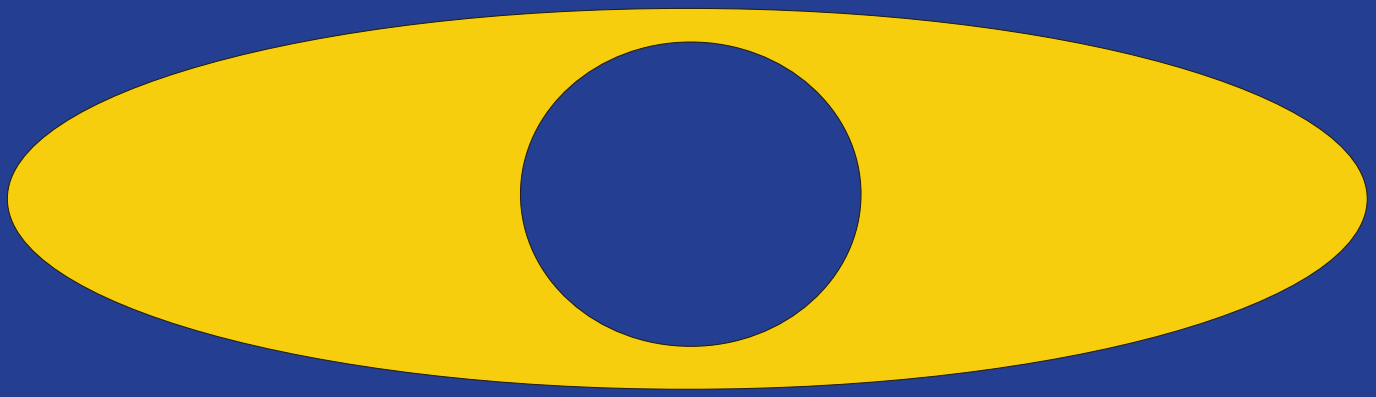
Retten til privatliv

I en biometrisk overvåget verden



Udarbejdet af: Henrik Wold Høffner & Julian Bremer

Vejleder: Tanja Kammersgaard Christensen

AALBORG
UNIVERSITY

Juridisk kandidatspeciale

Retten til privatliv i en biometrisk overvåget verden

Engelsk titel:

The Right to Privacy in a World of Biometric Surveillance

Forfattere:

Henrik Wold Høffner

Studienr.: 20214642

Julian Bremer

Studienr.: 20215689

Studie:

Jura

Retsområde:

Databeskyttelsesret

Universitet:

Aalborg Universitet

Vejleder:

Tanja Kammersgaard Christensen

Afleveringsdato:

13. maj 2026

Abstract

The purpose of this thesis is to examine under which conditions biometric surveillance, understood as surveillance involving the processing of biometric data for the purpose of uniquely identifying a natural person, may be legitimized under the Charter of Fundamental Rights of the European Union and data protection law in countries of the European Union.

The right to privacy and the protection of personal data are fundamental rights protected by The European Charter of Fundamental Rights in article 7 and 8. However, interference in these rights may be justified when the conditions laid down in Article 52(1) of the charter are fulfilled. It follows from this article that any interference must have a legal basis, respect the essence of the protected rights in the Charter, pursue an objective of general interest recognized by the Union, and comply with the principle of proportionality.

The thesis analyses the legal framework governing biometric surveillance under the General Data Protection Regulation (GDPR), with particular emphasis on Article 9 concerning the processing of special categories of personal data. Since biometric data used for unique identification constitutes special categories of personal data, this processing is under strict requirements in order for the processing to be legal.

The analysis of the thesis will focus specifically on the regulations in Article 9(2)(g) GDPR and explicit consent under Article 9(2)(a) GDPR, where processing can be legitimized through either substantial public interest or the explicit consent of the data subject.

The thesis illustrates that biometric surveillance constitutes a serious interference with the right to privacy through an analysis of case law from the Court of Justice of the European Union, decisions from EU national data protection authorities, and other relevant legal sources.

Therefore, processing of special categories of personal data may only be legitimized if it is strictly necessary and supported by legal safeguards. These safeguards include proportionality assessment, which includes an evaluation of whether less intrusive alternatives are present, whether the processing is limited to what is necessary and whether adequate safeguards exist to protect the rights of the registered person.

Furthermore, the thesis concludes that in order for processing to be made legal substantial public interest must be interpreted restrictively and thus cannot be based only on a public interest. Additionally, explicit consent is only a relevant legal base if no power imbalance exists between the Data controller and the data subject and if the data subject has a genuinely free choice with regards to the processing.

Finally, the thesis argues that rapid technological developments in biometric surveillance increasingly challenge existing data protection frameworks, highlighting the continuing need for effective legal safeguards to ensure that the right to privacy is not gradually undermined.

Indholdsfortegnelse

1. Indledning

Frygten for total overvågning er ikke en nyopstået frygt, men har tidligere været genstand for stor opmærksomhed i fortiden. Det afspejles i en af de store romaner fra det 20. århundrede, hvor George Orwell i sin roman *1984* fra 1949 skildrer et dystopisk samfund præget af konstant overvågning, hvilket bl.a. kommer til udtryk i bogens centrale slogan *Big Brother is Watching You*.

På trods af frygten for overvågning, kan overvågning anskues som et tveægget sværd, da den på den ene side kan skabe trygge rammer, når dette sker for at forebygge kriminalitet og uro, men på den anden side kan den bidrage til en følelse af konstant overvågning hos den enkelte registrerede.

Denne problemstilling er i dag blevet forstærket af den teknologiske udvikling. Førhen bestod overvågning primært af passiv overvågning uden mulighed for direkte identifikation, men moderne teknologier har gjort det muligt at identificere den registrerede i realtid, ved at koble overvågningsdata sammen med biometriske analysesoftware, der matcher biometriske data med den enkelte registrerede.

Førhen krævede identifikation ofte en aktiv handling, såsom fremvisning af legitimation, hvorimod processen i dag ofte er automatiseret og usynlig. Dette svækker den registreredes bevidsthed om identitetseksponeringen, men det er mere effektivt og tillader en hurtigere identifikation.[1]

Retten til privatliv bliver derfor særligt udfordret af overvågningssystemer, der anvender biometriske data med henblik på entydig identifikation, da biometriske data er unikke og tæt knyttet til den enkelte registreredes identitet. En uretmæssig behandling af disse data kan derfor få vidtrækkende konsekvenser for den enkelte registrerede og give en følelse af konstant overvågning, hvilket kan medføre adfærdsændringer hos den registrerede.[2]

Overvågningen kan være nødvendig af hensyn til samfundsinteresser, hvorfor hensynet til kollektivet kan veje tungere end den enkeltes ret til privatliv. Derfor opstår der en afvejning af, om det ene går forud for det andet.

Formålet med specialet er derfor at illustrere, under hvilke forhold behandlingen af biometriske data kan anses for proportionel ift. overvågning.

[1] First Response Group (2024), s. 4f & 10 f

[2] Institut for menneskerettigheder (2019), s. 4 & 7

2. Problemformulering

Hvornår kan overvågning, der behandler biometriske data med det formål entydigt at identificere en fysisk person, legitimeres i henhold til Chartret og Databeskyttelsesretten?

3. Afgrænsning

Specialet har til hensigt at illustrere, hvornår overvågning der behandler biometriske data med det formål entydigt at identificere en fysisk person, kan legitimeres ud fra Den Europæiske Unions Charter om grundlæggende rettigheder[3] (Chartret), Databeskyttelsesforordningen[4] (GDPR) og databeskyttelsesloven[5] (DBL).

3.1 Personoplysninger

Det følger af GDPR art. 4, nr. 1., at personoplysninger udgør enhver form for information om en identificeret eller identificerbar fysisk person, hvormed menes en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator såsom et navn, identifikationsnummer, lokaliseringsdata, online identifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.[6]

Selvom biometriske data i sig selv udgør en personoplysning, vil personoplysningsbegrebet ikke blive behandlet yderligere i specialet, da det forudsættes, at læseren har et indgående kendskab til, hvad der udgør en personoplysning.

3.2 Dataansvarlig og databehandler

Den dataansvarlige er den, der afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger, jf. GDPR art. 4, nr. 7. En databehandler er derimod den, der behandler personoplysninger på vegne af den dataansvarlige, jf. GDPR art. 4, nr. 8. Både den dataansvarlige og databehandleren kan bestå af en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ.[7]

---

[3] DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER 2012/C 326/02

[4] Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

[5] Lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven)

[6] Lotterup & Nielsen, 2025, s. 242

[7] Trzaskowski et al., 2025, s. 66 f

Specialet vil ikke gå yderligere i dybden med, hvorvidt der er tale om en databehandler eller dataansvarlig, da ansvaret for disse pågældende aktører ikke vurderes at være af relevans for besvarelsen af problemformuleringen.

3.3 Bøder

En række af dommene, herunder *Google Spain*[8] med stor præcedensværdi, diskuterer, hvorvidt den omhandlede krænker alene er at betegne som databehandler eller som dataansvarlig. Dette har relevans for det bødeomfang, som den pågældende kan blive pålagt, da dataansvarlige, der er involveret i behandling, vil hæfte for den skade, der er forvoldt af behandling, der overtræder GDPR, jf. GDPR art. 82, stk. 2, 1. pkt. En databehandler vil dog alene hæfte for den skade, som behandlingen har medført, hvis denne ikke har opfyldt sine forpligtelser i henhold til GDPR, eller hvis denne har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser, jf. GDPR art. 82, stk. 2., 2. pkt.
Specialet behandler ikke denne problemstilling yderligere, da den vurderes at være irrelevant for besvarelsen af problemformuleringen.

3.4 EMRK

Specialets fokus på GDPR og Chartret betyder, at specialet afgrænses for at behandle EMRK[9]. Ved overvågning af personer vil der ske et indgreb i retten til privatliv, hvilket potentielt kan være i strid med EMRK art. 8 om retten til privatliv.[10] Chartret art. 7 regulerer ligeledes retten til privatliv og uddybes yderligere i Chartret art. 8 om retten til beskyttelse af personoplysninger. Det følger yderligere af Chartrets art. 52, stk. 3, at i det omfang Chartret indeholder rettigheder svarende til EMRK, vil den have samme betydning og omfang i EMRK. Dette er dog ikke hinder for, at EU-retten kan yde en mere omfattende beskyttelse. Retspraksis har vist, at når Den Europæiske Unions Domstol (EUD) afsiger afgørelser, kan der forekomme henvisninger til praksis fra EMD[11] ved overlappende bestemmelser og vice versa, hvorfor disse bestemmelser skal fortolkes ens.[12] Derved vil EMRK implicit fortsat spille en rolle i specialet.

[8] Google Spain og Google, C-131/12, EU:C:2014:317
[9] Lovbekendtgørelse nr. 138 af 26/01/2022 om Den Europæiske Menneskerettighedskonvention
[10] Christensen, 2021, s. 127
[11] Den Europæiske Menneskerettighedsdomstol
[12] Christensen, 2021, s. 91

3.5 Retshåndhævelsesdirektivet

Retshåndhævelsesdirektivet[13] bygger i visse tilfælde direkte på bestemmelser fra GDPR, men der er også en række bestemmelser, hvor de adskiller sig fra GDPR.[14] Derfor er det ikke muligt at anvende retshåndhævelsesdirektivet og GDPR analogt, idet det kan medføre, at behandlingen efter den ene bestemmelse er legitim, mens det er retsstridigt efter den anden. Retshåndhævelsesdirektivet er blevet implementeret i dansk ret i form af Retshåndhævelsesloven,[15] og anvendelsesområdet er reguleret i retshåndhævelsesloven § 1, stk. 1. Herefter finder loven anvendelse for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, når behandlingen af personoplysninger foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner. Loven finder derfor anvendelse for retshåndhævende myndigheder, som behandler personoplysninger, og behandlingen har et af ovenstående formål.[16]

Fordi specialet fokuserer på de databeskyttelsesretlige rammer for offentlige og private aktørers behandling af biometriske data efter GDPR, vil behandlingsaktiviteter, der falder inden for ovenstående anvendelsesområde, ikke blive behandlet yderligere.

3.6 TV-overvågningsloven

Når der foretages videoovervågning, er det ikke alene GDPR, der vil finde anvendelse, men derimod også TV-overvågningsloven[17]. Det følger af Tv-overvågningslovens § 1, stk. 1, at denne handler mere om de fysiske lokationer, hvor der ikke må foretages tv-overvågning, og ikke om selve behandlingen af personoplysninger.

Specialet vil derfor ikke inddrage TV-overvågningsloven yderligere i dets betragtninger.

---

[13] Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA

[14] Christensen, 2021, s. 202

[15] Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer

[16] Christensen, 2021, s. 221 f

[17] Lovbekendtgørelse nr. 182 af 24/02/2023 om lov om tv-overvågning med senere ændringer

3.7 Databeskyttelsesretten

Specialet vil have et særligt fokus på samtykke og væsentlige samfundsinteresser som behandlingsgrundlag, når der sker behandling af biometriske data med formål at identificere den registrerede. Derfor vil specialet hovedsageligt behandle GDPR art. 5, stk. 1, litra c, d, og e, samt art. 9. stk. 2, litra a og g, hvorfor der afgrænses fra de øvrige bestemmelser i GDPR, som kun inddrages i det omfang, det er relevant.

Før der kan foretages en behandling af særlige kategorier af personoplysninger, skal der være hjemmel hertil i både art. 6 og 9 i GDPR. Bestemmelsen i art. 6 og dennes dertilhørende punkter vil dog ikke blive behandlet nærmere indgående, da specialet forudsætter, at når et indgreb vurderes efter art. 9, vil der allerede foreligge den nødvendige hjemmel hertil efter art. 6. Tilsvarende vil de supplerende bestemmelser i DBL behandles i det omfang, det er nødvendigt.

Derudover har specialet alene fokus på den situation, hvor den dataansvarlige indhenter samtykke direkte fra den registrerede til brug ved behandling af den registreredes personoplysninger, jf. GDPR art. 6, stk. 1, litra a, og art. 9, stk. 2, litra a. Dermed afgrænser specialet sig fra at behandle samtykke til videregivelse af personoplysninger til tredjemand.

Specialet vil tage udgangspunkt i behandlingen af private personers personoplysninger, hvorfor behandling af personoplysninger i forbindelse med ansættelsesforhold ikke vil blive inddraget i specialet.

Endvidere vil specialet ikke behandle de særlige betingelser, der gælder for børn i henhold til børns afgivne samtykke, jf. GDPR art. 8, stk. 1, stk. 1-3. Hvis barnet er under 16 år, er behandling kun lovlig, såfremt indehaveren af forældremyndigheden samtykker til behandlingen.

