biometriske malen, må dermed også anses omfattet av definisjonen. Dette vil for eksempel være et bilde av et ansikt eller et fingeravtrykk.

Det kan imidlertid stilles spørsmål ved på hvilket tidspunkt de biometriske prøvene faller inn under definisjonens anvendelsesområde.[73] Det er sentralt å avgjøre om de biometriske prøvene omfattes av definisjonen allerede på det tidspunktet de samles inn, eller om det avhenger av hvordan de behandles. Dette vil få betydning for når de er underlagt reglene for særlige kategorier av personopplysninger i art. 9 nr. 1.

Det fremgår av forordningens fortalepunkt 51 at fotografier ikke skal anses som biometriske opplysninger, med mindre de «behandles ved hjelp av et særskilt teknisk middel som gjør det mulig entydig å identifisere eller autentisere en fysisk person». Dette er fulgt opp i Personvernrådets retningslinjer til også å inkludere bilder fra overvåkningskameraer.[74] Det vises dermed til at ansiktsbilder ikke anses som biometriske opplysninger før de behandles i det biometriske system.

Hensikten med den ovennevnte avklaringen i fortalepunkt 51 var trolig å unnta innsamling av fotografier ved skoler, av arbeidsgivere eller i andre sammenhenger der hensikten ikke er å behandle disse i det biometriske system for identifikasjon. Det ville videre vanskeliggjort bruk av kameraovervåkning om alle bilder av personer automatisk skulle vært ansett omfattet av definisjonen. Fotografier som viser en «identifisert» eller «identifiserbar» person, men der personen kun identifiseres eller verifiseres av *øyet som ser*, vil dermed anses som alminnelige personopplysninger etter art. 4 nr. 1.

Den ovennevnte forståelsen innebærer at både offentlige og private virksomheters innsamling av fotografier og oppbevaring av disse, ikke vil være underlagt forbudet i art. 9 nr. 1. Dette kan gjøre at slike bilder lettere utsettes for misbruk ved at de oppbevares i databaser for senere å bli behandlet i det biometriske system uten den registrertes kunnskap.[75] Når bildene først er samlet inn, kan det også medføre misbruk av en tredjepart.[76] Dette kan være uheldige konsekvenser av at fotografiene kun er biometriske opplysninger ut fra hvordan de behandles.

[73] Kindt (2017) s. 532.
[74] EDPB, 3/2019, s. 15 avsnitt 73.
[75] Kindt (2017) s. 534.
[76] Kindt (2017) s. 533.

Hvorvidt fortalepunkt 51 også skal gjelde for andre biometriske prøver, som bilde av et fingeravtrykk, er usikkert. Personvernrådets uttalelse om at databaser med biometriske prøver («raw data») kan utgjøre en større risiko enn oppbevaring av malen, kan tilsi at de biometriske prøvene burde vært ansett omfattet av definisjonen allerede fra det tidspunkt de samles inn og oppbevares.[77] At bildene på dette tidspunkt ikke er behandlet i det biometriske system for identifikasjon, gjør ikke nødvendigvis behovet for beskyttelse mot fremtidig bruk mindre.

Innsamling av bilder av fingeravtrykk eller bilder av andre kjennetegn vil videre ofte være med det formål å identifisere eller verifisere en person i det biometriske system. Fotografier vil sammenligningsvis ofte også samles inn til andre formål. Dette kan tilsi at det var intensjonen å skille mellom innsamling av fotografier og innsamling av øvrige biometriske prøver som bilde av et fingeravtrykk.

På den andre siden kan sammenhengen i regelverket tilsi at også bilder av fingeravtrykk eller øvrige kjennetegn først er å regne som biometriske opplysninger når de behandles i det biometriske system. Dette kan også sies å i større grad være i tråd med ordlyden som henviser til at opplysningene må være et resultat av behandling i det biometriske system.

Konklusjonen er etter dette at både fotografier og øvrige biometriske prøver er omfattet av definisjonen først når de behandles i det biometriske system for identifikasjon. En slik forståelse av forordningen vil imidlertid kunne åpne for innsamling av store mengder bilder av biometriske kjennetegn til oppbevaring i databaser, og vil kunne øke risikoen for misbruk og viderebehandling utenfor den registrertes kontroll. Det presiseres imidlertid at forordningen ikke er helt klar på dette punkt, og at det er sentralt med en avklaring fra Personvernrådet eller EU-domstolen.

4.1.3 Vilkår om "fysiske, fysiologiske eller atferdsmessige egenskaper"

Etter art. 4 nr. 14 må personopplysningene som stammer fra en særskilt teknisk behandling være «knyttet til» ulike «fysiske, fysiologiske eller atferdsmessige egenskaper» ved en fysisk person. Dette er ulike biometriske kjennetegn, herunder fysiske kjennetegn som ansiktsform og fingeravtrykk, fysiologiske kjennetegn som blodårer og venemønster (fra engelsk: «vein

[77] EDPB, 3/2019 s. 18, avsnitt 89.

pattern»), og atferdsmessige kjennetegn som ganglag og stemme.[78] Definisjonen er svært vid og omfatter de fleste målbare kjennetegn ved en person.

De vanligste biometriske kjennetegnene som blir brukt til identifikasjon i dag er trolig fingeravtrykk, ansiktsform, håndavtrykk og netthinne- og irismønster.[79] Stemmegjenkjenning er også anvendt i større grad enn før.[80] Ansiktsgjenkjenningsteknologien har også gjort det mulig å måle andre fysiske og psykologiske kjennetegn ved en person, for eksempel etnisk opprinnelse og ansiktsuttrykk som avslører en persons følelser og trivsel.[81] Det at slike opplysninger kan avsløres fra et bilde eller fra overvåkningskameraer uten en persons kunnskap, viser de personvernrettslige utfordringene man står overfor ved bruk av denne typen teknologi.[82]

4.1.4 Vilkår om "muliggjør eller bekrefter» en entydig identifikasjon

Det er et vilkår etter art. 4 nr. 14 at den særskilte tekniske behandlingen «muliggjør eller bekrefter» en entydig identifikasjon. Ordlyden er en klar henvisning til at formålene med behandlingen må være identifisering eller verifisering[83] av en fysisk person.[84] Hvorvidt de aktuelle opplysningene faller innunder definisjonen i art. 4 nr. 14 vil dermed avhenge av hvilket formål opplysningene skal tjene. Biometriske opplysninger til rene kategoriseringsformål faller utenfor definisjonens anvendelsesområde.

Biometrisk identifisering innebærer at man avgjør hvem en konkret person er ved å sammenligne personens innhentede biometriske prøve eller mal med allerede lagrede maler av en rekke individer i en sentralisert database.[85] Dette er omtalt som et en-til-mange-søk (1:n), der en match avhenger av om vedkommende fra før er registrert i databasen.[86] Biometrisk identifisering blir mye brukt til politiformål og ved grenseoverganger, men kan også utgjøre

[78] Liu (2010) s. 55.
[79] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/
[80] Se for eksempel sak fra det britiske datatilsynet: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf Saken vil omtales ytterligere under kapittel 5 om samtykke.
[81] Artikkel 29-gruppen, 3/2012, s. 21.
[82] Artikkel 29-gruppen, 3/2012 s. 21.
[83] Ordet «autentisering» er også ofte brukt om verifiseringsformålet. Det er imidlertid også brukt som et synonym på identifisering. Jeg bruker derfor «verifisering» for å unngå sammenblanding av begreper. Se videre Jasserand (2016) s. 304–305 om begrepsbruken.
[84] Begrepsbruken er kritisert av Jasserand, som mener begrepene i forordningen bør samsvare med begrepsbruken i det biometriske fagmiljøet, se Jasserand (2016) s. 311.
[85] Liu (2010) s. 35.
[86] Liu (2010) s. 35.

en del av et verifiseringssystem der den registrerte i forbindelse med adgangskontroll til et kontorbygg blir identifisert før vedkommende blir verifisert.

Til forskjell fra biometrisk identifisering, vil man ved biometrisk verifisering forsøke å bekrefte en persons identitet og dermed hvorvidt personen er den vedkommende utgir seg for å være.[87] Dette innebærer et en-til-en-søk (1:1), der den innhentede biometriske prøven eller malen blir sammenlignet med en allerede lagret mal fra samme person.[88] Det er ved en slik sammenligning tilstrekkelig at malen er lagret lokalt i en enhet, og krever ikke lagring i en sentralisert database som ved identifisering. Dette er klart mer personvernvennlig enn identifisering, og er det mest brukte formålet med biometrisk identifikasjon etter GDPR. Eksempler på bruk av biometrisk verifisering er ved bruk av fingeravtrykk for innlogging med BankID, bruk av fingeravtrykk eller ansiktsgjenkjenning for innlogging på smarttelefon, og bruk av ansiktsgjenkjenning for adgangskontroll til en virksomhets kontorer.

Skillet mellom biometriske identifisering og biometrisk verifisering vil kunne få betydning for når behandlingen av biometriske opplysninger er i tråd med forordningen. Skillet er spesielt aktuelt for hvorvidt både identifisering og verifisering er omfattet av forbudet mot behandling i art. 9 nr. 1 (se kap. 4.2.1) og i hvilken grad den biometriske malen er å regne som en personopplysning (se kap. 4.3).