4. Metode

4.1 Retsdogmatisk metode

Dette speciale anvender den retsdogmatiske metode. Denne metode har fokus på de lege lata, dvs. gældende ret.[18]

Formålet med den retsdogmatiske metode er at beskrive, analysere og systematisere gældende retsregler inden for det relevante retsområde. Retsdogmatikkens undersøgelsesobjekt består af talrige kilder, og disse kilder varierer fra retsområde til retsområde.[19] I dette speciale vil metoden søges opfyldt ved anvendelse af diverse retskilder, herunder primært lovgivning og retspraksis, for at afdække, hvornår overvågning, der behandler biometriske data med det formål entydigt at identificere en fysisk person, kan legitimeres i henhold til Chartret og databeskyttelsesretten.

Dette gøres med udgangspunkt i EU Chartret samt GDPR, og som nationalt supplerende retsgrundlag anvendes Databeskyttelsesloven.

Den retsdogmatiske metode benyttes derfor for at fastlægge retstilstanden på specialets hovedområde. Ligeledes vil specialet indeholde en redegørelse af væsentlige begreber i databeskyttelsesretten. Ydermere vil projektet indeholde analyse og sammenligning af relevant praksis fra EU-medlemsstaterne og visse fortolkningsbidrag, herunder gennem GDPR's præambelbetragtninger samt retningslinjer fra det Europæiske Databeskyttelsesråd[20] (EDPB) og betænkning 1565/2017 for at kunne besvare problemformuleringen.

Ved anvendelse af den retsdogmatiske metode vil det være muligt at fastslå, hvornår overvågning, der behandler biometriske data med det formål entydigt at identificere en fysisk person, kan legitimeres i henhold til Chartret og databeskyttelsesretten.

4.2 Specialets anvendte retskilder

Kilderne til specialet er blevet fundet ved hjælp af Aalborg Bibliotekerne samt Aalborg Universitetsbibliotek. Ligeledes er der anvendt internetsøgemaskiner, kildefortegnelser fra

[18] Munk-Hansen, 2021, s. 91

[19] Munk-Hansen, 2022, s. 70 f & 211 f

[20] European Data Protection Board

litteraturen på lige fod med Generativ AI for at fremsøge relevante domme, afgørelser, betænkninger, retningslinjer og vejledninger. Disse er efterfølgende fundet på Retstidende, Karnov, Curia, Datatilsynets hjemmeside og GDPR-Hub.

4.2.1 Forordninger og love

Eftersom specialet tager udgangspunkt i, hvornår overvågning, der behandler biometriske data med det formål entydigt at identificere den registrerede, som udgør et indgreb, vil Chartret og GDPR udgøre de primære retskilder.

Chartret har forrang for national ret, hvis anvendelsen af den nationale ret er i strid med Chartret. National ret og anden EU-ret skal fortolkes i overensstemmelse med Chartret, hvilket betegnes som en fortolkning, der er konform med Chartret. Denne konforme fortolkning kan medføre, at Chartret har indirekte virkning i forholdet mellem private. Det er dog ikke Chartret i sig selv, der har virkning over for private, men derimod det relevante retsgrundlag, som er fortolket i lyset af Chartret, der har virkning over for private. Hvis denne fortolkningsvirkning holder sig inden for rammerne af almindelige fortolkningsprincipper, vil der ikke være nogen principiel problemstilling angående Chartrets virkning i national ret.[21]

Chartret kan efter omstændighederne have direkte virkning i forholdet mellem private, hvilket betegnes som horisontal virkning. Dette skyldes, at traktaterne efter fast praksis kan tillægges horisontal virkning, hvis traktatbestemmelserne er ubetingede og tilstrækkeligt præcise, idet borgere kan påberåbe deres individuelle rettigheder i medfør af primær EU-ret tillige i sager over for andre private.[22]

Da GDPR er en forordning, følger det af TEUF[23] art. 288, 1. og 2. pkt., at den er almengyldig samt bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat. GDPR gælder således, som den er vedtaget og fungerer som en lov i medlemsstaterne, hvorfor den ikke skal implementeres i national ret.[24] Dette modificeres dog i en lang række tilfælde i GDPR, da visse af dennes regler fastslår, at medlemsstaterne inden for nærmere afgrænsede områder enten kan eller skal fastsætte nationale regler.[25] Overordnet vil der tages udgangs-

[21] Christoffersen et al., 2018, s. 51
[22] Christoffersen et al., 2018, s. 52
[23] Traktaten om den Europæiske Unions funktionsmåde 2008/C 115/01
[24] Neergaard & Nielsen, 2024, s. 154 f
[25] Nielsen & Lotterup, 2025, s. 1023

punkt i DBL, når der skal anvendes et nationalt supplerende retsgrundlag for at kunne vurdere, hvornår overvågning der behandler biometriske data med det formål entydigt at identificere en fysisk person, kan legitimeres i henhold til Chartret og databeskyttelsesretten.

4.2.2 Domme og afgørelser

Retspraksis fra EUD udgør en central retskilde inden for databeskyttelsesretten som følge af EUD's position, der fortolker GDPR's bestemmelser.[26] I EU-retten er en af de helt centrale bestemmelser TEUF art. 267, som fastlægger, at EUD har kompetence til at afgøre præjudicielle spørgsmål om fortolkningen af traktaterne samt gyldigheden og fortolkningen af retsakter udstedt af Unionens institutioner, organer, kontorer eller agenturer.[27] Det følger af TEUF, art. 288, stk. 4, at retspraksis fra EUD er bindende i alle enkeltheder, som dommen er rettet imod, hvorfor EUD i sidste ende bestemmer, hvordan GDPR skal forstås og fortolkes ud fra de sager, der bliver forelagt til domstolsprøvelse.[28] Når EUD afsiger dom om gyldigheden eller fortolker retsakter, bliver deres afgørelser retsskabende og vil have en præjudikatværdi for fremtidige afgørelser.[29] Denne præjudikatværdi gør sig gældende ved, at EU-organer og medlemsstater må indrette deres praksis i overensstemmelse med dommens afgørelse. Retspraksis fra EUD bliver i specialet anvendt for at kunne fastlægge de lege lata.

Retspraksis fra nationale domstole er tillige en retskilde, idet de afgør konkrete retstvister og fastlægger, hvad der er gældende ret i den konkrete sag.[30] Databeskyttelsesretten kræver, ligesom andre retsregler, at disse får en nærmere udfyldning for at fastlægge regelforståelsen, hvorved der skabes en præjudicerende virkning for fremtiden.[31] Derfor vil retspraksis normalt udgøre en central retskilde for at fastlægge de lege lata, men indenfor databesyttelsesretten er det ikke tilfældet. I Danmark bliver tvister ofte afgjort af Datatilsynet, og det er kun sjældent, at de indbringes for de danske domstole.[32] Derfor kan specialet kun i meget begrænset omfang anvende national retspraksis, og gældende ret fastlægges på anden måde for at svare på problemformuleringen.

[26] Motzfeldt & Næser, 2025, s. 32 f
[27] Nielsen & Tvarnø, 2021, s. 136 & 138
[28] Blume, 2020, s. 68
[29] Nielsen & Tvarnø, 2021, s. 165 f
[30] Blume 2020, s. 45
[31] Blume, 2018, s. 45 f
[32] U.2023B.51, s. 53

Praksis fra de nationale tilsynsmyndigheder spiller en væsentlig rolle inden for databeskyttelsesretten, hvilket udgør en fravigelse fra udgangspunktet om at administrativ praksis ikke tillægges en sådan værdi.[33] Det følger af GDPR art. 51, stk. 2 og art. 57, stk. 1, litra g, at de enkelte medlemsstater skal udpege en eller flere tilsynsmyndigheder, og at disse skal samarbejde på tværs af medlemsstaterne. Det følger af DBL § 27, stk. 1, at Datatilsynet er udpeget til at have tilsynskompetence på alle områder inden for DBL's og GDPR's anvendelsesområde, som er underlagt den danske jurisdiktion og anden lovgivning, som ligger inden for GDPR's rammer for særregler om behandling af personoplysninger.[34]
Selvom der er enighed om, at anvendelsen af GDPR skal ske ensartet i alle medlemsstater, vil afgørelser fra andre medlemsstaters doms- og administrativ praksis ikke virke normativt i dansk ret, hvorfor andre medlemsstaters doms- og administrativ praksis ikke kan fastlægge regler, der bestemmer her i landet.[35]
Dette er dog ikke ensbetydende med, at de øvrige medlemsstaters doms- og administrative praksis ikke kan anvendes til at uddrage principper, grundsætninger og hensynsafvejninger for at finde frem til gældende databeskyttelsesret i tilfælde, hvor retsanvendelsen kræver et skøn eller en fortolkning[36].
I projektet vil der inddrages EU-domme, en dansk dom og administrativ praksis hovedsageligt fra Danmark, men der vil også inddrages administrativ praksis fra Sverige, Spanien og en dom fra Frankrig.

Det fremgår af betænkning 1565/2017[37], at GDPR i høj grad korrelerer med, hvad der fulgte af det tidligere databeskyttelsesdirektiv, som persondataloven[38] var baseret på.[39] Ligeledes er det blevet bekræftet i en række EU-domme, hvor domstolen udtaler: *Der foretages ikke en sondring mellem de bestemmelser [...], idet disse bestemmelser skal anses for at have et ens indhold* .[40] På baggrund af ovenstående vil fortolkningen af retspraksis fra før ikrafttrædelsen af GDPR i 2018, hvor tidligere databeskyttelsesdirektivet gjaldt, anses som

[33] Motzfeldt & Næser, 2025. s. 34
[34] Lovforslag L 68 FT 2017-18, s. 196
[35] Blume, 2018, s. 62 f
[36] U.2023B.51, s. 52
[37] Betænkning 1565/2017, s. 15
[38] Lov nr. 429 af 31/05/2000 om behandling af personoplysninger med senere ændringer - obs. historisk
[39] Lotterup & Nielsen, 2025, s. 160
[40] C-184/20 præmis 58 & C-460/20 præmis 79

retningsgivende for fortolkningen af GDPR, hvis bestemmelserne fra det dagældende direktiv er videreført i GDPR.[41]

4.2.3 Kilder, der bidrager til retskildefortolkninger

Besvarelsen af problemformuleringen bliver understøttet af motiverne for loven i form af diverse præambler og lovforarbejder med henblik på at klarlægge, hvad lovgivernes intention har været med lovgivningen.

Det fremgår af TEUF art. 296, 2. pkt., at alle retsakter skal have en begrundelse, hvorfor EU-retsakter har præambelbetragtninger, for at opfylde begrundelseskravet.[42] I specialet inddrages præambelbetragtninger fra GDPR, der har 173 præambelbetragtninger, og præambelbetragtninger fra AI Act, der har 180 præambelbetragtninger, som alle uddyber selve grundlaget for bestemmelsen. Derfor er det nødvendigt at afklare, hvilken betydning de har i forhold til specialet.[43]

EU-Domstolen fastslog i dommen C-215/88 *Casa Fleischhandels*[44] følgende om præambelbetragtninger:

> *En betragtning i en forordning kan være et vejledende moment ved fortolkningen af en retsregel, men kan ikke i sig selv være en retsregel.*[45]

Det kan derfor lægges til grund, at præambelbetragtninger udgør et væsentligt fortolkningsbidrag, der skal tages i betragtning, når enkelte bestemmelser skal forstås.[46] Derimod kan præambelbetragtninger ikke stå alene, og hvis det skulle ske, at den direkte er modstridende til en bestemmelse, vil bestemmelsen gå forud.[47]

Ved fortolkning af danske retsregler er det lovforarbejderne, der udgør baggrunden for, hvad lovgivers intention bag de enkelte retsregler har været.[48] Lovforarbejderne vil almindeligvis bygge på årelange analyser og lign. fra sagkyndige udvalg udmundet i betænkninger, med henblik på at klarlægge, hvad hensigten har været med lovgivningen.[49] I specialet

[41] Lotterup & Nielsen, 2025, s. 161
[42] U.2014B.293, s. 293 f
[43] Blume, 2020, s. 61 f
[44] Casa Fleischhandels, C-215/88, EU:C:1989:331
[45] Casa Fleischhandels, præmis 31
[46] Blume 2018, s. 61
[47] Blume, 2020, s. 62
[48] Blume 2020, s. 40
[49] Munk-Hansen, 2022, s. 317 f

vil det hovedsageligt være lovforarbejderne[50] fra databeskyttelsesloven, der bliver behandlet. Idet GDPR trådte i kraft i 2016 med virkning fra 2018, har der kun været 2 år til at gennemføre den nationale følgelovgivning, hvorfor det ikke har været muligt at nedsætte et sagkyndigt udvalg til at udarbejde en betænkning. Derimod blev betænkningen[51] udarbejdet af Justitsministeren med inddragelse af ekspertgrupper og ekstensiv bidrag fra Datatilsynet, hvortil der i forarbejderne bliver refereret til, især når der bliver redegjort for, hvordan de enkelte bestemmelser skal forestås.[52]
Motiverne for loven fungerer som fortolkningsmateriale, og modsat loven er disse ikke forpligtende.[53]

4.2.4 Retlige inspirationskilder

EU-retten anerkender, at EU's institutioner kan udgive ikke-bindende retstilkendegivelser i form af henstillinger og udtalelser, jf. TEUF art. 288. Henstillinger og udtalelser er ikke umiddelbart anvendelige i national ret, idet de ikke tillægger rettigheder til borgeren, som kan påberåbes i en stat. Derimod kan de anvendes som fortolkningsbidrag om, hvordan EU's institutioner fortolker bindende retstilkendegivelser, og kan udgøre forløbere for bindende regulering på området.[54]
I specialet inddrages retningslinjer, henstillinger og vejledninger fra EDPB. Formålet med EDPB's retningslinjer er at sikre ensartet anvendelse af GDPR i medlemsstaterne, jf. GDPR art. 70, stk. 1. EDPB's vejledninger vil udgøre ikke-bindende retstilkendegivelser, men deres vejledninger er bindende for de nationale tilsyn og vejledningerne kan bidrage til inspiration og forståelse af GDPR.[55]
Yderligere inddrages vejledninger fra Datatilsynet, som har til opgave bl.a. at sikre offentlighedens forståelse og kendskab til risici, regler, garantier og rettigheder i forbindelse med behandling samt fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til denne forordning, jf. GDPR art. 57, stk. 1 b og d.
Det fremgår af vejledning om administrative forskrifter[56], at vejledninger aldrig må indeholde bindende forskrifter. Det skal derimod anvendes til orienterende meddelelser om

[50] Lovforslag L 68 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven), Folketinget 2017-18, 25. oktober 2017
[51] Betænkning 1565/2017
[52] Blume, 2020, s. 41 f
[53] Evald, 2023, s. 37
[54] Munk-Hansen, 2022, s. 288 f.
[55] Motzfeldt & Næser, 2025 s. 24 f
[56] Vejledning nr. 9594 af 9. juli 2021 om administrative forskrifter, pkt. 1, 5.1 og 5.2.

f.eks. reglers praksis, fortolkning og indhold samt andre oplysninger, der kan have betydning for forståelsen af reglen og dens anvendelse. Men grundet den specielle stilling som Datatilsynets vejledninger har, og da retspraksis ofte indretter sig i overensstemmelse heraf, er der blandt forfattere uenighed om, hvorvidt de faktisk udgør en bindende retskilde.[57] Specialet vil ud fra et forvaltningsretligt synspunkt og i overensstemmelse med vejledning om administrative forskrifter tage udgangspunkt i, at Datatilsynets vejledninger, ligesom EDPBs vejledninger, udgør ikke-bindende retstilkendegivelser, hvorfor de ikke udgør en retskilde.[58]
Alligevel har vejledningerne i praksis en stor indflydelse, fordi de fleste dataansvarlige indretter sig efter dem. Ligeledes kan det med stor sikkerhed forventes, at en afgørelse fra tilsynsmyndighederne træffes i overensstemmelse med vejledningerne.[59] Grundet totalharmonisering, kan andre nationale tilsynsmyndigheders afgørelser anvendes i specialet, ligesom det er tilfældet med domme og administrative praksis.
Derfor er vejledningerne særlig relevante i specialet for at kunne fastlægge de lege lata.

Yderligere inddrages retslitteratur som fortolkningsbidrag, hvilket benyttes til at understøtte forståelsen for anvendelsen af retsregler. Retslitteratur har ikke en retlig legitimitet, hvorfor der tages højde for, at retslitteraturen ikke udgør en bindende retskilde.[60] Netop derfor bliver retslitteraturen i specialet udelukkende brugt som fortolkningsbidrag, for at skabe et større overblik for forståelse af retskilderne, men ikke til at fastlægge de lege lata.

4.2.5 Retskildefortolkning

Formålet med lovfortolkningen er at fastlægge, hvad der konkret er retsreglens udstrækning, og den har ikke andre formål end at kvalificere, hvilke tilfælde der er omfattet af retsreglen.[61] For at besvare problemformuleringen må relevante retskilder identificeres og derpå fortolkes for at fastlægge de lege lata. Idet GDPR og Chartret er omdrejningspunktet, vil udgangspunktet være en EU-retlig metode for retskildefortolkningen.
Når EUD skal fortolke retskilder, vil udgangspunktet være dens ordlyd. Ordlyden fremgår som en kombination alle dens sprogversioner, som skal betragtes ligestillet, hvilket blev

[57] Motzfeldt & Næser, 2025, s. 24, Blume 2020, s. 44. f, Udsen 2022, s. 50 f
[58] Udsen, 2022, s. 50 f
[59] Blume, 2020, s. 45 & 63 f
[60] Munk-Hansen, 2022, s. 289 f
[61] Munk Hansen, 2022, s. 305

fastslået i C-283/81 *CILFIT*[62].[63] Derudover skal der tages hensyn, og kun anvendes begreber fra EU-retten, fordi indholdet af begreberne ikke nødvendigvis er den samme som de nationale begreber.[64] Derudover vil der ved formålsfortolkning lægges særlig vægt på retskildens formålsbestemmelse og præambelbetragninger, hvorimod forarbejderne ikke kan tillægges samme betydning som f.eks. ved de danske forarbejder.[65] Endvidere udgør EU-retten et dynamisk retssystem, hvorfor EU-rettens udviklingstrin spiller en vigtig rolle ved fortolkning.[66] EUD anvender en dynamisk fortolkning, hvortil der anvendes en udviklings- og målsætningsorienteret fortolkningsstil, som tager udgangspunkt i fællesskabsrettens nuværende udviklingstrin.[67] Slutteligt er det et vigtigt princip i fortolkningen af EU-retlige kilder, at medlemsstaterne har pligt til at fortolke national ret i overensstemmelse med EU-retten. Det betyder, at hvis retspraksis udvikler sig på EU-plan, må praksis også udvikle sig nationalt. Dette begrænses dog af, at der ikke er pligt til at fortolke *contra legem.*[68]

[62] CILFIT, C-283/81, EU:C:1982:335, præmis 18-20
[63] Motzfeldt & Næser, 2025, s. 50
[64] Neergaard & Nielsen, 2024, s 174
[65] Motzfeldt & Næser, 2025, s. 50
[66] Neergaard & Nielsen, 2024, s 177
[67] Munk-Hansen, 2022, s. 325
[68] Hamer & Schaumburg-Müller 2020, s. 149 f

5. Overvågning af den registrerede

Overvågningen af den registrerede indledes allerede inden fødslen, hvor det som foster følges gennem hele graviditeten, hvilket efterfølges af en overvågning af, om borgeren følger det offentlige vaccinationsprogram. Senere i den registreredes liv vil tillige oplysninger om dennes årlige indkomst, arbejdssted, civilstatus osv., blive indsamlet af SKAT. Den registrerede vokser derfor op i et samfund, hvor det offentlige systematisk og omfattende indsamler data om denne, hvilket borgeren accepterer, og endda i visse tilfælde støtter, da det skaber muligheden for et mere sikkert samfund.[69]

I dette afsnit introduceres, hvordan retten til privatliv har fået større betydning gennem tiden, hvilket søges realiseret ved en historisk gennemgang af retten til privatliv. Dette gøres med henblik på at tydeliggøre at overvågning bestemt ikke er et nyt koncept. Dette bliver efterfulgt af Chartrets regulering af retten til privatliv og hvilke behandlinger, der kan legitimere et indgreb i retten til privatliv. Dernæst præsenteres mål af almen interesse, der har til formål at illustrere, hvornår der kan foreligge et mål af almen interesse. Til sidst vil samspillet mellem Chartret og GDPR blive beskrevet.

5.1 Et historisk perspektiv på retten til privatliv

Retten til privatliv er ikke et nyopstået fænomen. Dette princip kan med sikkerhed spores tilbage til det 19. århundrede, men det er dog ikke udelukket, at fænomenet som koncept har sit udspring i en tidligere del af historien.[70] Men princippet har fået en større signifikans i nutidens samfund i takt med den teknologiske udvikling, hvilket har medført en større frygt for overvågning for den enkelte borger.[71]

Under den kolde krig I Danmark opstod der i 1960'erne og 1970'erne en kraftig debat om etablering og anvendelse af registre, idet offentlige myndigheder og private virksomheder igangsatte behandling af personoplysninger ved hjælp af datamater[72]. Det var særligt mulighederne for at samkøre, registre og kontrollere den enkelte borgers adfærd på tværs af myndigheder, der gav anledning til bekymring, hvilket resulterede i nedsættelsen af Registerudvalget. Efterfølgende afgav Registerudvalget to delbetænkninger, der senere dannede grundlag for udarbejdelsen af lov om private registre og lov om offentlige myndigheders registre, de såkaldte registerlove.[73] Disse trådte i kraft i 1978 og havde til formål at

[69] Christensen, 2021, s. 42
[70] Trzaskowski, 2021, s. 37
[71] Blume, 2020, s. 33
[72] Datidens computere
[73] Motzfeldt & Næser, 2025, s. 17

regulere adgangen til at oprette registre samt behandlingen af oplysningerne heri, herunder videregivelse og samkøring af registre.[74]

Udenretligt var der også fokus på de stigende muligheder for databehandling, hvorfor OECD[75] darbejde det første internationale dokument vedrørende beskyttelse af personoplysninger *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* hvilket i 1980 blev vedtaget. Europarådet vedtog i 1981 det første retligt bindende internationale instrument inden for databeskyttelsen, som blev kaldt konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (Konvention 108).[76] Det er fastlagt i art. 1, at formålet har været at sikre:

> *The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy*

I EU blev det første Persondatadirektiv[77] vedtaget i 1995., hvilket medførte at persondataloven blev implementeret i dansk ret og i år 2000 afløste Registerlovene.[78] Behovet for at sikre en bedre beskyttelse af personoplysninger samt ønsket om at fremme mulighederne for øget digitalisering i Europa førte til et forslag til en databeskyttelsesreform, der blev fremsat af Kommissionen i 2012. Efter fire års forhandlinger blev GDPR vedtaget i 2016, hvorefter den fik virkning fra 25. maj 2018.[79]

Retten til privatliv kan, som nævnt tidligere, spores tilbage til det 19. århundrede, hvor Samuel Warren og Louis Brandeis argumenterede for, at en *right to be let alone* kunne blive etableret under common law systemet i USA. Baggrunden for dette var udviklingen i teknologi og forretning, hvor "øjeblikkelige billeder" og avisvirksomheder havde invaderet de hellige distrikter af privat- og nationalt liv.[80]

En anden vigtig udgivelse omkring privatlivet er Alan F. Westin's *Privacy and Freedom* fra 1967, hvori han argumenterede for, at overvågning var et essentielt middel for at kunne

[74] Motzfeldt & Næser, 2025, s. 17 f

[75] Organisation for Economic Co-operation and Development

[76] Trzaskowski, 2021, s. 39

[77] Persondatadirektivet: Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

[78] Motzfeldt & Næser, 2025, s. 17 f

[79] Motzfeldt & Næser, 2025, s. 20

[80] Trzaskowski, 2021, s. 37 f

udøve kontrol. Sidenhen har dette ført til flere kodificerede lovbestemmelser, hvilket inkluderer *The United Nations Universal Declaration of Human Rights* art. 12, som blev vedtaget i 1948, hvoraf følgende fremgår:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks.*[81]

I 1999 blev der truffet en beslutning om udarbejdelsen af Chartret, der havde til formål at tydeliggøre eksisterende grundlæggende rettigheder uden at tillægge dem yderligere retsvirkninger indenfor EU-retten, som trådte i kraft 2000. Chartret var dog ikke juridisk bindende for medlemsstaterne, den blev først juridisk bindende med Lissabon-traktatens ikrafttræden.[82] Siden d. 1. december 2009 har Chartret udgjort en del af EU's primærret og har samme rang i retskildehierarkiet som EU-traktaterne TEU[83] og TEUF.[84]

5.2 EU's Charter

Fortolkningen og anvendelsen af Chartret ved de nationale domstole følger EU rettens almindelige bestemmelser, herunder bestemmelserne om præjudiciel forelæggelse. EUD vil ikke fortolke national ret, da dette udelukkende påhviler de nationale domstole. Derimod kan præjudicielle spørgsmål om national rets fortolkning af EU-retten forelægges EU, hvis der er usikkerhed om fortolkningen af det EU-retlige spørgsmål. Nationale myndigheder har pligt til at respektere og anvende Chartret, når de gennemfører EU-retten.[85]

Retten til privat- og familieliv er forankret i Chartrets art. 7, hvilket tillige er fastsat i EMRK art. 8., men Chartret adskiller sig fra EMRK ved at have et overlap mellem privatlivsbeskyttelsen i art. 7 og beskyttelsen af personoplysninger i art. 8.[86]

Det følger af EU Chartret om grundlæggende rettigheders art. 7:

> *Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.*

Retten til og beskyttelsen af privatlivets fred er således en grundrettighed.[87] Heraf følger det, at enhver behandling af personoplysninger samt overvågning i princippet vil udgøre

[81] Trzaskowski, 2021, s. 38 f
[82] Christoffersen et al., 2018, s. 36 f
[83] Konsoliderede udgaver af traktaten om den Europæiske Union 2008/C 115/01
[84] Neergaard & Nielsen, 2024, s.143
[85] Ersbøll, 2016, s. 31
[86] Christoffersen et al., 2018 s. 126
[87] Trzaskowski et al., 2024, s. 36

et indgreb i denne grundlæggende rettighed.[88] Retten til privatliv er dog ikke en absolut rettighed, men såfremt et indgreb skal foretages, skal dette opfylde de fire kumulative betingelser i Chartrets art. 52, stk. 1.[89] Afsnit 5.3 og 5.4 vil gennemgå, hvordan disse betingelser gennemgås i praksis. Endvidere er der en nær sammenhæng mellem Chartrets art. 7 om retten til respekt og Chartrets art. 8 om beskyttelsen af personoplysninger. Når EUD skal behandle sager vedr. beskyttelse af personoplysninger, vil der oftest ske behandling af begge artikler.[90]

Chartrets art. 8 har følgende indhold:

> *Stk. 1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.*
>
> *Stk. 2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.*
>
> *Stk. 3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.*

Formålet med Chartrets art. 8 er at sikre en selvstændig beskyttelse af personoplysninger.[91] Chartret art. 8 er en kodificering af rettigheder, der fremgår forskellige steder i EU-retten, hvoraf de centrale bestemmelser findes i TEUF art. 16 og TEU art. 39. Det fremgår af disse bestemmelser, at Rådet kan fastsætte regler for behandling af personoplysninger. I forlængelse heraf gælder det, at Chartrets art. 8 skal udøves på de begrænsninger og med de betingelser, der er fastlagt i traktatbestemmelserne, jf. Chartrets art. 52, stk. 2. I forlængelse heraf gælder det, at begreberne "personoplysning" og "behandling" skal fortolkes i overensstemmelse med de sekundære retsakters begreber inden for databeskyttelsesretten.[92]

Chartrets art. 8 er ikke en absolut bestemmelse, da bestemmelsen skal ses i sammenhæng med dens funktion i samfundet.[93]

Chartrets art. 8, stk. 2, tillader, at behandling af personoplysninger kan foretages, forudsat at visse betingelser er opfyldt. Disse betingelser skal ses i nær sammenhæng med Chartrets

[88] Trzaskowski et al., 2024, s. 61
[89] Christensen, 2021, s. 155
[90] Christoffersen et al., 2018 s. 137 f
[91] Christoffersen et al., 2018, s. 136
[92] Christoffersen et al., 2018, s. 137
[93] Christoffersen et al., 2018, s. 139

art. 52, stk. 1, der foreskriver, at der kan foretages indgreb i Chartrets rettigheder på visse nærmere opregnede vilkår.[94]

Når EUD skal vurdere, om der er sket en begrænsning i den registreredes ret til privatliv, vil de vurdere, om betingelserne i undtagelsesbestemmelsen[95] er opfyldt. Chartrets art. 52, stk. 1., har følgende ordlyd:

> Stk. 1. *Enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved dette charter, skal være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.*

Det følger af bestemmelsen, at der kan foretages indskrænkninger i Chartrets bestemmelser, herunder bl.a. retten til privatliv og retten til beskyttelse af personoplysninger. En sådan indskrænkning skal dog opfylde de fire kumulative betingelser:[96]

1. Indgrebet skal have hjemmel i lov,
2. Respektere det væsentligste indhold af rettigheden,
3. Forfølge et mål af almen interesse, der er anerkendt af Unionen eller et behov for beskyttelse af andres rettigheder og friheder,
4. Indgrebet skal iagttage proportionalitetsprincippet.[97]

Det forudsættes, når et indgreb skal have hjemmel i lov, at bestemmelsen skal være af en vis kvalitet og være klar og præcis, så det er muligt at vurdere rækkevidden af et muligt indgreb. Ligeledes skal der fremgå en række mindstekrav, som regulerer rækkevidden af foranstaltningen.[98] Ligeledes skal indgrebet respektere det væsentligste indhold af rettigheden, hvilket forudsætter, at der ikke må ske et indgreb i det, der udgør kerneindholdet i selve grundrettighederne. Det er ikke muligt at lave en generel retningslinje herfor, men overordnet gælder det, at der ved indgrebet ikke må ske en alvorlig reducering af substansen af grundrettigheden.[99]

---

[94] Christoffersen et al., 2018, s. 139

[95] Undtagelsesbestemmelsen refererer til Chartretsart. 52, stk. 1., der fastslår de gældende betingelser for, at EU-institutionerne og medlemsstaterne kan foretage indgreb i de af Chartrets rettigheder, jf. Christoffersen et al, 2018, s. 570

[96] Retslitteraturen kalder det også de fire kumulative betingelser for den treleddet test

[97] Christoffersen et al., 2018, s. 570

[98] Hervey et al., 2014 s. 1473 f

[99] Christoffersen et al., 2018, s. 574

Når indgrebet skal forfølge et mål af almen interesse, der er anerkendt af Unionen, forudsættes det, at det er generelle interesser, som kan udledes af de generelle formål i TEU art. 2 og 3, samt andre interesser, der beskyttes af specifikke bestemmelser i traktaterne.[100] Nedenfor fremgår de generelle formål i TEU art. 2 og 3.