4.1.5 Vilkår om "entydig identifikasjon"

For at de aktuelle opplysningene skal anses som biometriske opplysninger, må de muliggjøre eller bekrefte en «entydig identifikasjon» etter art. 4 nr. 14. Bestemmelsen sett i sammenheng tilsier klart at både identifiserings- og verifiseringsformål er omfattet. Begrepet «identifikasjon» må dermed ses i sammenheng med hvorvidt identifiseringen eller verifiseringen kan knyttes til en «identifisert eller identifiserbar fysisk person» etter art. 4 nr. 1. Det vil for eksempel være tilfeller av verifisering av en persons adgang til et område der man ikke kan spore opplysningene tilbake til en bestemt person. Opplysningene om personen vil dermed være anonyme, og vil ikke være omfattet av GDPR.

Illustrerende er saken om Visma Retail fra Personvernnemnda under det tidligere personverndirektivet og Lov 14. april 2000 nr. 31 om behandling av personopplysninger

[87] Liu (2010) s. 34.
[88] Liu (2010) s. 34.

(personopplysningsloven).[89] Saken gjaldt hvorvidt dagligvarebutikken Bunnpris kunne benytte kundenes fingeravtrykk for alderskontroll ved kjøp av alkoholholdige varer i selvbetjente kasser. Det ble påpekt at systemet var et rent verifiseringssystem der fingeravtrykket kun skulle knyttes opp mot en tidligere lagret mal på vedkommendes fødselsdato. Som ID ble det kun brukt et løpenummer for å finne malen i databasen. Personvernnemnda kom til at slike rene verifiseringssystemer ikke skulle anses som identifikasjon i lovens forstand, og at det ikke var snakk om behandling av personopplysninger. Det ble særlig lagt vekt på at den innsamlede malen ikke innebar behandling av personopplysninger. Det kan imidlertid diskuteres hvorvidt slik biometrisk verifisering vil kunne gjøres anonymt etter forordningen.[90] Jeg kommer tilbake til dette i kap. 4.3.

Identifikasjonen skal videre etter bestemmelsens ordlyd være «entydig». En naturlig forståelse av «entydig» er at identifikasjonen må være klar eller sikker. Ettersom «identifikasjon» må forstås i lys av personopplysningsdefinisjonen i art. 4 nr. 1, tilsier det at «entydig» viser til terskelen for identifikasjon.[91] At identifikasjonen må være tilnærmet klar eller sikker kan dermed tilsi at det må være snakk om opplysninger om en «identifisert» person etter art. 4 nr.1. Dette innebærer som tidligere nevnt i kap. 3.1 at de biometriske opplysningene må kunne skille vedkommende fra andre, og vil både gjelde ved identifisering og verifisering av en person. Denne forståelsen innebærer at biometriske opplysninger om en «identifiserbar» person faller utenfor definisjonen i art. 4 nr. 14, og anses som alminnelige personopplysninger etter art. 4 nr. 1.

[89] PVN-2011-11 (Visma Retail).
[90] Avgjørelsen er kritisert av Nancy Yue Liu i «Biometri, fingeravtrykk og personvern», *Lov&Data,* 110 (2012) s. 9 (LoD-2012-110-9). Liu argumenterer for at det ved en match mellom personens fingeravtrykk og databasen, vil være opplysninger om en «identifisert eller identifiserbar» person og at malen i dette tilfellet ikke er en anonym opplysning.
[91] Se Jasserand (2016) s. 305-306 med videre henvisninger.

4.2 Forbud mot behandling av biometriske opplysninger etter art. 9 nr. 1

4.2.1 Formålet må være å "entydig identifisere" en person

Det sentrale vilkåret for at biometriske opplysninger skal være forbudt å samle inn eller behandle på annen måte etter art. 9 nr. 1, er at formålet må være å «entydig identifisere» en fysisk person. Der formålet med innsamlingen er å kategorisere personer, kommer ikke art. 9 nr. 1 til anvendelse.[92] Henvisningen til identifiserings- og verifiseringsformål, som det vises til i definisjonen i art. 4 nr. 14, er utelatt fra art. 9 nr. 1. Det kan dermed stilles spørsmål ved om det kun er identifiseringsformålet som er omfattet av forbudet.

En naturlig forståelse av «identifisere» er at det viser til forhold der man ønsker å finne ut hvem en person er i et en-til-mange-søk. En isolert tolkning av ordlyden tilsier dermed at det kun er rene identifiseringsformål som er omfattet av forbudet. Dette vil kunne innebære at verifiseringssystemer, som for eksempel Iphones bruk av ansiktsgjenkjenning for å åpne telefonen eller annen verifisering av identitet for adgangskontroll, vil kunne falle utenfor forbudet i art. 9 nr. 1. Det vil imidlertid fortsatt være biometriske opplysninger etter art. 4 nr. 14, men opplysningene er da underlagt reglene for alminnelige personopplysninger.

På den andre siden kan bestemmelsen forstås i sammenheng med begrepet «entydig identifikasjon» i art. 4 nr. 14 slik at det avgjørende er om identifiseringen eller verifiseringen er knyttet til en «identifisert» person i art. 4 nr. 1. Dette medfører at innsamling av biometriske opplysninger til både identifiserings- og verifiseringsformål kan anses som særlige kategorier av personopplysninger etter art. 9 nr. 1.[93]

Det fremgår av fortalepunkt 51 at fotografier ikke er omfattet av definisjonen, og dermed ikke er å anse som en særlig kategori av personopplysninger, med mindre de behandles med et særskilt teknisk middel «som gjør det mulig entydig å identifisere eller autentisere en fysisk person». Her brukes begrepet «entydig å identifisere» som en motsetning til verifiseringsformål (autentisering). Sammenligningsvis brukes «entydig identifikasjon» i

[92] EDPB, 03/2019 s. 16, avsnitt 79.
[93] I denne retning, se Jasserand (2016) s. som mener at art. 4 nr. 14 og art. 9 nr. 1 må forstås i sammenheng. Hun presiserer imidlertid at det er knyttet usikkerhet til dette. Motsatt, se Kindt (2017) s. 535 og Kuner, Bygrave og Docksey (2020) s. 214 som legger til grunn at art. 9 nr. 1 trolig kun omfatter biometrisk identifisering.

definisjonen i art. 4 nr. 14. Dette tilsier at begrepet i art. 9 nr. 1 bør forstås på samme måte som i fortalepunkt 51, slik at forbudet kun omfatter identifiseringsformål.

Den norske oversettelsen avviker imidlertid på dette punkt fra den engelske offisielle versjonen av forordningen. I den offisielle versjonen brukes begrepet «unique identification» som en motsetning til verifiseringsformålet i fortalepunkt 51. Dette begrepet brukes tilsvarende i definisjonen i art. 4 nr. 14, mens forbudet i art. 9 nr. 1 bruker «uniquely identifying». Av hensyn til sammenheng i forordningen var det imidlertid trolig ikke hensikten at «unique identification» i art. 4 nr. 14 kun skulle vise til identifiseringsformålet.[94] Sammenhengen mellom fortalepunkt 51 og art. 9 nr. 1 må dermed tilsi at det kun er biometriske opplysninger med identifiseringsformål som er omfattet av forbudet.

Ved innsamling og bruk av biometriske opplysninger vil det både ved identifisering og verifisering foretas en sammenligningsprosess.[95] Den vesentlige forskjellen mellom formålene er måten opplysningene lagres på. Verifisering anses som mer personvernvennlig ved at opplysningene ofte lagres lokalt i en enhet, mens man ved identifisering lagrer opplysningene i en sentralisert database.[96] Til tross for at forskjellen i lagringsmetode for de to formålene ikke er omtalt i GDPR, vil det kunne forsvare at verifiseringsformål ikke skal være underlagt like streng regulering som identifisering.

På den andre siden er identifisering og verifisering ofte nøye knyttet sammen og det vil i mange tilfeller være vanskelig å skille formålene fra hverandre. Illustrerende er Esso-saken fra Personvernnemnda.[97] Saken gjaldt hvorvidt Esso, som arbeidsgiver, kunne benytte fingeravtrykk som adgangskontroll til et tankanlegg, begrunnet i sikkerhetsbehov. I forbindelse med adgangskontrollen ble personen først identifisert ved at det ble benyttet et adgangskort til å finne malen i databasen. Personen ble deretter bekreftet å ha adgang til anlegget. Saken viser at det i mange tilfeller vil skje en identifisering før personen verifiseres, og at det av den grunn kan være uheldig å skille mellom formålene.

Det er i forlengelsen av dette også en risiko for formålsutglidning i verifiseringssystemer. [98] Det vil i mange tilfeller være mulig å bruke et biometrisk system til både identifisering og

[94] Se Jasserand (2016) s. 306 som konkluderer med at hensikten i art. 4 nr. 14 må ha vært å vise til terskelen for identifikasjon av biometriske opplysninger som personopplysninger, fremfor å vise til identifiseringsformålet.
[95] Kindt (2017) s. 527.
[96] Kindt (2017) s. 527.
[97] PVN-2006-10 og Liu (2012) s. 9.
[98] Liu (2012) s. 9.

verifisering, og malen vil ofte kunne lagres sentralt også der formålet er å verifisere en person.[99] Det kan dermed være uheldig å utelate verifiseringsformål fra forbudet i art. 9 nr. 1.

Den teknologiske utviklingen kan likevel tilsi at det er hensiktsmessig med et mindre strengt regime for biometriske opplysninger med verifiseringsformål.[100] Flere kan på den måten benytte seg av tilgjengelig teknologi og implementere sikrere og mer effektive systemer for tilgangskontroll. Dersom også verifiseringsformål skal være omfattet av forbudet i art. 9 nr. 1, vil det i mange tilfeller hindre offentlige og private virksomheter å ta i bruk ny teknologi.

Dersom verifiseringssystemer skal være unntatt forbudet i art. 9 nr. 1, bør imidlertid bruken og oppbevaringen av opplysningene reguleres ytterligere. Dette spesielt for å sikre at opplysningene lagres lokalt i en enhet, slik at de i mindre grad er utsatt for misbruk eller at opplysningene kommer på avveie. Personvernrådet har kommet med forslag til hvordan biometriske opplysninger bør lagres for best mulig ivaretakelse av personopplysningsvernet.[101] GDPR har imidlertid ingen bestemmelser som vil sikre ivaretakelsen av personopplysningene dersom verifiseringsformål ikke skal anses omfattet av forbudet i art. 9 nr. 1.

Det konkluderes etter dette med at forbudet i art. 9 nr. 1 kun omfatter identifiseringsformål. Det kan ha gode grunner for seg om verifiseringsformål er unntatt fra forbudet, i lys av at innsamling og bruk av opplysninger til verifisering av identitet kan gjøres langt sikrere enn ved identifiseringsformål. Biometriske systemer blir i stor grad brukt til verifisering etter GDPR, og det vil derfor åpne for at mange virksomheter lettere kan benytte seg av denne typen teknologi. En avklaring fra Personvernrådet eller EU-domstolen er imidlertid nødvendig for at man med sikkerhet kan unnlate å anse biometriske opplysninger med verifiseringsformål som en særlig kategori av personopplysninger.

[99] Liu (2012) s. 9.
[100] Dette er bl.a. støttet av Kindt så lenge de biometriske opplysningene ikke lagres i sentrale databaser, se Kindt (2017) s. 535.
[101] Se EDPB, 3/2019, s. 18, avsnitt 88-89 der det nevnes ulike lagringstiltak som at biometriske prøver («raw data») bør slettes fra databasen, kryptering av lagrede biometriske opplysninger og begrensning av tilgangen til biometriske opplysninger.

4.3 Biometriske opplysninger som personopplysninger

Som tidligere nevnt er biometriske opplysninger først og fremst personopplysninger så lenge de kan knyttes til en «identifisert» eller «identifiserbar» fysisk person, jf. art. 4 nr. 1. Det fremgår videre av bestemmelsen at en person vil være «identifiserbar» både der personen kan identifiseres «direkte» og «indirekte». EU-domstolen uttalte i Breyer-dommen at ordet «indirekte» viser til at informasjonen alene ikke trenger å medføre identifisering, men at flere opplysninger samlet kan medføre slik identifisering.[102] Det er, som tidligere nevnt i kap. 3.1, også tilstrekkelig at en person kan skilles ut fra andre eller at slik utskillelse er mulig.

I vurderingen av om en person er «identifiserbar» skal det tas hensyn til «alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking», jf. fortalepunkt 26. Det skal videre i denne vurderingen tas hensyn til «alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utviklingen», jf. fortalepunkt 26.

Ved biometrisk identifisering og verifisering er en person vanligvis identifisert ved at vedkommende skilles ut fra andre.[103] Biometriske prøver, for eksempel ansiktsbilder eller bilder av fingeravtrykk, vil klart vanligvis utgjøre opplysninger om en «identifisert» eller «identifiserbar» person.

Utgangspunktet er at også den biometriske malen er å regne som en opplysning om en identifisert eller identifiserbar person.[104] Artikkel 29- gruppen har imidlertid uttalt at malen ikke vil anses som en personopplysning der lagringen av malen medfører at den ikke «med noen rimelige midler» («by no reasonable means») kan identifisere den registrerte.[105] Dette er langt på vei i tråd med det ovennevnte fortalepunkt 26 i forordningen. Det har imidlertid vært diskutert i hvilke tilfeller den biometriske malen dermed ikke skal anses som en personopplysning.[106]

[102] Dom av 19. oktober 2016 [C5], C-582/14, *Breyer,* ECLI:EU:C:2016:779 avsnitt 41.
[103] Artikkel 29-gruppen, 2003 s. 5.
[104] Artikkel 29-gruppen, 2003 s. 5.
[105] Artikkel 29-gruppen, 2003 s. 5, fotnote 11.
[106] Se bl.a. Liu (2010) s. 140–144 og Els. J. Kindt, Privacy and data protection issues of Biometric Applications: A Comparative Legal Analysis, 2013 s. 94–118.

I Personvernrådets veileder om bruk av videoovervåkning blir det gitt en rekke uttalelser om forslag til hvordan man kan minimere risiko ved behandling av biometriske opplysninger, herunder blant annet om ulike lagringsalternativer, kryptering av malen og retningslinjer for sletting.[107] Dette ble imidlertid ansett som en del av dataminimeringsprinsippet, uten at det ble vist til at malen kunne gjøres anonym med slike lagringsmetoder.

I den tidligere nevnte saken om Visma Retail fra Personvernnemnda, ble malen ansett som en anonym opplysning i forbindelse med verifisering av alder.[108] I vurderingen av hvorvidt personopplysningsloven 2000 § 12 kom til anvendelse ble det vist til at fingeravtrykket kun ble lagret som mal i systemet og at malen kun skulle registreres under hvorvidt personen var over eller under 18 år. Det ble dermed argumentert med at malen ikke ville være egnet til å identifisere personen.

I den ovennevnte saken ville kundens fingeravtrykk matches med den tidligere lagrede malen hver gang vedkommende ville kjøpe alkoholholdige varer i de selvbetjente kassene. Det er dermed vanskelig å unngå at malen linkes direkte til vedkommende som avgir fingeravtrykk på stedet.[109] Verifiseringssystemet ville dermed skille ut personen fra andre. Artikkel 29-gruppen har fastslått at det ikke er nødvendig å finne frem til en persons navn for å identifisere vedkommende, og at det er tilstrekkelig at man benytter andre identifikatorer til å skille ut en person fra en gruppe mennesker.[110] Dette gjenspeiles også i forordningens fortalepunkt 26 der «utpeking» kan være nok for å identifisere en person. Det er av denne grunn vanskelig å forstå hvorfor ikke malen ble ansett som en personopplysning i denne saken.

Det ble i saken om Visma Retail også vist til at det ikke er mulig å reversere en fingeravtrykksmal tilbake til selve fingeravtrykket. Det er imidlertid nyere forskning som åpner for en slik reversering.[111] Hvor nøyaktig en slik reversering blir vil blant annet avhenge av hvor nøyaktig kodet malen er. Artikkel 29-gruppen har i denne forbindelse lagt vekt på at man må finne en balanse der malen inneholder nok informasjon til at den med sikkerhet kun

[107] EDPB, 3/2019 s. 18, avsnitt 88-89.
[108] PVN-2011-11.
[109] Liu (2012) s. 9.
[110] Artikkel 29-gruppen, Opinion 4/2007, s. 14.
[111] Liu (2012) s. 9. Se også Jasserand (2016) s. 303 som viser til forskere som Adler, Bromba, Ross, Shah, Cain og Jain. Disse har kommet frem til at den biometriske malen delvis kan reverseres.

kan knyttes til et individ, samtidig som den ikke må inneholde mer informasjon enn nødvendig for å unngå en slik reversering.[112]

Hvorvidt malen er reversibel er imidlertid ikke nødvendigvis av betydning for hvorvidt den er en personopplysning etter art. 4 nr. 1. Der personopplysninger behandles i det biometriske system for identifiserings- eller verifiseringsformål, ville det være svært motstridende om malen i visse tilfeller kunne anses for å være en anonym opplysning og dermed ikke omfattet av forordningen.[113] At malen krypteres eller lagres på annen sikker måte, vil ikke nødvendigvis gjøre at malen ikke lenger kan knyttes til en identifisert eller identifiserbar person. Formålet med behandlingen i det biometriske system tilsier dermed klart at malen i de fleste tilfeller må anses som en personopplysning etter art. 4 nr. 1.

Artikkel 29-gruppen uttalte også i 2018 at til tross for at malen har en begrenset mengde med informasjon og er i kodet form, er det et format som skal fungere som en unik identifikator i en automatisert sammenligningsprosess.[114] Den skal i denne forbindelse tillate at informasjon om personen blir sammenholdt med andre informasjonskilder.[115] Malen måtte dermed anses som en biometrisk opplysning. Malens funksjon som en unik identifikator skiller seg også fra passord eller andre koder som ikke vil kunne knyttes til en spesifikk person.