TEU Art 2 fastslår de værdier, som traktaten er bygget på:

> *Unionen bygger på værdierne respekt for den menneskelige værdighed, frihed, demokrati, ligestilling, retsstaten og respekt for menneskerettighederne, herunder rettigheder for personer, der tilhører mindretal. Dette er medlemsstaternes fælles værdigrundlag i et samfund præget af pluralisme, ikke-forskelsbehandling, tolerance, retfærdighed, solidaritet og ligestilling mellem kvinder og mænd.*

TEU art. 3 fastslår de gældende mål i henhold til traktaten:

> *1. Unionens mål er at fremme freden, sine værdier og befolkningernes velfærd.*
>
> *2. Unionen giver borgerne et område med frihed, sikkerhed og retfærdighed uden indre grænser, hvor der er fri bevægelighed for personer, kombineret med passende foranstaltninger vedrørende kontrol ved de ydre grænser, asyl, indvandring og forebyggelse og bekæmpelse af kriminalitet. [...]*
>
> *5. Unionen forsvarer og fremmer i forbindelserne med den øvrige verden sine værdier og interesser og bidrager til beskyttelsen af sine borgere. Den bidrager til fred, sikkerhed, bæredygtig udvikling af jorden, solidaritet og gensidig respekt folkene imellem,[...]og beskyttelse af menneskerettighederne, især børns rettigheder, samt nøje overholdelse og udvikling af folkeretten, herunder overholdelse af principperne i De Forenede Nationers pagt.*
>
> *6. Unionen forfølger sine mål med passende midler inden for de beføjelser, der er tildelt den i traktaterne.*

Ud fra de ovenstående traktatfæstede bestemmelser har mål af almene interesser, som er anerkendt af Unionen, et bredt anvendelsesområde. Ligeledes vil et behov for beskyttelse af andres rettigheder og friheder også opfylde betingelsen[101] At indgrebet skal iagttage proportionalitetsprincippet, forudsætter det at retsakten ikke må gå videre end, hvad der er passende og nødvendigt for at gennemføre det formål, der tilstræbes, og byrden ved indgrebet må ikke være uforholdsmæssigt i forhold til det tilsigtede mål.[102] Hvis indgrebet opfylder alle betingelser, vil der kunne ske et legitimt indgreb.

[100] Christoffersen et al., 2018, s. 575 f
[101] Christoffersen et al., 2018, s. 575 f
[102] Hervey et al., 2014 s. 1480 f

5.3 Den registreredes ret til beskyttelse af sit privatliv

Retten til respekt for privatlivet er en grundlæggende rettighed, og det er en central forudsætning for et moderne demokratisk samfund, da den enkelte registrerede skal kunne leve sit liv uden frygt for vilkårlig overvågning. Såfremt der består et ønske i at opretholde et samfund, hvor den registrerede kan bevæge sig frit, og hvor deres liv ikke er fuldstændig transparent, er det derfor nødvendigt med en begrænsning af adgangen til overvågning.[103] Overvågning er i dag et vidtrækkende fænomen og er således ikke blot begrænset til opstillede kameraer i stræder eller på veje, men kan også udmønte sig i oplagrede data, der skal verificere den pågældendes identitet, f.eks. for at få adgang til en bestemt ydelse.[104] Herved kan der opstå en frygt blandt de registrerede, om at deres data bliver lagret i store databaser, hvortil der ingen kontrol er over, hvem der har adgang til dem.[105]

Analysen af dommene i det følgende afsnit foretages med henblik på at fastslå, hvilke principper der gælder ved indgreb i retten til privatliv. Disse principper vil være relevante, når det skal vurderes, hvorvidt det kan legitimeres, at der foretages overvågning med det formål at behandle biometriske data til entydig identifikation.

Skepsis over nødvendigheden af statens adgang til ens personoplysninger, var netop en bekymring Schwarz havde, hvilket førte til en domstolsprøvelse i dommen *C-291/12, Schwarz*[106].

> Dommen omhandlede en registreret, Michael Schwarz, som havde ansøgt om at få udstedt et pas, men han bestred, at dette skulle ske under forudsætning af, at han skulle afgive sit fingeraftryk. Schwartz begrundede det med, at *Pasforordningen*[107], som havde til formål at beskytte mod svigagtig brug af pas, ville udgøre et uretmæssigt indgreb i hans ret til privatliv, fordi det var mere vidtgående end nødvendigt.
>
> EUD fastslog, at et fingeraftryk udgjorde en personoplysning og dermed et indgreb i retten til privatliv. EUD begrundede det med, at aftryk ville indeholde unikke oplysninger om fysiske personer, der ville gøre det muligt at identificere fysiske personer klart og tydeligt. Domstolen konkluderede, at kravet om fingeraftryk var pro-

[103] Bønsing et al., 2018, s. 29 f
[104] First Response Group (2024), s. 4f & 10 f
[105] Bertelsmann Foundation (2016), s. 86
[106] Schwarz, C-291/12, EU:C:2013:670
[107] Forordning (EF) nr. 2252/2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, som ændret ved Forordning (EF) nr. 444/2009

portionalt og ikke mere vidtgående, end hvad der var nødvendigt for at opfylde formålet, hvorfor Schwartz måtte acceptere det legitime indgreb i privatlivet, hvis han ønskede at få et pas.

Dommen viser, at der ikke kan foreligge et gyldigt samtykke som behandlingsgrundlag fra den registrerede til behandling af persondata, hvis behandlingen generelt er en nødvendighed for at kunne bruge den pågældende ydelse, som må anses som et alment behov, og hvortil der i realiteten ikke findes et alternativ.[108] Det forudsættes derfor, at der foreligger et andet behandlingsgrundlag, som skal være fastlagt ved lov, hvis behandlingen skal være legitim, jf. Chartrets art. 8, stk. 2. Hvis der sker et berettiget indgreb af retten til privatliv, følger det af Chartrets art. 52, stk. 1, at indgreb for det første skal være fastlagt i lovgivning, for det andet respektere Chartrets væsentligste indhold, for det tredje svare til mål af almen interesse, der er anerkendt af Unionen, eller det er et behov for beskyttelse af andres rettigheder og friheder og for det fjerde iagttage proportionalitetsprincippet om nødvendighed.[109] Herved ses det, at EUD ved vurderingen af, om indgrebet er omfattet af undtagelsesbestemmelsen i henhold til Chartrets art. 52, stk. 1, undersøger de fire kumulative betingelser.

Den første betingelse, der bliver undersøgt er, om indgrebet er fastlagt ved lov, hvilket er opfyldt, idet Pasforordningen fastlægger ved lov, at der er krav om biometrisk identifikation.[110] Dernæst skal indgrebet udgøre en almen interesse, hvilket i retslitteraturen ofte er angivet som hensyn til den nationale sikkerhed, bekæmpelse af terror og bekæmpelse af grov kriminalitet.[111] Dommen viser, at forebyggelse af forfalskning af pas og forhindre svigagtig brug heraf, som tilsammen tilsigter at forhindre ulovlig indrejse af personer på unionens område, også udgør mål af almene interesser.[112] For det tredje skal indgrebet respektere de af Chartret væsentligste rettigheders indhold, hvilket vurderes at være tilfældet i denne dom, da indgrebet kun forholder sig til det væsentligste og overordnet respekterer retten til privatliv.[113]

Slutteligt skal det vurderes, om indgrebet er proportionelt med hensyn til de mål der forfølges, hvorfor det skal vurderes om de midler, der er blevet iværksat, er egnede til at nå de forfulgte formål, og ikke er mere vidtgående end nødvendigt til at nå disse mål.[114] Hertil

[108] C-291/12, præmis 32
[109] C-291/12 præmis 34
[110] C-291/12 præmis 35
[111] Christoffersen et al., 2018, s. 576
[112] C-291/12, præmis 36-37
[113] C-291/12, præmis 39
[114] C-291/12, præmis 40

vurderer EUD, at lagringen medfører en forebyggelse for forfalskningen af pas, og at myndighedernes opgaver lettes ved denne lagring.[115] Derudover indgår det i proportionalitetsvurderingen, om der foreligger mindre indgribende alternativer. Det eneste alternativ, der vurderes at have samme virkning som fingeraftryk, er en IRIS-scanner. IRIS-scanneren vurderes dog at være et dyrt og lige så indgribende alternativ, hvorfor der ikke er tale om et mindre indgribende alternativ. I proportionalitetsvurderingen indgår også en vurdering af, hvordan de biometriske oplysninger opbevares. Oplysningerne skal lagres i en chip i passet, og passet bliver opbevaret af indehaveren, hvorfor det ikke er muligt at lave en central database til opbevaring, som ville føre til en større risiko for at der kan ske misbrug af data. Opbevaringen er derfor begrænset til, hvad der er nødvendigt for at kunne opnå formålet.[116] Det skal også vurderes om fejlagtige oplysninger, som skyldes forordningens bestemmelser, kan få vidtgående konsekvenser, og om der er truffet forebyggende foranstaltninger. EUD vurderer, at der ville kunne opstå scanningsfejl af fingeraftrykket, men disse fejl skal afhjælpes ved, at de kompetente myndigheder udfører en mere dybdegående kontrol for at fastslå den pågældendes identitet, hvorfor dette ikke medfører vidtgående konsekvenser.[117]

Det følger af det ovenstående, at EUD tillægger retten til privatliv stor betydning, og at behandling skal være proportionel.

I dommen *C-460/20, TU & RE*[118] tog EUD stilling til, om thumbnails (miniaturebilleder) udgjorde et større indgreb i retten til privatliv end tekst, og om disse miniaturebilleder derfor skulle fjernes fra resultaterne ved en billedsøgning fra internetsøgemaskinen.

> Der blev offentliggjort tre miniaturebilleder af TU & RE i artikler, der ifølge TU & RE indeholdt urigtige oplysninger om dem. TU & RE anmodede herefter internetsøgemaskinen og webstedudgiveren om at fjerne linkene til disse artikler, da de mente, at visse udsagn i artiklerne var urigtige. EUD konkluderede, at offentliggørelse af miniaturebilleder kunne have større indvirkning på den registrerede ret til privatliv end offentliggørelse af tekster.

EUD vurderer, at billeder uden supplerende tekstforklaring, som f.eks. miniaturebilleder, kan medføre et særligt alvorligt indgreb i den registreredes ret, fordi det er en persons image og udgør en af personlighedens vigtigste egenskaber, da det muliggør en adskillelse

[115] C-291/12, præmis 41
[116] C-291/12, præmis 60 & 62
[117] C-291/12, præmis 44
[118] TU og RE mod Google, C-460/20, EU:C:2022:962

af personen fra en forsamling af mennesker, og fotografierne ville kunne fortolkes på flere måde.[119] Resultatlisten fra billedsøgninger adskiller sig fra artikler, som både indeholder billeder og supplerende tekstforklaring, fordi resultatlisten kun indeholder miniaturebilleder. Grundet ovenstående vil en internetsøgning, hvor der kun vises miniaturebilleder, som vedrører den pågældende person, udgøre et særligt alvorligt indgreb i retten til privatliv.[120]
EUD konkluderer, at internetsøgemaskinens udbredelse af personoplysninger kan udgøre et mere alvorligt indgreb i den registreredes ret til privatliv, end webstedudgiverens offentliggørelse af selvsamme personoplysninger, hvorfor der skal foretages to forskellige rettigheds- og interesseafvejninger for, om indgrebet er legitimt.[121]
Det følger af ovenstående dom, at EUD, ved vurderingen af om der foreligger et alvorligt indgreb i retten til privatlivet, tillægger fotografier stor betydning, idet de afslører personers fysiske attributter. Dette kan resultere i en entydig identifikation af den pågældende, hvorfor der foreligger et særligt alvorligt indgreb. Der skal derfor tages hensyn til at beskytte den registreredes image, når fotografier behandles.[122]

Ud fra de ovenstående domme kan det konkluderes, at EUD, ved vurderingen af om en begrænsning i retten til privatliv indgreb er legitimt, vil inddrage undtagelsesbestemmelsen, der muliggør indgreb, såfremt det opfylder fire kumulative betingelser. Ligeledes er det ikke muligt at anvende samtykke som behandlingsgrundlag ved nødvendige ydelser, der må anses som almene behov, og hvortil der ikke foreligger alternativer. Derudover er der et krav om opbevaringsbegrænsning ved behandling af personoplysninger, så oplysningerne kun opbevares i det tidsrum, der er nødvendigt til opfyldelse af formålet, hvorfor der skal ske en løbende revurdering af gyldigheden.
Endvidere vil et offentliggjort fotografi med den registrerede udgøre et større indgreb i retten til privatliv, end hvis billedet vedkommende indgår i en offentliggjort tekst. Dermed bekræftes det, at fotografier har en særlig stilling inden for retten til privatliv, da de er uløseligt forbundet med den pågældende persons image.
Overordnet forudsætter ethvert indgreb i retten til privatliv, at indgrebet er proportionalt, men indgrebene har forskellige karakter, hvorfor der skal ske en rettigheds- og interesseafvejning for, om det enkelte indgreb er foreneligt med Chartret.