Den teknologiske utviklingen har videre medført økt bruk av biometriske opplysninger til identifiserings- og verifiseringsformål i både offentlige og private virksomheter. Det er i denne forbindelse i stor grad den biometriske malen som samles inn og oppbevares for videre bruk. Den økte bruken vil naturlig kunne medføre en økt risiko for misbruk av slike opplysninger. Utviklingen i teknologi vil også klart vanskeliggjøre anonymisering av malen. Dette tilsier at den bør anses som en personopplysning så lenge den benyttes til disse formålene.

Det har avslutningsvis også vært tatt til orde for at malen kan anses som en anonym opplysning der den for eksempel blir brukt til verifisering av en person og lagret lokalt i en enhet som et adgangskort uten noen tilknytning til vedkommendes navn eller andre

[112] Artikkel 29-gruppen, 3/2012 s. 4.
[113] Se Kindt (2013) s. 117 som etter en nøye vurdering konkluderer med at malen må anses som en personopplysning der formålet er identifisering eller verifisering.
[114] Artikkel 29-gruppen, Opinion on Commission proposals on establishing a framework for interoptability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, 2018 s. 8.
[115] Artikkel 29-gruppen, Opinion on Commission Proposals, 2018 s. 8.

identifiserbare opplysninger.[116] En slik løsning med lagring i en enhet vil være langt mer personvernfremmende, men hvorvidt det gjør malen til en anonym opplysning er mer usikkert. Det vil imidlertid føre for langt å gå inn i denne diskusjonen her.

Det konkluderes etter dette med at den biometriske malen i de aller fleste tilfeller må anses som en personopplysning etter art. 4 nr. 1 der formålet er identifisering eller verifisering av en person. Hvorvidt det vil kunne være tilfeller der malen skal kunne anses som en anonym opplysning og utenfor forordningens anvendelsesområde er imidlertid fortsatt usikkert, og avhenger av en avklaring fra Personvernrådet eller EU-domstolen.

[116] Grijpink mener malen i slike tilfeller må anses som en anonym opplysning da det vil kreve uforholdsmessig med tid og midler for å gjøre malen identifiserbar, se Liu (2010) s. 141. Liu mener en slik utforming er personvernfremmende og at personen blir mindre identifiserbar, men at det er usikkert om en slik utforming vil tilfredsstille kravet til anonymitet.

5 Samtykke som grunnlag for innsamling av biometriske opplysninger

5.1 Generelt om samtykke som behandlingsgrunnlag

Samtykke som behandlingsgrunnlag er en sentral del av personvernregelverket i EU, der retten til selvbestemmelse og kontroll over egne personopplysninger utgjør sentrale hensyn.[117] Reglene om samtykke ivaretar disse hensynene og gjør den enkelte i stand til å påvirke bruken av personopplysninger som gjelder vedkommende selv.[118] Samtykke er inntatt i forordningen som behandlingsgrunnlag i art. 6 nr. 1 og i art. 9 nr. 2, i forbindelse med automatiserte avgjørelser etter art. 22 nr. 2 bokstav c og i forbindelse med overføring av personopplysninger til tredjeland i art. 49 nr. 1 bokstav a.

Samtykke som behandlingsgrunnlag i art. 6 og art. 9 er langt på vei en videreføring av reglene i personverndirektivet. Forordningens regler om samtykke er imidlertid blitt ytterligere styrket og gjort klarere.[119] Definisjonen av samtykke fremgår nå av art. 4 nr. 11, det er innført ytterligere krav til samtykke i art. 7 og det er ytterligere krav til samtykke for barn under 16 år i art. 8. Fortalepunktene 32, 33, 42 og 43 inneholder også informasjon om hvordan samtykkereglene bør forstås og praktiseres.

Samtykke er videre definert i art. 4 nr. 11 som en «frivillig, spesifikk, informert og utvetydig viljeserklæring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende». Det er videre et tilleggskrav for særlige kategorier av personopplysninger i art. 9 nr. 2 bokstav a at samtykke skal være «uttrykkelig». Hva som ligger i dette

[117] Opinion of Advocate General Szpunar, C-61/19, *Orange Romania* 4. mars 2020 avsnitt 36. Generaladvokatene er medlemmer av EU-domstolen og oppnevnt på samme måte som dommere. Generaladvokatene kommer vanligvis med rådgivende uttalelser om hvordan en sak for EU-domstolen bør avgjøres. Til tross for denne rådgivende rollen, blir deres oppfatninger ofte fulgt opp av domstolen. Se mer om deres rolle på https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)642237 (lest 15. mai 2020).
[118] C-61/19 avsnitt 37.
[119] Se Kuner, Bygrave og Docksey (2020) s. 181 som mener det er en vanlig misoppfatning at reglene for samtykke har blitt vesentlig strengere i forordningen. Reglene er langt på vei en videreføring av rettstilstanden slik den var under direktivet, men kravene har blitt tydeligere med forordningen.

tilleggskravet og hvorvidt det påvirker hvordan samtykke gis, har vært opphav til usikkerhet.[120] Dette vil vurderes nærmere i kap. 5.3.1.

Det fremgår videre av art. 7 nr. 2 at «[d]eler av en slik erklæring som er i strid med denne forordning, (...) ikke [skal] være bindende». Bestemmelsen viser dermed til at et samtykke som er i strid med forordningens øvrige bestemmelser, ikke anses som rettslig bindende. Artikkel 29-gruppen har videre uttalt at et samtykke fra den registrerte må være i tråd med forordningens øvrige prinsipper, herunder særlig prinsippene om rettferdighet, nødvendighet og proporsjonalitet etter GDPR art. 5.[121] Dataminimeringsprinsippet som en begrensning på hva det kan samtykkes til vil behandles nærmere i kap. 5.4.

De ovennevnte kravene til samtykke er svært viktig for å forhindre at virksomheters ønske om effektive løsninger og økonomiske interesse bidrar til forsøk på omgåelse av loven for å ta i bruk biometriske systemer og ny teknologi i strid med den registrertes interesser. Biometriske opplysningers sensitive karakter kan også tilsi at samtykke bør være et foretrukket behandlingsgrunnlag i tilfeller der den behandlingsansvarlige kan velge mellom flere grunnlag. Det er imidlertid klart at behandlingsgrunnlagene i forordningen rettslig sett er likestilte.

Kravene til samtykke ved innsamling av biometriske opplysninger vil i de neste kapitlene vurderes nærmere. Det vil i denne forbindelse vises til relevant praksis fra ulike nasjonale tilsynsmyndigheter i EU for å illustrere problemstillingene og hvordan de er håndtert. Det presiseres at praksis fra disse tilsynsmyndighetene ikke er rettslig bindende ved fortolkningen av forordningen, men at de i mangel av andre autoritative kilder gir en viktig anvisning på hvordan samtykkekravet ved innsamling av biometriske opplysninger skal forstås.

[120] Det var blant annet usikkerhet rundt hva som kreves av et informert samtykke, hvorvidt den registrerte kunne gi passivt samtykke og hva som ligger i kravet til «uttrykkelig» samtykke. Det var derfor intensjonen å styrke og tydeliggjøre samtykkereglene. Se Kuner, Bygrave og Docksey (2020) s. 177.
[121] EDPB, 05/20 s. 5, avsnitt 5.

5.2 Vilkår for gyldig samtykke etter art. 6 nr. 1 bokstav a jf. art. 4 nr. 11

5.2.1 Samtykket må være "frivillig" avgitt

Som tidligere nevnt er det et krav etter art. 4 nr. 11 at samtykket er avgitt «frivillig». En naturlig forståelse av «frivillig» er at samtykket må være valgfritt å avgi for den registrerte. Det fremgår videre av fortalepunkt 42 at samtykke ikke anses som frivillig avgitt om det ikke foreligger en «reell valgmulighet» eller der den registrerte «ikke er i stand til å nekte å gi eller trekke et samtykke uten at det er til skade for vedkommende». For at samtykket skal være reelt må den registrerte dermed kunne avslå uten noen reell frykt for represalier.

Det fremgår videre av fortalepunkt 43 at et samtykke ikke bør danne grunnlag for behandling av personopplysninger der det er en «klar skjevhet mellom den registrerte og den behandlingsansvarlige, særlig dersom den behandlingsansvarlige er en offentlig myndighet og det derfor er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendighetene som kjennetegner den bestemte situasjonen». Dette tilsier langt på vei at en skjev maktbalanse vil gjøre det vanskelig for den behandlingsansvarlige å bygge på samtykke som behandlingsgrunnlag.

Illustrerende i denne sammenheng er en sak fra det britiske datatilsynet, Information Commissioner's Office (ICO), der Her Majesty's Revenue and Customs (HMRC) med ansvar for innsamling av skatter i Storbritannia, samlet inn opptak av over 7 millioner menneskers stemme for bruk til verifisering/identifisering av kundene ved spørsmål over hjelpetelefon.[122] Stemmeopptakene utgjorde biometriske opplysninger etter GDPR art. 4 nr. 14, og ble ansett som en særlig kategori av personopplysninger etter art. 9 nr. 1. ICO kom til at kravene til samtykke ikke var innfridd.

Kundene ble informert om at verifiseringsmetoden var en sikrere og mer effektiv metode gjennom et automatisk opptak når de ringte hjelpetelefonen. Kundene ble deretter bedt om å gjenta «my voice is my password», uten noen informasjon om muligheten for annet

[122] ICO, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf avsnitt 13.

identifiseringsalternativ.[123] Der biometriske opplysninger skal brukes til identifiserings- eller verifiseringsformål, må den behandlingsansvarlige kunne tilby andre alternative muligheter som ikke innebærer behandling av biometriske opplysninger og som ikke innebærer noen tilleggskostnad for den registrerte.[124] Dette kan for eksempel være muligheten for å benytte et adgangskort og en kode i stedet for bruk av biometriske opplysninger.[125]

ICO uttalte videre at det var en klar skjevhet i maktforholdet mellom HMRC og dens kunder.[126] Dette gjaldt særlig for kundene som av velferdsgrunner befant seg i et avhengighetsforhold til myndighetene. Det ble ikke informert om at kundene kunne avslå å samtykke uten at dette ville være til skade for kundene. Samtykket var dermed klart ikke «frivillig» avgitt etter art. 4 nr. 11.

I tillegg til at offentlige myndigheter vil kunne ha vanskeligheter med å bygge på samtykke i kraft av sin særegne maktposisjon, var de grunnleggende kravene til samtykke heller ikke fulgt i den ovennevnte saken. Saken kunne derfor stilt seg annerledes om kundene var ytterligere informert om hva et samtykke ville innebære, om de hadde mulighet til å svare ja eller nei på om de ønsket å samtykke, og dersom de var sikret et annet alternativ til biometrisk identifikasjon. Det er likevel klart at det å gi fra seg biometrisk informasjon til myndigheter og andre i overordnede forhold kan forsterke følelsen av overvåkning for de registrerte, og mye kan dermed tilsi at samtykke ikke bør benyttes som behandlingsgrunnlag i slike tilfeller.

En skjevhet i maktbalanse kan også oppstå i forholdet mellom elever og skoler. Den svenske tilsynsmyndigheten, Datainspektionen, bøtela en videregående skole i Sverige på 200 000 svenske kroner for bruk av ansiktsgjenkjenningsteknologi for å registrere elevenes oppmøte.[127] Formålet var å effektivisere registreringen av oppmøte. Det var snakk om et prøveprosjekt der 22 av elevene hadde samtykket til bruken av teknologien. De elevene som

[123] ICO, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf avsnitt 15.
[124] EDPB, 3/2019 s. 17.
[125] Se for eksempel saken fra Personvernnemnda, PVN-2006-10 (Esso), der ansatte ved et tankanlegg kunne velge å benytte seg av ID-kort og en kode i stedet for fingeravtrykk. Samtykket ble derfor ansett for å være frivillig avgitt med en reell valgmulighet.
[126] ICO, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf avsnitt 24.
[127] Datainspektionen, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

ikke ville delta i prøveprosjektet kunne avstå fra dette ved at oppmøte ble foretatt på vanlig måte. Samtykket kunne også når som helst trekkes tilbake.

Det svenske datatilsynet mente likevel at elevenes avhengighetsforhold til skolen gjorde samtykket ugyldig.[128] Elevene var helt avhengig av skolen hva gjelder karakterer, studiefinansiering og muligheter for videre utdanning eller arbeid.[129] Til tross for at de øvrige kravene til samtykke langt på vei var innfridd, var det skjevheten i maktbalansen som gjorde samtykket ugyldig. Skoler vil derfor ha store vanskeligheter med å bygge på samtykke fra elever for biometrisk identifikasjon. Det var også snakk om bruk av ansiktsgjenkjenningsteknologi som kan gi en forsterket følelse av overvåkning og kontroll.

Det franske datatilsynet, CNIL, kom også i 2019 med en uttalelse om at bruk av ansiktsgjenkjenningsteknologi på to skoler i Marseilles og Nice som et prøveprosjekt, var i strid med GDPR.[130] CNILs avgjørelse ble ført for forvaltningsdomstolen i Marseilles, som 27. februar 2020 fulgte opp CNILs uttalelse om at behandlingen var ulovlig.[131] Dette er den første saken om ansiktsgjenkjenning for franske domstoler. Domstolen slo fast at samtykket til bruk av biometrisk identifikasjon var ugyldig som følge av det skjeve maktforholdet mellom skolen og elevene. Ansiktsgjenkjenningsteknologiens inngripen i personopplysningsvernet var også av betydning for avgjørelsen. Dataminimeringsprinsippets betydning i avgjørelsen vil omtales ytterligere i kap. 5.4.

I forbindelse med skjevhet i maktforhold som skranke for hvorvidt et samtykke er avgitt frivillig, er det også i et typisk arbeidsforhold problematisk å bygge på samtykket til den registrerte.[132] Personvernrådet går langt i å anslå at en arbeidstakers samtykke sjeldent vil være ansett for å være avgitt frivillig, med mindre det foreligger særegne forhold hvor det er klart at det å avslå å samtykke ikke vil innebære noen konsekvenser for arbeidstakeren.[133] Det

---

[128] Datainspektionen, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf s. 5.
[129] Datainspektionen, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf s. 5.
[130] CNIL, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position
[131] Forvaltningsdomstolen i Marseilles, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf
Se også avisartikkel på engelsk om saken: Biometric Update, «High Court rules against biometric facial recognition use in high schools», 28. februar 2020, https://www.biometricupdate.com/202002/french-high-court-rules-against-biometric-facial-recognition-use-in-high-schools (lest 27. mars 2020).
[132] EDPB, 05/20 s. 9, avsnitt 21.
[133] EDPB, 05/20 s. 9, avsnitt 21 og 22.

kan i denne forbindelse stilles spørsmål ved om en arbeidsgiver lovlig vil kunne anvende fingeravtrykk eller ansiktsgjenkjenningsteknologi som adgangskontroll til virksomhetens kontorer eller til systemer som oppbevarer sensitivt materiale med samtykke som behandlingsgrunnlag.

I en veiledende uttalelse fra det danske Datatilsynet fra 2019 var spørsmålet om en bedrift kunne registrere de ansattes timer ved hjelp av fingeravtrykksavlesning.[134] Datatilsynet vurderte i denne forbindelse hvorvidt samtykke kunne være et mulig behandlingsgrunnlag i slike tilfeller. De kom imidlertid til at et slikt samtykke ikke ville være avgitt frivillig da det ikke kunne garanteres at arbeidstakeren kunne nekte å samtykke uten noen frykt for represalier. Det ble likevel ikke avvist at et slikt samtykke i visse tilfeller kunne være gyldig.

I den tidligere nevnte saken fra Personvernnemnda om Esso fra 2006, ønsket Esso å ta i bruk fingeravtrykksavleser som adgangskontroll på et av deres tankanlegg.[135] Arbeidsgiver bygde i dette tilfellet på samtykke fra de ansatte. De som ikke ønsket å avgi fingeravtrykk, kunne i stedet anvende en kombinasjon av kode og kort. Fingeravtrykksystemet ble særlig begrunnet i et behov for sikkerhet for å hindre at uvedkommende skulle få adgang til tankanlegget.

I vurderingen av om de ansattes samtykke kunne anses for å være avgitt frivillig, ble det lagt vekt på at de kunne velge å benytte seg av annen identifikasjonsmetode enn ved biometri. De ansatte ble derfor ansett for å ha en reell valgmulighet. Det kan imidlertid spørres om dette er tilstrekkelig etter forordningen i lys av nyere praksis. Dersom arbeidsgiver anser det nødvendig å ta i bruk fingeravtrykksgjenkjenning av sikkerhetsmessige årsaker, kan det stilles spørsmål ved om de ansatte egentlig har noen reell mulighet til å avslå uten å føle et visst press på å godta denne formen for adgangskontroll.

En slik forståelse vil imidlertid langt på vei avskjære arbeidsgivere fra å benytte biometrisk identifikasjon, og kravet til et «frivillig» samtykke bør derfor trolig tolkes noe mindre strengt. Mye tilsier at et samtykke i arbeidsforhold lettere vil kunne anses gyldig der biometrisk identifikasjon anses nødvendig av sikkerhetsmessige årsaker enn der identifikasjonsmetoden benyttes til timeregistrering eller lignende.

[134] Datatilsynet (Danmark), https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/maj/vejledende-udtalelse-om-anvendelsen-af-fingeraftryk-til-brug-for-registrering-af-ansattes-komme-gaa-tider/
[135] PVN-2006-10.

5.2.2 Samtykket må være en «spesifikk, informert og utvetydig» viljesytring

At samtykke må være en «spesifikk» erklæring tilsier etter sin ordlyd at det må være et konkret formål med innsamlingen. Dette formålet må ikke favne for vidt, da det i slike tilfeller vil være vanskelig å vite hva den registrerte egentlig samtykker til. Dette henger nøye sammen med prinsippet om formålsbegrensning i art. 5 nr. 1 bokstav b. For biometriske opplysninger vil det ofte være ulike sikkerhetsformål som er aktuelle. Dette må imidlertid spesifiseres nærmere, for eksempel kan formålet være å hindre identitetstyveri eller å hindre at uvedkommende får adgang til en virksomhet eller et område.