[119] C-460/20, præmis 95- 96, 100 & 106
[120] C-460/20, præmis 94
[121] C460/20, præmis 93 & 102
[122] C460/20, præmis 100

5.4 Mål af almen interesse i forhold til Chartret

I takt med at der sker en udvikling af kommunikationen og udveksling af oplysninger, grundet de digitale løsninger, er det blevet meget lettere at interagere med hinanden. Denne videreudvikling kan desværre også misbruges til planlægning af terrorisme og kriminalitet, fordi forbrydere lettere kan komme i kontakt med hinanden og benytte digitale platforme til udbredelsen.[123] Derfor opstår der et behov for forebyggelsen af disse handlinger, hvortil overvågning er et anvendt redskab, som får større og større aktualitet.[124] I forlængelse heraf kan der opstå en frygt for, at det skaber et overvågningssamfund og borgernes ret til ikke at blive overvåget krænkes.[125] Det bliver derfor en balancegang mellem overvågning begrundet i mål af almene interesser på den ene side, modsat retten til respekt for privatliv og kommunikation samt beskyttelsen af personoplysninger på den anden side.[126] Analysen af dommene i det følgende afsnit foretages med henblik på at fastslå, hvilke principper der gælder ved overvågning. Disse principper vil være relevante, når det skal vurderes, hvorvidt det kan legitimeres, at der foretages overvågning med det formål at behandle biometriske data til entydig identifikation.

EUD tog stilling til balancegangen mellem total overvågning og respekt for privatliv i *de forenede sager C-293/12 og C-594/12 Digital Rights Ireland*[127].

> Dommen handlede om, at Digital Rights Ireland m.fl. klagede over den massive overvågning af deres telefoner, der fandt sted på baggrund af indførelsen af logningsdirektiv[128]. Direktivet pålagde teleudbyderne at lagre alle trafik- og lokaliseringsdata vedrørende deres brugere. Formålet var, at det skulle hjælpe med bekæmpelsen af international terrorisme med henblik på opretholdelse af international fred og sikkerhed, hvilket var et legitimt formål i henhold til EU's almene interesser. Disse data skulle lagres i minimum seks måneder og maksimalt 24 måneder. De eneste data som ikke skulle opbevares, var opkald, der ikke havde opnået forbindelse til modtageren.

[123] Blume, 2018, 352
[124] Blume, 2018, 84
[125] Blume, 2018, s. 354
[126] Blume & Herrmann, 2018, s. 281
[127] Digital Rights Ireland m.fl., de forenede sager C-293/12 og C-594/12, EU:C:2014:238
[128] Direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF

> Domstolen konkluderede derfor, at selvom direktivet forfulgte et sagligt formål i henhold til EU's almene interesser, så var direktivet for vidtgående og medførte en følelse af konstant overvågning hos borgeren, og der manglede klare og præcise bestemmelser for rækkevidden af indgrebet i retten til privatliv. Derfor var direktivet ugyldigt, fordi den havde overskredet de grænser, som undtagelsesbestemmelsen krævede henset til Chartret.

Ud fra ovenstående dom kan det konkluderes, at selvom der foreligger et anerkendt legitimt formål med at behandle personoplysninger, så skal det stadig overholde Chartrets undtagelsesbestemmelse. EUD fastslår, at det ved afgørelsen af, om der foreligger et indgreb i retten til privatliv, er uden betydning om indgrebet har medført eventuelle ubehageligheder for den registrerede.[129] Indgrebet vurderes af EUD til at være meget vidtrækkende og af særlig alvorlig karakter, idet den registrerede ikke er oplyst om lagringen og den efterfølgende anvendelse af vedkommendes personoplysninger. Dette egner sig til at skabe en følelse af konstant overvågning af den registreredes privatliv.[130]

Som fastlagt i *Schwarz*[131], indebærer undtagelsesbestemmelsen indledningsvist, at der skal foreligge en lovhjemmel, før indgrebet kan foretages, hvilket i dette tilfælde er direktivet. Indgreb skal yderligere forfølge et mål af almen interesse, der er anerkendt af Unionen, hvilket er opfyldt i denne dom, da bekæmpelse af international terrorisme udgør en sådan almen interesse.[132] Yderligere skal indgrebet respektere det væsentligste indhold af rettighederne i henhold til Chartret, som i det konkrete tilfælde er Chartrets art. 7 og 8. EUD fastslår, at direktivet udgør et særligt alvorligt indgreb, men idet det ikke giver adgang til indholdet af de elektroniske kommunikationer, respekterer direktivet de rettigheder, der følger af Chartrets art. 7.[133] Ligeledes vil Chartrets art. 8 væsentligste indhold respekteres, da direktivet fastslår, at dette skal respektere principperne for databeskyttelse og datasikkerhed.[134] Slutteligt skal det vurderes, om indgrebet iagttager proportionalitetsprincippet, dvs. er begrænset til det strengt nødvendige.[135] I denne vurdering indgår bl.a., hvor mange personer der har adgang til de pågældende data, eller om de lagrede data er undergivet en forudgående myndighedskontrol, hvilket direktivet tillige ikke fastlægger som forpligtelser for medlemsstaterne.[136] Derudover er varigheden af lagringen af data udslagsgivende,

[129] Digital Rights Ireland, præmis 33
[130] Digital Rights Ireland, præmis 37
[131] Schwarz, C-291/12, EU:C:2013:670
[132] Digital Rights Ireland, præmis 42
[133] Digital Rights Ireland, præmis 39
[134] Digital Rights Ireland, præmis 40
[135] Digital Rights Ireland, præmis 52
[136] Digital Rights Ireland, præmis 62

da direktivet fastsætter varigheden som værende mellem 6 og 24 måneder, uden at der foretages en sondring af relevansen af de lagrede data, samtidigt med at lagringens tidsrum ikke er betinget af nødvendighed.[137]

Grundet manglen af tilstrækkelige garantier, som sikrer en effektiv beskyttelse af den registreredes ret til privatliv, overskrider direktivet de grænser, som undtagelsesbestemmelsen kræver, og direktivet udgør derfor et uretmæssigt indgreb i retten til privatliv.[138] Modsat følger det af dommen, at der kan foretages et gyldigt indgreb, hvis de fire kumulative betingelser i undtagelsesbestemmelsen er opfyldt, selvom det kan skabe en følelse af konstant overvågning.

Som konsekvens af afsigelsen af *Digital Rights Ireland* og ugyldigheden af logningsdirektivet 2006/24, bliver fokusset øget ift. i hvilken grad medlemsstaterne har mulighed for at logge data.[139] I modsætning til Digital Rights Ireland, hvor den principielle tvist vedrørte gyldigheden af direktivet, forholdt det sig anderledes i de forenede sager *C-203/15 & C-698/15, Tele2 Sverige*[140]. Spørgsmålet var, hvorvidt national lovgivning kunne tillade generel og udifferentieret overvågning via logning, eller om sådanne ordninger, ligesom logningsdirektivet, måtte anses for at være i strid med EU Charter of Fundamental Rights.[141]

> Dommen handlede om en national logningslov i Sverige med hjemmel i ePrivacy-direktivet[142], der pålagde teleudbydere at foretage udifferentieret lagring, herunder tele- og lokaliseringsdata. Sveriges justitsminister havde efter *Digital Rights Ireland* fået udarbejdet en rapport, der konkluderede at logningsloven ikke var i strid med principperne udledt af Digital Rights Ireland, hvorimod teleudbyderen Tele2 var af modsat overbevisning. Formålet med lovgivningerne var at bekæmpe grov kriminalitet, hvortil den registreredes adfærd gennem logning blev overvåget. Lovgivningen foreskrev, at der skete logning af alle, selv hvis der ikke forelå indicier for, at der var begået noget kriminelt. Dataene omfattede kommunikationsdatoen, klokkeslæt, navn og adresse på den registrerede bruger eller abonnenten etc. Sammenhængen af disse data ville derfor gøre det muligt at gøre sig bekendt med, hvil-

[137] Digital Rights Ireland, præmis 64

[138] Digital Rights Ireland, præmis 69

[139] Blume 2018, s. 143

[140] Tele2 Sverige m.fl., de forenede sager C-203/15 og C-698/15, EU:C:2016:970

[141] Christensen 2021, s. 170f

[142] Direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved direktiv 2009/136/EF, art. 15, stk. 1

ket kommunikationsmiddel der var blevet brugt, tidspunktet for beskeden og hvorfra kommunikationen var foregået. EUD konkluderede, at undtagelsesbestemmelsen i Chartret var til hinder for en national lovgivning, der gav adgang til en generel og udifferentieret lagring af data, samtidigt med at logningen af dataene ikke var begrænset til grov kriminalitet.

Det fremgår af de ovenstående domme, at et indgreb foretaget i den registreredes ret til privatliv, kan legitimeres i henhold til Chartrets undtagelsesbestemmelse, såfremt fire kumulative betingelser er opfyldt. ePrivacy-direktivet fastslår, at nationale retsforskrifter, der fraviger princippet om fortrolighed af kommunikation og tilhørende trafikdata, kun kan vedtages, når dette er begrundet i hensyn til den nationale sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem. Disse hensyn er udtømmende, hvorfor medlemsstaterne ikke kan vedtage forskrifter af andre hensyn end dem, der fremgår af direktivet. Herved ses det, at indgrebet skal henføres til et af de lovfastsatte hensyn. EUD foretager derfor en prøvelse af, om undtagelsesbestemmelsen er opfyldt, da det nationalt supplerende retsgrundlag skal fremgå i et af de udtømmende hensyn i direktivet.[143]

Dernæst kan det udledes af dommen, at det er muligt for medlemslandene, i henhold til direktivet at fastsætte legitime indgreb i retten til privatliv i national lovgivning, hvis dette sker med henblik på bekæmpelse af kriminalitet, eller hvis indgrebet forfølger et lignende mål af almen interesse, som er anerkendt af EU.[144]

Ved at kombinere logningsdata vil det gøres muligt, at der kan drages konklusioner om de registreredes privatliv, herunder deres vaner i hverdagen, opholdssteder, kontaktpersoner, anvendte IP-adresser osv. Ligeledes omfatter det også tredjemand, som kommunikerer med den registrerede.[145] Uagtet lovgivningen ikke tillader lagring af indholdet af en elektronisk kommunikation, og derfor ikke udgør en krænkelse, kan lagringen af trafik- og lokaliseringsdata alligevel påvirke brugernes brug af deres elektronisk midler, hvorfor der foreligger et indgreb.[146] I forlængelse heraf udgør et sådant indgreb, hvis den registrerede

[143] Tele2 Sverige, præmis 90 & 115
[144] Tele2 Sverige, præmis 103
[145] Tele2 Sverige, præmis 98
[146] Tele2 Sverige, præmis 101

ikke bliver informeret om lagringen, et særligt alvorligt indgreb og er egnet til at skabe en følelse af, at deres privatliv konstant bliver overvåget.[147]
Imidlertid anerkender EUD, at et sådant indgreb alligevel kan være retmæssigt, når det sker for at bekæmpe grov kriminalitet. Derimod betyder det, at kriminalitet, der ikke er omfattet af grov kriminalitet, ikke kan legitimere et sådant indgreb.[148] Selvom indgreb kan være retmæssige af hensyn til terror- og kriminalitetsbekæmpelse, kan en generel og udifferentieret logning ikke anses for nødvendig hertil.[149]
Ligeledes fortolker EUD, at direktivet sammenholdt med Chartrets art. 7, 8 samt art. 52, stk. 1 er til hinder for, at der kan laves en national lov, hvis den ikke indeholder begrænsninger for overvågningen. Endvidere skal der være adgang til en forudgående kontrol foretaget af en domstol eller af en uafhængig administrativ myndighed, samtidig med at der stilles krav om, at de pågældende data lagres på EU's område.[150]
På baggrund af dommen kan det lægges til grund, at masseovervågning som udgangspunkt vil være i strid med Chartret. Modsætningsvist følger det af dommen, at et mål af almen interesse muliggør, at der foretages målrettet overvågning i overensstemmelse med Chartret.

I medfør af de afsagte EU-domme opstod der et spørgsmål, om den danske logningsbekendtgørelse[151] var i overensstemmelse eller ugyldig efter EU-retten. Højesteret behandlede i sagen UfR.2022.2162 H, om retsudviklingen havde medført, at den danske bekendtgørelse var i strid med EU-retten.

> Ligesom i de ovenstående EU-domme, erklærede den danske højesteret sig enig i, at logningen skulle være proportionel og ikke måtte ske vilkårligt. Begge parter i sagen var enige om, at dele af logningsbekendtgørelsen var uforenelig med EU-retten. Derimod var der uenighed, om dette ville medføre, at hele bekendtgørelsen var ugyldig, eller blot ugyldighed for de retsregler, der var uforenelig med EU-retten, hvorfor de ikke måtte finde anvendelse. Højesteret udtalte følgende:
> *Som anført [...] indebærer medlemsstaternes EU-retlige loyalitetsforpligtelse og princippet om EU-rettens forrang, at danske domstole skal undlade at anvende regler i*

[147] Tele2 Sverige, præmis 100
[148] Tele2 Sverige, præmis 102
[149] Tele2 Sverige, præmis 103
[150] Tele2 Sverige, præmis 125
[151] Bekendtgørelse nr. 988 af 28. september 2006

> *national ret, i det omfang dette ville være i strid med umiddelbart anvendelige EU-regler.*

Det kan således lægges til grund, at selvom dele af logningsbekendtgørelsen var i strid med EU-retten, ville der ved konkret domstolsprøvelse tages højde for retsudviklingen, grundet den EU-retlige loyalitetsforpligtelse og EU-rettens forrang. Derved sikres harmonisering af EU-retten blandt medlemsstaterne, selvom den nationale lovgivning ikke altid kan følge med retsudviklingen. Ligeledes betyder det også, at tilsynsmyndighederne skal iagttage retsudviklingen inden for EU-retten, grundet forrangsprincippet og det gælder generelt, at national retspraksis har høj præjudikatsvirkning inden for forvaltningsretten.[152] Den ovenstående dom er derfor med til at udtrykke EU-rettens forrangsprincip, hvis en national lov er i uoverensstemmelse med EU-retten.

På baggrund af dommen *Digital Rights* og *Tele2 Sverige*, kan det virke til, at der eksisterer et totalt forbud mod udlevering af logningsdata, medmindre sagen omhandler grov kriminalitet, eller hvis indgrebet udgør et mål af almen interesse. EUD valgte i dommen *C-207/18 Ministerio Fiscal*[153] at fastlægge, hvornår der alligevel kan ske udlevering af data, selvom forholdet ikke opfylder kravene fra de ovenstående domme.

> Hernández Sierra fik stjålet sin telefon og tegnebog. I forbindelse med efterforskningen anmodede myndighederne om at få adgang til dataene for at kunne opklare forbrydelsen. Forbryderen valgte at aktivere den stjålne telefon med et SIM-kort, hvorfor myndigheden anmodede om at få identificeret indehaveren og få oplysninger om dennes efternavn, fornavn og evt. adresse.
>
> EUD konkluderede, at ePrivacy-direktivet udtømmende regulerede til hvilket formål national lovgivning kunne give myndigheder adgang til data, der blev lagret af teleudbydere. Samtidig forudsatte det en afvejning om, hvor vidtgående indgrebet var i forhold til retten til privatliv, ved udlevering af data sammenholdt med den strafbare handling. Dataene fra sagen, herunder navn og adresse, var ikke af en sådan karakter, at indgrebet kunne kategoriseres som et alvorligt indgreb i retten til privatliv, hvorfor adgangen til at foretage indgreb ikke skulle begrænses i medfør af Chartret. Derimod ville oplysninger om kommunikations- og lokationsdata have været for vidtgående i forhold til den strafbare handling.

[152] Bønsing, 2023, s 48f & 60

[153] Ministerio Fiscal, C-207/18, EU:C:2018:788

Fordi strafsanktionen for den konkrete forbrydelse efter spansk lovgivning ikke er omfattet af grov kriminalitet og grundet præcedens fra *Digital Rights Ireland* og *Tele2 Sverige*, har den tidligere antagelse været, at myndighederne ikke kan få udleveret data om den registrerede, der har begået en almindelig strafbar handling.[154] Dommen fastslår, at offentlige myndigheder kan få adgang til dataene, hvis den registrerede har begået en forbrydelse, uagtet om der ikke foreligger grov kriminalitet, såfremt det ikke er muligt at drage præcise slutninger om vedkommendes privatliv.[155] I forlængelse heraf kræves det altid ved et indgreb, at der foreligger udtømmende klare og præcise retsregler, der angiver under hvilke formål myndighederne kan få dataene udleveret, og den pågældende lovgivning skal afveje alvoren i indgreb sammenlagt med hvilke data, der kan behandles.[156] I det konkrete tilfælde tillader ePrivacy-direktivet udtømmende, at de formål, der muliggør behandling udgøres af efterforskning, afsløring eller retsforfølgning af overtrædelser i den nationale straffelov, hvis behandlingen af dataene er proportional i forhold til indgrebet.[157]

Der behøves således ikke foreligge grov kriminalitet, før der legitimt kan foretages et indgreb i borgerens ret til privatliv, men det kræver fortsat, at indgrebet skal opfylde de fire kumulative betingelser, hvor der skal sondres mellem, hvilken form for data der udleveres ift. den strafbare handling.[158] Hvis der foreligger en almindelig strafbar handling, kræver indgrebet, at de omhandlende data kvalificeres som værende af ikke-alvorlig karakter, før myndighederne kan få adgang til dataene. Myndighederne vil først kunne foretage et alvorligt indgreb i retten til privatliv, hvis der foreligger grov kriminalitet.[159]

EUD vurderer, at indgreb, hvor der sker udlevering af efternavn, fornavn og evt. adresse, ikke udgør et alvorligt indgreb, idet der ikke kan drages præcise slutninger om vedkommendes privatliv. Derimod vil indgrebet være alvorligt, hvis dataene omfatter lokations- og kommunikationsdata, herunder hyppigheden og placeringen, hvorfra der er kommunikeret med visse personer i en bestemt periode.[160]

Endelig kan det udledes af dommen, at Chartrets art. 7 og 8 ikke skal være til hinder for at forebygge, efterforske, afsløre eller retsforfølge forbrydere, men indgreb skal begrænses til det strengt nødvendige, og muligheden for indgreb skal stadfæstes tilstrækkelig klart i

[154] Ministerio Fiscal, præmis 21-25
[155] Ministerio Fiscal, præmis 60-61
[156] Ministerio Fiscal, præmis 52
[157] Ministerio Fiscal, præmis 59-61
[158] Ministerio Fiscal, præmis 51
[159] Ministerio Fiscal, præmis 61
[160] Ministerio Fiscal, præmis 60 & 63

loven. Chartret har til formål at beskytte den registrerede mod vilkårlig overvågning, hvorfor ethvert indgreb skal opfylde de fire kumulative betingelser.

Som tidligere gennemgået er der i medfør af *Tele2 Sverige* indført et forbud mod total masselagring af trafik- og lokationsdata. Lagring af data i større omfang kan kun finde sted, hvis det er begrænset til det strengt nødvendige, dvs. afgrænset ift. område og/eller personer og udgør et mål af almen interesse. I *de forenede sager C-511/18, C-512/18 & C-520/18 La Quadrature Du Net* [161] anerkendte EUD, at der kunne foretages en målrettet masselagring af trafik- og lokationsdata, hvis dette var begrundet i hensyn til den nationale sikkerhed.

> En fransk datanetværksforening, La Quadrature Du Net, ønskede en annullering af de dekreter, der muliggjorde, at der kunne foretages en masselagring af de registreredes data, hvis dette var begrundet i national sikkerhed. Dette blev begrundet med, at de pågældende dekreter bl.a. tilsidesatte retten til privatliv. Lovgivningerne ville omfatte alle elektroniske kommunikationsmidler samt oplysninger på de registrerede, der anvendte disse midler, og dette uden at indføre en form for undtagelse. De lagrede data udgjorde kommunikationskilden, kommunikationsdatoen, telefonnummer og IP adresse. Indholdet af selve kommunikationen var dog ikke omfattet. EUD konkretiserede de hensyn, der ville udgøre et mål af almen interesse, og efterfølgende konkluderede de, at art. 52, stk. 1., sammenholdt med art. 7 og 8 var til hinder for lovgivningsmæssige foranstaltninger, der foreskriver generel og udifferentieret logning af trafik- og lokaliseringsdata. Derimod kunne teleudbydere blive påbudt at foretage generel og udifferentieret logning i en begrænset periode, hvis medlemsstaten stod overfor en trussel mod den nationale sikkerhed.

Dommen starter indledningsvis med, at EUD anfører et obiter dictum af omstændigheder, der udgør mål af almen interesse, som kan legitimere indgreb i retten til privatliv. De oplistede interesser udgør, ikke udtømmende, bekæmpelse af terrorisme, bekæmpelse af børnepornografi, strafferetlig efterforskning, bekæmpelse af grov kriminalitet, beskyttelsen af den nationale sikkerhed. Fælles for disse interesser er, at de skal bidrage til beskyttelsen af andres rettigheder og friheder.[162]

Efterfølgende kan det udledes af dommen, at EUD vurderer, hvorvidt de fire kumulative betingelser i henhold til Chartrets art. 52, stk. 1., er opfyldt for at indgrebet kan legitimeres.

[161] La Quadrature du Net m.fl., de forenede sager C-511/18, C-512/18 og C-520/18, EU:C:2020:791.
[162] La Quadrature Du Net, præmis 76, 122

Indledningsvist skal det fastslås, at den hjemmel, som har til formål at regulere udtømmende, hvornår indgrebet kan finde sted. I det konkrete tilfælde udspringer hjemlen af ePrivacy-direktivet, som fastlægger, hvornår der kan ske målrettet logning af trafik- og lokationsdata[163] Derudover skal indgrebet respektere de af Chartrets væsentligste rettigheder, hvilket vurderes af EUD til at være opfyldt, idet indgrebet er målrettet bekæmpelse af grov kriminalitet, og dette skal ikke hindre de forebyggende foranstaltninger.[164] Selvom de enkelte oplysninger ikke i sig selv er udslagsgivende, vil en sammenkobling af selvsamme oplysninger medføre, at oplysningerne udgør et indgreb i retten til privatliv. EUD vurderer, at sammenkoblingen af trafik- og lokaliseringsdata kan afsløre en række forhold om de registreredes privatliv, som er lige så følsomme som selve indholdet af kommunikationen, hvis der sker en sammenkobling af f.eks. opholdssteder, vaner i dagligdagen, færden i sociale miljøer osv., fordi disse data gør det muligt at skabe en profil af den registreredes privatliv.[165]

Den tredje betingelse forudsætter, at indgrebet forfølger et mål af almen interesse, som er anerkendt af unionen, hvilket i dette scenarie er bekæmpelse af grov kriminalitet, forebyggelse af alvorlige indgreb mod den nationale sikkerhed og beskyttelse af den nationale sikkerhed.[166] EUD bedømmer, hvorvidt beskyttelse af den nationale sikkerhed vejer tungere end andre formål, der udgør mål af almene interesser, grundet TEU art. 4, stk. 2. Derfor kan den nationale sikkerhed begrunde foranstaltninger, der indebærer indgreb i retten til privatliv, som er mere alvorlige end dem, som disse andre formål kan begrunde, forudsat at de øvrige krav i Chartret art. 52, stk. 1 er opfyldt.[167]

Som den fjerde betingelse i undtagelsesbestemmelsen, skal indgrebet være begrænset til det strengt nødvendige, hvilket inkluderer en lovgivning bundet i national ret, der angiver, hvornår en foranstaltning kan vedtages, der har til formål at behandle personoplysninger.[168] I nødvendighedskravet indgår bl.a., hvor lang tid det pågældende indgreb vil vare ved, eller under hvilke forudsætninger det vil finde sted, da dette ikke må overstige et forudsigeligt tidsrum. I forlængelse heraf må indgrebet ikke have en systematisk karakter.[169] Det skal sandsynliggøres, at der foreligger tilstrækkeligt konkrete omstændigheder for, at medlemsstaten står over for en alvorlig trussel mod den nationale sikkerhed. Truslen skal

[163] La Quadrature Du Net, præmis 141
[164] La Quadrature Du Net, præmis 121 & 146
[165] La Quadrature Du Net, præmis 117
[166] La Quadrature Du Net, præmis 146
[167] La Quadrature Du Net, præmis 136
[168] La Quadrature Du Net, præmis 132
[169] La Quadrature Du Net, præmis 138

anses for at være reel og aktuel eller forudsigelig, og tidsmæssigt skal indgrebet være begrænset til det strengt nødvendige, men med mulighed for forlængelse. Indgrebet skal være underlagt strenge garantier mod misbrug af oplysningerne samt indgrebet skal kunne gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed.[170] Derimod vil en lovgivning, der foreskriver generel og udifferentieret lagring, der foretages med henblik på bekæmpelse af kriminalitet, overskride det strengt nødvendige.[171] I modsætning hertil vil indgrebet fortsat være foreneligt med Chartret, hvis logning er begrænset til et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, hvor der formodes at grov kriminalitet er indblandet .[172] Det geografiske område kan baseres på objektive og ikke-diskriminerende grundlag, som f.eks. de områder hvor der bliver begået et højt niveau af grov kriminalitet samt områder hvor der foreligger en formodning herfor. Derudover vil områder, der besøges af et stort antal personer eller strategiske steder, såsom lufthavne og/eller banegårde[173] tillige opfylde dette kriterium.

Hvis der foretages lagring af dataene, er det vigtigt at der foreligger lovbestemte frister for, hvornår disse data skal slettes eller anonymiseres.[174] Fristerne kan dog overskrides, hvis det er nødvendigt for at opklare strafbare handlinger eller angreb mod den nationale sikkerhed, såvel som i den situation hvor sådanne angreb er konstateret eller hvor der foreligger rimelig grund til at mistænke, at der er begået sådanne strafbare handlinger eller angreb.[175]

Indsamling af data i realtid, som muliggør lokalisering af terminaludstyr, vil udgøre et særligt alvorligt indgreb. Da oplysningerne er af følsom karakter, skal der sondres mellem den adgang, der sker i realtid og den adgang, der ikke sker i realtid. Førstnævnte vil være mere indgribende i retten til privatliv, idet den gør det muligt at foretage en næsten fuldstændig overvågning af de registrerede.[176] Realtidsovervågning kan dog tillades, når denne er begrænset til personer, der med rimelig grund mistænkes for at være involveret i terrorvirksomhed, og er underlagt en forudgående prøvelse, der foretages af en domstol eller uafhængig administrativ enhed, så indsamling i realtid kun tillades i overensstemmelse med, hvad der er strengt nødvendigt.[177]

---

[170] La Quadrature Du Net, præmis 137-139
[171] La Quadrature Du Net, præmis 141
[172] La Quadrature Du Net, præmis 144
[173] La Quadrature Du Net, præmis 150
[174] La Quadrature Du Net, præmis 160
[175] La Quadrature Du Net, præmis 161
[176] La Quadrature Du Net, præmis 187
[177] La Quadrature Du Net, præmis 192

Det kan på baggrund af ovenstående retspraksis udledes, at retten til privatliv vægtes højt, men indgreb kan dog finde sted, såfremt det opfylder de fire kumulative betingelser i undtagelsesbestemmelsen, jf. Chartrets art. 52, stk. 1. Selvom et indgreb således forfølger et mål af almen interesse, som er anerkendt af Unionen, kan indgrebet kendes ugyldigt, hvis det ikke er begrænset til det strengt nødvendige, hvori bl.a. indgår, om indgrebet er undergivet en forudgående myndighedskontrol, hvor mange personer, der har adgang til de pågældende data og det tidsmæssige aspekt af indgrebet. Derudover vil der være forbud mod et indgreb, der foretager overvågning af alle registreredes data, medmindre dette er begrundet i hensyn til den nationale sikkerhed.
Ligeledes vil et vidtgående indgreb i den registreredes ret til privatliv forudsætte, at der foreligger grov kriminalitet, men hvis der foreligger en almindelig strafbar handling, kræver indgrebet, at de omhandlede data kvalificeres som værende af ikke-alvorlig karakter i henhold til retten til privatliv.
Indgreb, der foretages med henblik på overvågning, kan derfor foretages, hvis de fire kumulative betingelser i undtagelsesbestemmelsen er opfyldt, herunder hvis mål af almen interesse overstiger hensynet til retten til privatliv. Herved ses det, at retten til beskyttelse af personoplysninger, som skal ses i sammenhæng med retten til privatliv, ikke er en absolut rettighed, da denne, i henhold til proportionalitetsprincippet, skal ses i sammenhæng med sin funktion i samfundet samt afvejes i forhold til andre grundlæggende rettigheder, jf. GDPR-præambel 4, 2., pkt.