At samtykke må være spesifikt henger også sammen med kravet til at det må være «informert». Dette gjenspeiles i prinsippet om åpenhet etter art. 5 nr. 1 bokstav a. Etter fortalepunkt 42 må den registrerte som minstekrav kjenne til den behandlingsansvarliges identitet og formålet med behandlingen. Personvernrådet stiller imidlertid også blant annet krav om at det informeres om hvilke opplysninger som samles inn og muligheten til å trekke tilbake samtykke.[136]

I den ovennevnte saken fra det britiske datatilsynet, ICO, der HMRC anvendte stemmegjenkjenningsteknologi for verifisering, ble ikke de registrerte tilstrekkelig informert om hvordan deres biometriske opplysninger skulle behandles eller at det var valgfritt å samtykke til innsamlingen.[137] Dette var ikke i tråd med kravene til et informert samtykke. Mangelen på et slikt informert samtykke oppfyller heller ikke hensynene til den registrertes selvbestemmelsesrett og muligheten til å kunne påvirke hvilke opplysninger som behandles om en selv.

Avslutningsvis skal samtykket også være «utvetydig». Det at samtykket skal være «utvetydig» innebærer at det skal gis «en erklæring eller en tydelig bekreftelse» på at vedkommende samtykker til innsamlingen etter art. 4 nr. 11. En slik bekreftelse vil være klarest der den er avgitt skriftlig. Dette vil også gjøre det lettere for den behandlingsansvarlige å kunne påvise at samtykke er gitt etter art. 7 nr. 1. Det kreves også en viss aktivitet fra den

[136] EDPB, 05/20 s. 15, avsnitt 64.
[137] Se avgjørelsen på: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf avsnitt 21.

registrerte der passivitet eller forhåndsavkryssede bokser ikke anses gyldig.[138] Facebook anvender ansiktsgjenkjenningsteknologi på bilder for identifisering av personer og deres relasjoner til deres «tag-funksjon», og hadde tidligere allerede automatisk krysset av for samtykke til bruk av ansiktsgjenkjenningsteknologi på bilder på plattformen, slik at den registrerte aktivt måtte endre dette til den avkreftende boksen dersom vedkommende ikke ønsket å samtykke.[139] En slik praksis er dermed ikke lenger i tråd med GDPR.

5.3 Vilkår for gyldig samtykke etter art. 9 nr. 2 bokstav a

5.3.1 Samtykke må være "uttrykkelig"

Etter art. 9 nr. 2 bokstav a stilles det et ytterligere krav om at samtykket må være «uttrykkelig». Det kreves dermed noe mer enn ordinært samtykke etter art. 6 nr. 1 bokstav a. En naturlig forståelse av «uttrykkelig» er at samtykket må være klart. Det vises dermed til måten samtykke skal uttrykkes på.[140] Et samtykke vil i denne forbindelse klart være fremsatt uttrykkelig i en skriftlig erklæring, men kan også oppfylles gjennom utfylling av et elektronisk skjema, ved e-post, og ved elektronisk signatur.[141] Personvernrådet har også uttalt at et samtykke kan gis muntlig, men at det da vil kunne være vanskelig å påvise at samtykket var avgitt før innsamlingen av personopplysningene.[142]

Som tidligere nevnt, har det vært usikkerhet rundt hva som skiller et «uttrykkelig» samtykke i art. 9 nr. 2 fra art. 4 nr. 11 der samtykke skal være «utvetydig» og gitt «ved en erklæring eller en tydelig bekreftelse». Hensikten var trolig at «uttrykkelig» skulle være et ytterligere vilkår som stiller strengere krav til samtykke.[143] Der «utvetydig» trolig sikter til at det ikke må være noen tvil om at den registrerte har samtykket, viser «uttrykkelig» til at det må samtykkes konkret til innsamlingen av de særlige kategoriene av personopplysninger som en separat prosess fra samtykke til øvrige personopplysninger, og at den behandlingsansvarlige spesifikt

[138] Se fortalepunkt 32. Se også EU-domstolens avgjørelse i dom av 1. oktober 2019 [GC], *Planet 49,* C-673/17, ECLI:EU:C:2019:801, avsnitt 52 og 65, der det ble fastslått at en nettsides forhåndsavkryssede bokser ikke utgjorde gyldig samtykke fra kundene når de aktivt måtte fjerne avkryssingen dersom de ikke ønsket å samtykke.
[139] Leo Kelion, «Facebook seeks facial recognition consent in EU and Canada», *BBC*, 18. april 2018, https://www.bbc.com/news/technology-43797128 (lest 11. mars 2020).
[140] EDPB, 05/20 s. 20, avsnitt 93.
[141] EDPB, 05/20 s. 20-21, avsnitt 93-94.
[142] EDPB, 05/20 s. 21, avsnitt 94. Det er et krav etter GDPR art. 7 nr. 1 at den behandlingsansvarlige må kunne «påvise» at et samtykke er avgitt.
[143] Personvernrådet legger til grunn at «uttrykkelig» er et tilleggsvilkår som stiller ytterligere krav til samtykke, se EDPB, 05/20 s. 21, avsnitt 92. Se også Kuner, Bygrave og Docksey (2020) s. 185.

ber om et slikt samtykke fra den registrerte.[144] Kravet til uttrykkelig samtykke går dermed noe lenger enn kravet til utvetydighet i art. 4 nr. 11.

Det vil klart variere i hvilken grad samtykke kan avgis uttrykkelig av den registrerte. Ved bruk av automatisert ansiktsgjenkjenning i kameraovervåkning, for eksempel i en butikk for tilpasset reklame, vil det klart være vanskelig å innhente uttrykkelig samtykke fra kundene før innsamlingen av personopplysninger. Motsetningsvis vil det ved bruk av ansiktsgjenkjenning som adgangskontroll til en virksomhets kontorer være lettere å tilfredsstille kravet ved å innhente samtykke fra vedkommende før innsamlingen av personopplysningene.

Som tidligere nevnt tar Facebook i bruk ansiktsgjenkjenningsteknologi på bilder og videoer for å identifisere personene på bildene og deres relasjoner. Bilder blir i den forbindelse sammenlignet med malen som er lagret av brukerne som samtykker til dette.[145] For innsamling av denne typen opplysninger er det dermed krav om at samtykket må være «uttrykkelig». Man vil i dag kunne trykke ja eller nei på spørsmål om man vil tillate denne typen behandling av biometriske opplysninger. Det er også enkelt å trekke tilbake samtykket i Facebooks innstillinger. Praksisen er dermed trolig i tråd med kravet til «uttrykkelig» samtykke.

5.4 Dataminimeringsprinsippet som begrensning for hva det kan samtykkes til

Personopplysningene som samles inn skal være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for». Prinsippet om dataminimering kommer også til anvendelse der den behandlingsansvarlige bygger på samtykke som grunnlag for den aktuelle behandlingen. Det vises videre til fremstillingen av dataminimeringsprinsippet i kap. 2.3.3.

Dataminimeringsprinsippet setter en viktig begrensning på adgangen til å samle inn og ellers behandle biometriske opplysninger. Ettersom GDPR er teknologinøytral og dermed ikke konkret adresserer de ulike problemstillingene som kan oppstå ved utviklingen av denne typen teknologi, er det viktig at innsamlingen av opplysninger begrenses. De ulike

[144] Kuner, Bygrave og Docksey (2020) s. 185.
[145] https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf s. 5.

biometriske teknikkene vil også kunne variere i den grad de oppleves inngripende i personopplysningsvernet.

En sentral del av dataminimeringsprinsippet er at det må vurderes om formålet kan oppnås på en annen rimelig måte enn ved bruk av biometrisk identifikasjon.[146] Det vil i mange tilfeller være mulig å benytte mindre inngripende midler enn biometriske identifiserings- eller verifiseringsmetoder. I tilfeller der den behandlingsansvarlige bygger på samtykke som behandlingsgrunnlag, skal den registrerte tilbys andre alternativer enn biometrisk identifikasjon for å sikre at samtykke er reelt og valgfritt. Så lenge man tilbyr andre alternativer, vil man kunne argumentere for at den biometriske identifikasjonen ikke er nødvendig for å oppnå formålet etter dataminimeringsprinsippet. Dette vil imidlertid avskjære samtykke som et behandlingsgrunnlag for innsamling av biometriske opplysninger. Dette var trolig ikke intensjonen bak reglene i forordningen, og kan tilsi at dataminimeringsprinsippet må praktiseres noe mildere ved samtykke enn ved øvrige behandlingsgrunnlag.

Illustrerende er den tidligere nevnte saken om bruk av ansiktsgjenkjenning på elever ved en svensk skole for registrering av oppmøte. I tillegg til at samtykke vanskelig kunne avgis frivillig i tråd med art. 4 nr. 11, kunne registrering av oppmøte skje på en langt mindre inngripende måte enn ved bruk av ansiktsgjenkjenningsteknologi. Denne formen for fraværskontroll var svært inngripende i elevenes integritet, og ikke nødvendig for å oppnå formålet.[147] Ettersom ansiktsgjenkjenningsteknologien er spesielt inngripende i den enkeltes personopplysningsvern, er det grunn til å tro at bruk av denne formen for teknologi ofte vil anses som overdreven for å oppnå det bestemte formålet.

Den tidligere nevnte saken fra Frankrike der ansiktsgjenkjenningsteknologi ble innført som adgangskontroll til to skoler som et prøveprosjekt, illustrerer også problematikken.[148] Det ble bygd på samtykke som behandlingsgrunnlag og formålet var å forhindre at uvedkommende skulle få adgang til skolene. Den franske tilsynsmyndigheten, CNIL, mente imidlertid at bruken av ansiktsgjenkjenning på elevene var i strid med GDPRs krav til dataminimering. Det ble i denne forbindelse uttalt at formålet om å bevare sikkerheten ved skolene kunne oppnås

[146] Se fortalepunkt 39.
[147] Datainspektionen, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf s. 12.
[148] CNIL, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position Se også avisartikkel på engelsk om saken: Laura Kayali, «French privacy watchdog says facial recognition trial in high schools is illegal», Politico 29. oktober 2019, https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/ (lest 27. februar 2020).

ved bruk av langt mindre inngripende midler i den enkeltes personopplysningsvern og individuelle friheter. Det ble også vist til at ansiktsgjenkjenning gir en klart forsterket følelse av overvåkning og risiko for at personopplysningene kommer på avveie ved datainnbrudd eller lignende. Det ble dermed ikke ansett nødvendig å anvende ansiktsgjenkjenningsteknologi ved skolene. Også forvaltningsdomstolen i Marseilles fulgte opp CNILs avgjørelse, og viste til at formålet kunne oppnås med langt mindre inngripende midler.[149]

Både den svenske og den franske saken viser at det skal mye til for at skoler skal kunne bygge på samtykke som behandlingsgrunnlag for bruk av ansiktsgjenkjenningsteknologi. Hvorvidt bruk av ansiktsgjenkjenningsteknologien i det hele tatt vil være nødvendig i et demokratisk samfunn og dermed tilfredsstille kravene til dataminimering i forordningen, er diskuterbart. EUs datatilsynsmann har uttalt at det er høyst usikkert om ansiktsgjenkjenningsteknologien tilfredsstiller kravet til dataminimering, og at risikoen for overdreven innsamling av opplysninger for å få et mest mulig nøyaktig resultat uten risiko for falsk positive og falsk negative resultater er høyst aktuell.[150] Ansiktsgjenkjenningsteknologien er dermed fortsatt svært kontroversiell og reiser både viktige personvernrettslige og etiske problemstillinger. Det viser også at GDPR som en teknologinøytral forordning kan komme til kort ved reguleringen av biometriske opplysninger.

Dataminimeringsprinsippet kan også sette begrensninger ved bruk av annen biometrisk teknologi som fingeravtrykksgjenkjenning. I en avgjørelse av det polske datatilsynet, Urząd Ochrony Danych Osobowych (UODO), ble det utstedt gebyr til en skole som samlet inn elevenes fingeravtrykk til bruk for verifisering ved betaling i skolens kantine.[151] Skolen bygde i denne forbindelse på skriftlig samtykke fra elevenes foreldre for behandling av elevenes

[149] Forvaltningsdomstolen i Marseilles, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf
Avisartikkel på engelsk om saken: https://www.biometricupdate.com/202002/french-high-court-rules-against-biometric-facial-recognition-use-in-high-schools (lest 27. mars 2020).
[150]Wojciech Wiewiórowski, «Facial recognition: A solution in search of a problem?», 28. oktober 2019 https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (lest 25. februar 2020). Dette er et blogginnlegg av EUs datatilsynsmann publisert på EUs datatilsyns hjemmesider og er ikke en offisiell uttalelse fra datatilsynet. EUs datatilsyn har videre ansvaret for tilsyn med EUs institusjoner med hjemmel i forordning 2018/1725 som ble fornyet i tråd med GDPRs ikrafttreden.
[151] Det polske datatilsynet: Prezes urzędu ochrony danych osobowych, 4. mars 2020, https://uodo.gov.pl/en/553/1102
Se også pressemelding fra Personvernrådet på engelsk: *Fine for processing student's fingerprints imposed on a school,* 5. mars 2020, https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en (lest 10. mars 2020).

fingeravtrykk. Driften av skolens kantine bygde imidlertid på art. 6 nr. 1 bokstav e, [152] og skolen kunne dermed ikke bygge på samtykke som behandlingsgrunnlag for innsamling av elevenes fingeravtrykksopplysninger.

Det polske datatilsynet uttalte videre at formålet om effektiv betaling i skolens kantine kunne gjennomføres med langt mindre inngripende midler enn bruk av fingeravtrykk. Det var ikke nødvendig å benytte fingeravtrykksgjenkjenning på elevene for at de skulle få tilgang til mat i skolens kantine. Elevene var også mindreårige. Fingeravtrykksystemet var derfor i strid med dataminimeringsprinsippet.

De ovennevnte sakene fra datatilsyn i Sverige, Frankrike og Polen viser at dataminimeringsprinsippet i mange tilfeller vil begrense adgangen til innsamling og bruk av biometriske opplysninger. Det kan innvendes mot denne praksisen at den registrerte ved samtykke selv har godtatt innsamlingen av personopplysningene, og at dataminimeringsprinsippet av den grunn ikke bør anvendes like strengt som der behandlingsansvarlig bygger på et av de øvrige behandlingsgrunnlagene. Det er imidlertid likevel viktig å unngå en overdreven innsamling av personopplysninger med den økte risikoen for misbruk dette kan medføre. Også biometriske opplysningers sensitive karakter tilsier at dataminimeringsprinsippet bør praktiseres strengt også ved samtykke som behandlingsgrunnlag.

[152] GDPR art. 6 nr. 1 bokstav e: «behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt».

6 Avsluttende bemerkninger

Vurderingen av art. 4 nr. 14 og art. 9 nr. 1 viser at forordningen i større grad enn før adresserer de personvernrettslige utfordringene som kan oppstå med biometrisk identifikasjon. Til tross for at definisjonen langt på vei er en videreføring av Artikkel 29-gruppens definisjon, er den helt sentral for et økt fokus på biometriske opplysninger i et personvernrettslig perspektiv. Både definisjonen og bestemmelsen om særlige kategorier av personopplysninger benytter imidlertid en annen terminologi enn den som benyttes i det biometriske fagmiljøet. Dette bidrar til økt uklarhet om hvordan bestemmelsene skal forstås og hvilke opplysninger som skal anses omfattet.

Det er videre mye som tilsier at det kun er biometrisk identifisering som skal anses som en særlig kategori av personopplysninger. Dette åpner for en mer vidtrekkende bruk av biometriske opplysninger til verifiseringsformål. Det vil også innebære at innsamling av biometriske opplysninger til verifiseringsformål, ikke nødvendigvis vil være underlagt regler om utarbeiding av DPIA. Til tross for at verifiseringsformål i mange tilfeller er mer personvernvennlig enn identifisering, er det også tilfeller der identifiserings- og verifiseringsformålet vil flyte over i hverandre. Dersom verifiseringsformål skal falle utenfor forbudet, bør det derfor utarbeides ytterligere regler om hvordan de biometriske opplysningene skal lagres for å sikre at opplysningene samles inn og videre behandles i tråd med forordningen. Den foreløpige uklarheten i hvordan bestemmelsen skal forstås, vil imidlertid trolig fortsatt medføre at de fleste som benytter seg av biometri til verifiseringsformål vil anse opplysningene som en særlig kategori av personopplysninger. Dette for å forsikre seg om at behandlingen er i tråd med forordningen.

Reglene om samtykke stiller høye krav til hvordan biometriske opplysninger kan samles inn. Drøftelsen viser at der behandlingsansvarlig og den registrerte står i et over- og underordnet forhold, skal det mye til for å anse et samtykke som avgitt frivillig. Offentlige myndigheter vil derfor svært sjeldent kunne bygge på samtykke som behandlingsgrunnlag. Til tross for at terskelen for et gyldig samtykke heves noe dersom de biometriske opplysningene er særlige kategorier av personopplysninger, viser drøftelsen at kravene til et gyldig samtykke for alminnelige personopplysninger allerede vil kunne være vanskelig å innfri.

Oppgaven viser også at behandlingsansvarlig vil kunne ha vanskeligheter med å innfri prinsippet om dataminimering ved innsamling av biometriske opplysninger. Det vil ofte være mulig å benytte andre mindre inngripende former for identifikasjon. Særlig ansiktsgjenkjenningsteknologien utfordrer dataminimeringsprinsippet ved både å være svært inngripende i den enkeltes integritet, og ved at den ofte vil kreve innsamling av store mengder opplysninger for å unngå falsk positive og falsk negative resultater. Den teknologiske utviklingen vil likevel klart medføre økt bruk av denne formen for identifikasjon. En avklaring fra Personvernrådet med retningslinjer om hvordan biometriske opplysninger kan behandles etter forordningen, er helt nødvendig for å sikre et effektivt regelverk.