5.5 Samspillet mellem EU's Charter og GDPR

Formålet med GDPR er at fastsætte regler, der skal beskytte fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger, jf. GDPR art. 1, stk. 1. Derudover har GDPR til formål at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, især beskyttelse af personoplysninger, jf. GDPR art. 1, stk. 2. Dette præciseres i GDPR-præambelbetragtning nr. 1, hvoraf det følger, at behandling af personoplysninger forudsætter en beskyttelse af fysiske personer, da der er tale om en grundlæggende rettighed. Rettigheden følger af Chartrets art. 8, stk. 1, og i traktaten om Den Europæiske Unions funktionsmåde (TEUF) art. 16, stk. 1, som fastslår, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. Det følger af GDPR-præambel 4, 2. pkt., at rettigheden ikke er en absolut ret, da denne i overensstemmelse med proportionalitetsprincippet, skal ses i sammenhæng med sin funktion i samfundet, og afvejes i forhold til andre grundlæggende rettigheder.

I GDPR-præambel 4, 3. pkt., fastsættes det, at GDPR overholder alle de grundlæggende rettigheder og følger de principper, der er fastlagt i Chartret, især retten til privatliv og familieliv samt beskyttelsen af personoplysninger.
Chartret udgør en del af primærretten, hvorimod GDPR, som er en forordning, vil indgå i den bindende sekundærregulering. Bindende sekundærregulering afleder deres ret fra primærretten.[178] Det følger af TEU art. 6, stk. 1 og Chartret art. 51, stk. 1, at retsakter inden for EU-retten skal respektere grundlæggende rettigheder og almindelige retsprincipper også kaldt *gyldighedsbetingelsen*, før retsakten er gyldig.[179] Derfor udgør Chartret fortsat en af de øverste retskilder, og hverken nationale regler eller sekundærregulering, heriblandt GDPR, må være i strid med bestemmelserne i Chartret indenfor EU-retten. Når EUD behandler persondataretlige spørgsmål, tillægger de fortsat Chartret en styrende betydning ved stillingtagen af spørgsmålet.[180]

6. Databeskyttelsesretten

Retten til privatliv er vigtig både for demokratiet og individets selvbestemmelse. Der skal eksistere en balance mellem ensomhed og kammeratskab, hvortil begge er nødvendige for demokratiets udvikling og individuel handleevne. Privatliv kan forstås ud fra et socio-politisk, psykologisk, historisk samt et evolutionært perspektiv, mens lovgivning ikke alene kan forklare privatliv, da det kun reflekterer de foretagne politiske beslutninger. Dette medfører dog ikke, at databeskyttelsesretten er uden betydning.[181]
I dette afsnit bliver Databeskyttelsesretten introduceret, hvilket inkluderer en uddybning af anvendelsesområdet. Derefter gives der en introduktion til de overordnede principper, der skal iagttages, når GDPR finder anvendelse, da disse principper altid skal iagttages, uanset hvilket behandlingsgrundlag, der er anvendt ved behandlingen af personoplysninger. Dette efterfølges af hvilke behandlingsgrundlag, der er relevante i forhold til behandling af biometriske data til entydig identifikation.

[178] Neergaard & Nielsen, 2024, s. 135
[179] Neergaard & Nielsen, 2024, s. 212
[180] Blume, 2018, s. 60
[181] Trzaskowski, 2021, s. 37

6.1 Anvendelsesområde

Databeskyttelsesretten finder anvendelse på behandling af personoplysninger, der foretages som led i aktiviteter, der udføres for en dataansvarlig eller databehandler, der er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej, jf. GDPR art. 3, stk. 1.

Det følger af GDPR art. 3, stk. 2, litra b, at Databeskyttelsesretten finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i unionen, hvis behandlingsaktiviteten bl.a. vedrører overvågning af registreredes adfærd, når deres adfærd finder sted i Unionen.[182] Uagtet den dataansvarlige eller databehandlerens lokation, finder databeskyttelsesretten anvendelse, når blot behandlingen har konsekvenser i EU (lex loci solutionis).[183]

Databeskyttelsens materielle anvendelsesområde følger af GDPR art. 2, stk. 1, hvoraf det fremgår, at GDPR finder anvendelse ved behandling af personoplysninger, der helt eller delvis iværksættes ved hjælp af automatisk databehandling, samt behandling af personoplysninger, der ikke foretages ved hjælp af automatisk databehandling, men som indgår i et register eller er bestemt til at indgå i et register.[184] I henhold til forståelsen af et register, er dette enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, uagtet om samlingen er centraliseret, decentraliseret eller opdelt efter funktionelle eller geografiske forhold.[185] Anvendelsesområdet kan begrænses i medfør af GDPR art. 2, stk. 2, såfremt behandlingsaktiviteten er opremset i GDPR art. 2, litra a-d, som er udtømmende.[186] I dette speciale vil ikke alle undtagelserne blive behandlet, men alene de for specialet mest relevante, herunder art. 2, stk. 2, litra c.

GDPR Art. 2, stk. 2., litra c indskrænker anvendelsesområdet for GDPR, hvis der er tale om behandling af personoplysninger foretaget af en fysisk person som led i rent personlige eller familiemæssige aktiviteter, også kaldet privatlivsundtagelsen.[187]

Bestemmelsen sigter således på de tilfælde, hvor behandlingen f.eks. består i privat korrespondance samt føring af adressefortegnelse over familie, venner og bekendte.[188]

[182] Nielsen & Lotterup, 2025, s. 230
[183] Nielsen & Lotterup, 2025, s. 235
[184] Trzaskowski, 2021, s. 42
[185] Trzaskowski & Sørensen, 2022, s. 67
[186] Nielsen & Lotterup, 2025, s. 218
[187] Nielsen & Lotterup, 2025, s. 221 f
[188] Nielsen & Lotterup, 2025, s. 221

I dommen *C-212/13 Ryneš*[189] tager EUD stilling til rækkevidden af privatlivsundtagelsen ved overvågning foretaget af private. Heraf følger det, at privatlivsundtagelsen er underlagt en streng fortolkning, da beskyttelsen af de registreredes grundlæggende rettigheder vægter højt.[190] Grundet det snævrere anvendelsesområde, vil overvågning, såfremt den dækker et offentligt område, om end kun delvist, udgøre en behandling af personoplysninger, fordi det ikke kan anses for at udgøre en rent personlig eller familiemæssig aktivitet at overvåge et offentligt område[191] Derfor vil behandlingen være underlagt de databeskyttelsesretlige krav om proportionalitet og nødvendighed. GDPR og DBL vil derfor ikke finde anvendelse for privatpersoner, der foretager overvågning, der i henhold til deres beskaffenhed alene er at kategorisere som *rent privat*.

6.2 Grundprincipperne

Databeskyttelsesrettens væsentligste principper fremgår af GDPR art. 5, der
skal iagttages i forbindelse med behandling af personoplysninger. art. 5 giver derfor ikke et selvstændigt retligt grundlag for, at der kan foretages en bestemt behandling af oplysninger, idet behandling forudsætter hjemmel hertil i enten art. 6 eller 9, eller i databeskyttelseslovens § 7, stk. 4.[192]

Art. 5 har til hensigt at skabe en balancegang mellem den registreredes ret til beskyttelse af sine personoplysninger på den ene side, og hvordan andre kan behandle den registreredes personoplysninger på en ansvarlig måde på den anden side.[193]

I det følgende vil alene de for specialet relevante bestemmelser blive oplistet, hvorfor ikke alle grundprincipperne bliver behandlet. Specialet fokuserer på art. 5, stk. 1, litra c, d og e, idet disse vurderes mest relevante for besvarelsen af problemformuleringen.

Det første relevante grundprincip er ***dataminimering***, jf. GDPR art. 5, stk. 1, litra c., hvoraf det følger, at en behandling af personoplysninger, som finder sted, skal være tilstrækkelig, relevant samt begrænset til, hvad der betinges af de behandlede formåls nødvendighed. Kravet om nødvendighed i behandlingen af personoplysninger afspejler således et proportionalitetsprincip.[194]

Det andet relevante grundprincip er ***rigtighed***, jf. GDPR art. 5, stk. 1, litra d, hvoraf det følger, at personoplysninger skal være korrekte, og såfremt det er nødvendigt, skal de være

[189] Ryneš C-212/13, EU:C:2014:2427
[190] Ryneš, præmis 29
[191] Ryneš, præmis 33
[192] Nielsen & Lotterup, 2025, s. 323
[193] Jakobsen et al., 2021, s. 27
[194] Nielsen & Lotterup, 2025, s. 340

ajourførte; ethvert passende skridt skal foretages for at garantere, at personoplysninger, der er fejlagtige i henhold til deres forudsatte behandlingsformål, straks skal slettes eller korrigeres.

Det tredje relevante grundprincip er ***opbevaringsbegrænsning***, jf. GDPR art. 5, stk. 1, litra e, hvoraf det følger, at personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

Kravet om begrænsning i opbevaring af personoplysninger forhindrer, at der sker en unødvendig ophobning af data.[195]

I dommen *C-131/12, Google Spain*[196] forholder EUD sig til, om retten til at blive glemt udgør en del af retten til privatliv. Selvom oplysninger, der fremgår om den pågældende person på internettet, er af ældre dato, kan behandlingen af personoplysninger dog stadig udgøre et alvorligt indgreb, hvis oplysningerne stilles til rådighed for den brede offentlighed, hvorfor der skal sondres mellem, hvor oplysningerne er tilgængelige.[197] Den registrerede har ret til at oplysningerne bliver slettet eller skjult, hvis oplysningerne påvirker denne negativt. Dette er undtaget i tilfælde, hvis tungtvejende hensyn begrunder det modsatte, f.eks. hvis informationen har stor samfundsmæssig relevans.[198] Oplysningerne skal glemmes, hvis de f.eks. er utilstrækkelige, irrelevante eller ikke længere er nødvendige i forhold til behandlingens formål og den tid, der er gået.[199] Der skal derfor ske en opbevaringsbegrænsning for at forhindre, at oplysningerne kommer den registrerede til skade. EUD understreger, at retten til privatliv som udgangspunkt går forud for offentliggørelse af personoplysninger, der er begrundet i enten økonomiske eller offentlige interesser. Offentlige interesser kan dog overstige retten til privatliv, hvis det godtgøres, at offentligheden skal have adgang til informationen. Derimod kan økonomiske interesser, der alene har et kommercielt formål, aldrig kunne godtgøre et alvorligt indgreb i retten til privatliv, men vil altid kræve understøttelse af andre interesser.[200]

[195] Nielsen & Lotterup, 2025, s. 350
[196] Google Spain og Google, C-131/12, EU:C:2014:317
[197] C-131/12, præmis 80
[198] C-131/12, præmis 81
[199] C-131/12, præmis 93
[200] C-131/12, præmis 97

6.3 Behandling af personoplysninger

Definitionen af behandlingen af personoplysninger er fastsat i GDPR art. 4, nr. 2. Definitionen er central, idet behandlingsbegrebet anvendes til at fastlægge GDPR's anvendelsesområde, jf. art. 2, stk. 1.

Forståelsen af hvad der udgør en behandling, følger de hidtidige definitioner i databeskyttelsesdirektivet, hvorfor Datatilsynets forhenværende praksis fortsat kan indgå som essentielle fortolkningsbidrag. Begrebet omfatter ikke blot registrering, opbevaring, videregivelse og samkøring af oplysninger, men tillige enhver form for håndtering af oplysninger.[201]

Derudover indeholder GDPR art. 4, nr. 2 en ikke udtømmende liste af eksempler på, hvad der udgør behandling af personoplysninger, herunder indsamling af personoplysninger. Anonymisering vil ikke være omfattet af begrebet, da formålet er at sikre, at der ikke sker en behandling af personoplysninger, som er omfattet af GDPR's anvendelsesområde.[202] Når der sker en indsamling af personoplysninger, vil dette være omfattet af definitionen af behandling, uanset lagringstiden, hvorfor tillige en midlertidig eller kortvarig lagring af personoplysninger vil være omfattet.[203] EDPB har præciseret, at et system der er online uafbrudt, og har til opgave at regulere adgang til faciliteterne, altid foretager en behandling af personoplysninger i det øjeblik indsamlingen sker. Behandlingen vil derfor ikke være betinget af varigheden, hvorfor det ikke er udslagsgivende at behandlingen har en ganske kortvarig karakter og sletning af et ikke-match sker øjeblikkeligt.[204]

Det følger af databeskyttelseslovens § 2, stk. 4, at uanset behandlingsformen, vil databeskyttelsesloven og GDPR gælde i forbindelse med TV-overvågning, hvorved der indgår oplysninger om en identificeret eller identificerbar fysisk person i form af billede og lyd.[205]

For at der kan foretages en behandling af personoplysning, forudsætter det, at der foreligger et behandlingsgrundlag, GDPR art. 6, stk. 1., fastslår de generelle betingelser herfor. Bestemmelsen gælder som udgangspunkt for enhver behandling af personoplysninger, som er omfattet af GDPR's anvendelsesområde.[206]

[201] Nielsen & Lotterup, 2025, s. 259
[202] Blume, 2018, s. 371 f
[203] Nielsen & Lotterup, 2025, s. 260
[204] EDPB's Retningslinjer 03/2019, afsnit 5.1: DT j. nr. 2021-431-0145, Afsnit 3.4
[205] Nielsen & Lotterup, 2025, s. 263
[206] Nielsen & Lotterup, 2025, s. 360

6.4 Behandlingsgrundlag

Det følger af Chartrets art. 8, stk. 2, at behandling af personoplysninger skal behandles rimeligt, i overensstemmelse med de angivne formål og i forlængelse heraf skal der til behandlingen enten indhentes samtykke, eller også skal behandlingen være berettiget ud fra et andet ved lov fastsat grundlag. Dette konkretiseres i GDPR præambelbetragtning 40, hvoraf det fremgår, at førend behandling af personoplysninger kan anses for lovlig, bør behandling enten være baseret på den registreredes samtykke, eller et andet legitimt grundlag fastlagt i enten GDPR, EU-retten eller medlemsstaternes nationale lovgivning.
Behandlingsgrundlaget for behandling af almindelige personoplysninger, som fremgår af bestemmelserne i GDPR art. 6, kan legitimeres, fordi de tilvejebringer de af Chartrets krævede grundlag for behandling af personoplysninger.[207] Hvis der er tale om særlige kategorier af personoplysninger, herunder biometriske data med det formål entydigt at identificere en fysisk person, vil behandlingen indebære en forøget risiko hos den registrerede, hvorfor GDPR art. 6 alene ikke vil udgøre den fornødne hjemmel.[208] Behandlingsgrundlag, der fremgår af GDPR art. 6, tilvejebringer ikke de af Chartrets krævede grundlag for behandling af særligt indgribende personoplysninger.[209]
I dette tilfælde forudsættes det, at der eksisterer både et behandlingsgrundlag efter art. 6, samtidigt med at en af undtagelsesbestemmelserne i art. 9, stk. 2, litra a-j finder anvendelse.[210]
Behandling af biometriske data med det formål entydigt at identificere en fysisk person er anført i GDPR art, 9, stk. 1, hvorfor det udgør kategori af særlige personoplysninger.
Når det er fastslået, at der sker en behandling i en særlig kategori af personoplysninger, skal behandlingen overholde både principperne, der fremgår af GDPR art. 5 for behandling af personoplysninger, og samtidigt have hjemmel til behandling i både GDPR art. 6 og 9.[211]
I specialet forudsættes det, at hvis behandlingsgrundlaget for behandling af biometriske data med det formål entydigt at identificere en fysisk person er opfyldt i medfør af GDPR art. 9, stk. 2, vil et af behandlingsgrundlagene efter GDPR art. 6, stk. 1 også være opfyldt. Derfor vil specialet ikke gå i dybere analyse med de generelle behandlingsgrundlag efter GDPR art. 6, stk. 1. GDPR art. 9 og dens indhold vil blive uddybet nærmere i afsnit 7.3.