Det kan avslutningsvis stilles spørsmål ved om biometriske opplysninger burde vært regulert i et eget regelverk, uavhengig av personvernregelverket. Dette ville åpnet for ulike regler knyttet til de ulike formatene, der man kunne forby behandling av biometriske prøver og kun tillate behandling av malen.[153] Man ville også hatt muligheten til å skille mellom de ulike formene for biometriske opplysninger der man kunne underlagt mer inngripende former for identifikasjon strengere regulering. Dette kunne bidratt til ytterligere klarhet i regelverket, større grad av forutberegnelighet og et sterkere vern om opplysningene.

[153] Paul De Hert, The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us, *European Data Protection Law Review,* Volume 2 (2016) nr. 4 s. 461–466 på s. 465.

7 Kilderegister

7.1 Lover

EØS-loven (1992)	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)
Personopplysningsloven (2000)	Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)
Personopplysningsloven (2018)	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

7.2 Forordninger og direktiver

Personverndirektivet (1995)	Europaparlaments og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger
Personvernforordningen (2016)	Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (GDPR)

LED («Law Enforcement Directive»)	Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS
Forordning 2018/1725	Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og agenturer og om fri utveksling av slike opplysninger og om opphevelse av forordning (EF) nr. 45/2001 og avgjørelse nr. 1247/2002/EF

7.3 Norske og internasjonale forarbeider

European Commission (2012)	European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)*, 25. januar 2012 s. 5 (Tilgjengelig på: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT (lest 2. april 2020))

Prop. 56 LS (2017-2018)	Prop.56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen*
Prop. 115 L (2017-2018)	Prop. 115 L (2017–2018) *Endringer i personopplysningsloven (bekjempelse av arbeidslivskriminalitet)*

7.4 Rettspraksis fra EU-domstolen

Sak C-424/10 og C-425/10	Dom av 21. desember 2011 [GC], *Ziolkowski og Szeja mfl.,* ECLI:EU:C:2011:866
Sak C-291/12	Dom av 17. oktober 2013 [C5], *Schwarz,* ECLI:EU:C:2013:670
Sak C-345/13	Dom av 19. juni 2014 [C5]*, Karen Millen Fashions,* ECLI:EU:C:2014:2013
Sak C-446/12 og C-449/12	Dom av 16. april 2015, *Willems and others,* ECLI:EU:C:2015:238
Sak C-582/14	Dom av 19. oktober 2016 [C5], *Breyer*, ECLI:EU:C:2016:779

Sak C-670/16	Dom av 26. juli 2017 [GC], *Mengesteab*, ECLI:EU:C:2017:587
Sak C-434/16	Dom av 20. desember 2017 [C5], *Peter Nowak,* ECLI:EU:C:2017:994
Sak C-673/17	Dom av 1. oktober 2019 [GC], *Planet49,* ECLI:EU:C:2019:801
Sak C-61/19	Opinion of Advocate General Szpunar 4 mars 2020, *Orange Romania*, ECLI:EU:C:2020:158

7.5 Veiledere og uttalelser fra EU-organer

A29WP Working document 2003	Article 29 Data Protection Working Party, *Working document on biometrics,* WP80, 2003
A29WP Opinion 4/2007	Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* WP136, 2007
A29WP Opinion 1/2010	Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP169
A29WP Opinion 3/2012	Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* WP193, 2012

A29WP Opinion 02/2012	Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services,* WP192, 2012
A29WP Guidelines on consent 2018	Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679,* WP259, 2018
A29WP Opinion 2018	Article 29 Data Protection Working Party, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration,* WP266, 2018
EDPB Guidelines 2/2019	European Data Protection Board, *Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects,* 2019
EDPB Guidelines 3/2019	European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices,* EDPB Plenary Meeting, 2019
EDPB Guidelines 05/20	European Data Protection Board, *Guidelines 05/20 on consent under Regulation 2016/679,* Version 1.1, 13 May 2020, adopted on 4 May 2020

7.6 Avgjørelser fra norske og internasjonale tilsynsmyndigheter

7.6.1 Internasjonale avgjørelser

Information Commissioner's Office (ICO)	ICO, Enforcement Notice to Her Majesty's Revenue and Customs, 9. mai 2019 (Tilgjengelig på: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf)
Datatilsynet (Danmark)	Datatilsynet, *Vejledende udtalelse om anvendelsen af fingeraftryk til brug for registrering af ansattes komme-/gå-tider*, 29. mai 2019 (Tilgjengelig på: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/maj/vejledende-udtalelse-om-anvendelsen-af-fingeraftryk-til-brug-for-registrering-af-ansattes-komme-gaa-tider/)
Datainspektionen	Datainspektionen, *Tillsyn enlight EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever,* sak DI-2019-2221, 20. august 2019 (Tilgjengelig på: https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf)

Commission nationale de l'informatique et des libertés (CNIL)	CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL precise sa position*, 29. oktober 2019 (Tilgjengelig på: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position)
Urząd Ochrony Danych Osobowych (UODO)	Det polske datatilsynet Urząd Ochrony Danych Osobowych (UODO), 18. februar 2020 (Tilgjengelig på: https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018)
Tribunal Administratif de Marseilles (forvaltningsdomstolen i Marseilles)	Tribunal Administratif de Marseilles, N° 1901249, 27. februar 2020 (Tilgjengelig på: https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf)

7.6.2 Norske avgjørelser

Esso	PVN-2006-10
Visma Retail	PVN-2011-11

7.7 Litteratur

7.7.1 Bøker

Fredriksen og Mathisen (2018)	Fredriksen, Halvard Haukeland, Mathisen, Gjermund, *EØS-rett,* 3. utg. Fagbokforlaget 2018
Kindt (2013)	Kindt, Els. J., *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis,* Springer 2013
Kuner, Bygrave og Docksey (2020)	Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher, *The General Data Protection Regulation: a commentary,* Oxford 2020
Liu (2010)	Liu, Nancy Yue*, Bio-privacy: Legal Challenges for Privacy Regulations of Biometric Identification and Authentication,* Faculty of Law, University of Oslo 2010
Schartum og Bygrave (2016)	Schartum, Dag Wiese, Bygrave, Lee A., *Personvern i Informasjonssamfunnet: En innføring i vern av personopplysninger,* 3. utg. Fagbokforlaget 2016
Skullerud mfl. (2019)	Skullerud, Åste Marie Bergseng, Rønnevik, Cecilie, Skorstad, Jørgen, Pellerud, Marius Engh, *Personopplysningsloven og personvernforordningen (GDPR), Kommentarutgave,* Universitetsforlaget 2019

Wessel-Aas (2018) — Wessel-Aas, Jon og Ødegaard, Magnus, *Personvern - publisering og behandling av personopplysninger,* Gyldendal Norsk Forlag 2018

7.7.2 Artikler

De Hert (2016) — De Hert, Paul, *The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us,* European Data Protection Law Review Volume 2 (2016) Issue 4

Jasserand (2016) — Jasserand, Catherine, *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data,* European Data Protection Law Review, vol. 2 (2016) nr. 3 s. 297-311

Kindt (2017) — Kindt, E. J., *Having yes, using no? About the new legal regime for biometric data,* Computer Law & Security Review 34 (2018) s. 523-538, 2017

Liu (2012) — Liu, Nancy Yue, *Biometri, fingeravtrykk og personvern,* LoD-2012-110-9, 2012

7.7.3 Nettsider

BBC (2018) — Leo Kelion, «Facebook seeks facial recognition consent in EU and Canada», *BBC*, 18. april 2018 (Tilgjengelig på:

https://www.bbc.com/news/technology-43797128) (lest 11. mars 2020)

Biometric Update (2020) — Biometric Update, «French high court rules against biometric facial recognition use in high schools», 28. februar 2020 (Tilgjengelig på: https://www.biometricupdate.com/202002/french-high-court-rules-against-biometric-facial-recognition-use-in-high-schools (lest 27. mars 2020))

CNIL (2019) — CNIL, «Facial recognition: for a debate living up to the challenges», 15. November 2019 (Tilgjengelig på: https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf (lest 11. februar 2020)).

Datatilsynet (2019) — Datatilsynet, «Biometri», 17. juli 2019, (Tilgjengelig på: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/) (lest 19. mars 2020).

EDPS (2019) — Wojciech Wiewiórowski, «Facial recognition: A solution in search of a problem?», 28. oktober 2019 (Tilgjengelig på: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (lest 27. februar 2020))

EDPB (2020) European Data Protection Board, «Fine for processing student's fingerprints imposed on a school», 5. mars 2020 (Tilgjengelig på: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en (lest 10. mars 2020)

European Parliament (2019) European Parliament, «Role of Advocates General at the CJEU», 10. oktober 2019 (Tilgjengelig på: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)642237 (lest 15. mai 2020))

Politico (2019) Laura Kayali, «French privacy watchdog says facial recognition trial in high schools is illegal», Politico 29. oktober 2019, (Tilgjengelig på: https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/) (lest 27. februar 2020).