[207] Motzfeldt & Næser, 2025, s. 165
[208] Knobel & Udsen, 2025, s. 160
[209] EDPB's Retningslinjer 05/2022, præmis 42-44: Motzfeldt & Næser, 2025, s. 165f
[210] Motzfeldt & Næser, 2025, s. 130
[211] Motzfeldt & Næser, 2025, s. 130

7. Biometriske data

Menneskelige biometriske karakteristika, hvoraf omfattet er fingeraftryk, stemme, ansigt osv., konstituerer særpræg, der er tilstrækkelige til at kunne identificere et individ.[212] Ansigtsgenkendelse medfører, at det menneskelige ansigt fungerer som en QR-kode, hvorefter den registrerede, ved scanning af dennes ansigt, vil kunne anvende dette til at identificere sig med. Dette kan anvendes til at adgangsregulere, hvem der får adgang til et sted, hvormed det er muligt at forebygge utryghedsskabende adfærd, men ansigtsgenkendelse bevirker også, at der sker overvågning, der kan identificere den registrerede, hvorfor spørgsmålet bliver, hvor grænsen går mellem retten til privatliv og og de tryghedsskabende foranstaltninger.[213]

I dette afsnit bliver biometriske data introduceret, hvilket inkluderer en uddybning af hvilke personoplysninger der udgør biometriske data og under hvilket behandlingsgrundlag oplysningerne kan behandles. Dernæst vil forskellen på identifikation og verifikation og blive introduceret. Dette vil blive efterfulgt af de behandlingsgrundlag, der i henhold til GDPR kan legitimere en behandling af biometriske data. Herefter vil praksis vedrørende disse behandlingsgrundlag blive gennemgået i henholdsvis afsnit 8 og 9.

7.1 Hvad er biometriske data

De af GDPR's forgængere, herunder databeskyttelsesdirektivet og persondataloven definerede ikke eksplicit begrebet "biometriske data", hvorfor det blev betragtet som almindelige persondata. Dette blev først præciseret ved indførelsen af GDPR, som oplister biometriske data som værende særlige kategorier af personoplysninger, idet det muliggør en entydig personidentifikation.[214]

Legaldefinitionen af hvad der udgør biometriske data fremgår af GDPR art. 4, nr. 14:

> *»biometriske data«: personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger*

[212] Jasserand, 2022, s. 295
[213] Samvirke April 2026 s. 42
[214] Nielsen & Lotterup, 2025, s. 315

For at supplere forståelsen for, hvad der udgør biometriske data, kan AI Act[215] anvendes. Det er fastslået i AI Act præambel 14, at begrebet i denne forordning skal fortolkes i overensstemmelse med definitionerne i GDPR, hvorfor der er sammenfald mellem begreberne. AI Act benyttes derfor til at præcisere, hvordan overvågningssystemer kan anvende biometriske data til at muliggøre autentifikation, identifikation eller kategorisering af fysiske personer og genkendelse af fysiske personers følelser.

EDPB har præciseret en række specifikke tekniske fremgangsmåder, hvorved det er muligt at identificere en fysisk person. Det fremgår af EDPB Guidelines 05/2022[216], at biometriske processer for entydig identifikation kan inddeles i to kategorier, henholdsvis i identifikation og verifikation. Begreberne "biometrisk identifikation" og "biometrisk verifikation" er nu blevet kodificeret i henholdsvis AI Act art. 3, nr. 35 og 36.
Derfor er forståelsen for hvilke biometriske processer, der kan anvendes til entydig identifikation sammenfaldende mellem GDPR art. 4, nr. 14 og AI Act, art 3, nr. 34, men der er sket en indskrænkning af definitionen, idet følgende ikke længere er omfattet: *muliggør eller bekræfter en entydig identifikation af vedkommende*. Dette er begrundet i, at identifikationen er opdelt i to forskellige biometriske processer, henholdsvis biometrisk identifikation og -verifikation, jf. AI Act 3, nr. 35 og 36.
Biometriske data udgør enhver personoplysning, der behandles ved hjælp af en specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika, hvilket f.eks. omfatter fingeraftryk, ansigtsbilleder og menneskelige træk, der udledes af deres fysiske, fysiologiske, adfærdsmæssige eller psykologiske egenskaber. Disse karakteristika udgør biometriske data, idet de muliggør eller bekræfter en entydig identifikation af personen.[217]

For at forhindre, at ethvert af de ovenstående eksempler vil udgøre en behandling af biometrisk data, præciserer GDPR præambelbetragtning nr. 51, 2. Pkt., hvornår behandling af personoplysninger udgør biometriske data. Først når der sker behandling ved en specifik teknisk fremgangsmåde, der har til hensigt at entydigt identificere eller verificere en fysisk person, vil det være omfattet af den særlige kategori af personoplysninger, jf. GDPR art. 9,

[215] Forordning (EU) 2024/1689 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens)
[216] EDPB Retningslinjer 05/2022 og EDPB Udtalelse 11/2024
[217] EDPB Retningslinjer 05/2022, præmis 7

stk. 1. Derfor vil f.eks. behandlingen af et fotografi ikke udgøre en særlig kategori af personoplysninger, medmindre behandlingen foretages med henblik på at identificere eller verificere den fysiske person.

7.2 Identifikation og verifikation

Som anført i ovenstående afsnit deles de biometriske processer op i henholdsvis biometrisk identifikation og -verifikation. Når biometriske data behandles med det formål entydigt at identificere en fysisk person, oprettes der en biometrisk skabelon, som udgør en repræsentation af ens tydelige biometriske træk. Denne skabelon formodes at være entydig og unik for den registrerede og gør det muligt at sammenligne skabelonen med andre skabeloner, der tidligere er blevet produceret. Processen kan derfor deles op i to trin: oprettelse af en skabelon, efterfulgt af sammenligning af skabelonerne.[218] Begge processer anvender genkendelsesteknikker, som er baseret på et estimeret match mellem den skabelon, der udarbejdes med en eller flere skabeloner, der er lagret. Hvis denne sammenligning overstiger en fastsat tærskel, vil systemet antage, at der foreligger et match.[219]

Forskellen ligger i, hvordan sammenlægningsprocessen behandles i henholdsvis biometrisk verifikation og -identifikation.[220] Forskellen på de to forskellige biometriske processer fremgår af AI Act -art. 3, nr. 35 og 36.

Når biometriske data behandles med det formål at verificere gælder følgende:

> AI Act -art. 3, nr. 36 beskriver verifikation som værende følgende: *»biometrisk verifikation«: automatiseret, en-til-en-verifikation, herunder autentificering, af fysiske personers identitet ved at sammenligne deres biometriske data med tidligere afgivne biometriske data*.

Dette stemmer overens med EDPB's forståelse af biometrisk verifikation, som har til formål at bekræfte en biometrisk påstand gennem sammenligning. Systemet sammenligner en på forhånd registreret skabelon med en enkelt nyoprettet skabelon. Denne funktion består derfor i at sammenligne to skabeloner med hinanden, hvorfor det kaldes 1:1-verifikation.[221]

Når biometriske data behandles med det formål at identificere gælder følgende:

> AI Act -art. 3, nr. 35 beskriver identifikation som værende følgende: *»biometrisk identifikation«: automatiseret genkendelse af fysiske, fysiologiske, adfærdsmæssige*

[218] EDPB retningslinjer 05/2022, præmis 9
[219] EDPB retningslinjer 05/2022, præmis 11
[220] EDPB udtalelse 11/2024, præmis 21
[221] EDPB retningslinjer 05/2022, præmis 10

> *eller psykologiske menneskelige træk med henblik på at fastslå en fysisk persons identitet ved at sammenligne den pågældende persons biometriske data med biometriske data om enkeltpersoner lagret i en database*.

Dette stemmer overens med EDPB's forståelse af biometrisk identifikation, som har til formål at søge i en database med biometriske skabeloner for at returnere, om der foreligger et match, der kan tilskrives en enkelt person. Denne funktion er således afhængig af at kunne sammenligne skabelonen med en bestående database, der indeholder referenceskabeloner. Denne funktion består i at sammenligne mange skabeloner, hvorfor det kaldes 1:mange-identifikation.[222]

Der har tidligere hersket uvished om der sker en behandling af særlig kategorier af personoplysninger ved verifikation. Bl.a. har Datatilsynet i tidligere afgørelser[223] haft den opfattelse, at verifikation ikke ville være underlagt GDPR art. 9, stk. 1, fordi det ikke sker med det formål entydigt at identificere en fysisk person. I Spanien har det Spanske Datatilsyn (AEPD) netop fastlagt i en afgørelse[224], om behandlingen af biometrisk verifikation var omfattet af den særlige kategori af personoplysninger. Her fastslog AEPD, at verifikation, der har til formål at identificere en fysisk person, altid vil være omfattet af den særlige kategori af personoplysninger, jf. GDPR art. 9, stk. 1. Dette stemmer også overens med den seneste udtalelse[225] og guideline[226] fra EDPB.
EU-retten er et dynamisk retssystem, hvilket medfører at der hele tiden sker en udvikling af retten.[227] Idet Datatilsynets afgørelser er fra henholdsvis 2018 og 2019, hvorimod AEPD-afgørelsen er fra 2023, vil det ikke nødvendigvis betyde, at Datatilsynets fortolkning har været forkert, men måske har det stemt overens med den daværende opfattelse af *de lege lata*. En afgørelse der er afsagt i 2019, vil derfor nødvendigvis længere være retvisende for en afgørelse om samme problemstilling afsagt i 2026, selvom der ikke er indført nye lovbestemmelser på området, kan der derimod være sket en ændring inden for rammerne af beføjelsen.

Fordi sammenligningsprocessen i de to biometriske processer foregår på forskellige måder, er det relevant at vurdere, om det ene system er mere indgribende i retten til privatliv,

[222] EDPB retningslinjer 05/2022, præmis 10
[223] DT j.nr. 2019-31-1650, kap. 31: DT j.nr. 2018-211-0135, kap 3.2
[224] GDPRhub AEPD (Spain) - EXP202305134
[225] EDPB udtalelse 11/2024, præmis 21
[226] EDPB retningslinjer 05/2022, præmis 12
[227] Neergaard & Nielsen, 2024. s. 177

end det andet. I *Schwarz*[228] fastslår EUD, at opbevaringen af de biometriske data spiller en betydelig rolle, for at vurdere, om indgrebet i retten til privatliv er nødvendigt.[229] I vurderingen af hvilke risici der er forbundet med opbevaring af biometriske data, er der forskel på, om opbevaringen sker i en database eller om det sker decentralt hos den registrerede selv.[230] Den decentrale opbevaring er med til at sikre, at dataene kun behandles med henblik på at opfylde formålet, og mindsker samtidig risikoen for uautoriseret adgang til oplysningerne.[231] I forlængelse heraf har EDPB vurderet, at anvendelsen af store centrale databaser til identifikation kan få alvorlige konsekvenser for den registrerede, hvis der f.eks. sker uautoriseret adgang til databaserne, hvorfor den risikofyldte opbevaringen udgør et alvorligt indgreb i retten til privatliv[232] Derimod vil anvendelsen af skabeloner til verifikation, der kun er lagret hos den enkelte, under visse omstændigheder indebære færre risici, hvis den lokale opbevaring ledsages af de fornødne garantier[233], hvorved alvoren af indgrebet mindskes sammenlignet med den centrale lagring.[234]

Ud fra *Schwarz*[235] kan det udledes, at under visse forudsætninger, vil en verifikation udgøre et mindre indgreb i retten til privatliv end identifikation. Ved vurderingen af om der kan foretages overvågning med biometrisk data, bør det vurderes, om formålet kan opnås ved at anvende verifikation frem for identifikation.

7.3 Behandlingsgrundlaget for biometriske data

Behandling af biometriske data er, som den eneste af de særlige kategorier af personoplysninger, underlagt et specifikt formålskrav. Forbuddet i GDPR art. 9, stk. 1, finder således kun anvendelse, såfremt de biometriske oplysninger behandles med henblik på entydig identifikation af en person. Modsætningsvis betyder det, at hvis behandlingen af biometriske data sker til et andet formål, skal behandlingsgrundlaget kun have hjemmel i GDPR art. 6.

Et eksempel på hvor der sker en behandling af biometriske data, men hvor formålet ikke er entydig identifikation, fremgår af Datatilsynets sag *Alexandra Institut*[236].

---

228 Schwartz, C-291/12, EU:C:2013:670
229 Schwartz, præmis 63
230 Schwartz, præmis 59-60
231 Schwartz, præmis 56-57
232 EDPB udtalelse 11/2024, præmis 63
233 Se hertil afsnittet om *A.2 Registreredes rettigheder og garantier, der kan gennemføres af dataansvarlige* i EDPB udtalelse 11/2024
234 EDPB udtalelse 11/2024, præmis 40
235 Schwartz, C-291/12, EU:C:2013:670
236 DT j.nr. 2023-211-0004

> Datatilsynet vurderede i denne sag, at lydfiler med optegnede stemmer udgjorde biometriske data. Idet stemmer udgøres af unikke talemønstre såsom tonehøjde, rytme, udtalelse, sprog og dialekt, ville det være muligt at identificere en persons identitet på baggrund af ens stemme. Formålet med behandlingen var ikke at identificere stemmerne, men derimod at udvikle og forbedre dansk tale-teknologi, som skal bruges til at genkende dansk tale og læse dansk tekst højt. Det specifikke formålskrav var således ikke opfyldt, hvorfor behandlingen af personoplysninger kun skal have hjemmel efter GDPR art. 6.

Udgangspunktet er, at behandlingen af biometriske data er forbudt når en sådan har til formål entydigt at identificere en fysisk person, jf. art. 9, stk. 1, men behandling kan dog alligevel være tilladt, såfremt den har sit behandlingsgrundlag i de af GDPR art. 9, stk. 2 nævnte undtagelser.

Undtagelserne i litra a, c, d, e og f finder direkte anvendelse, mens litra b, g og h kræver supplerende national lov, for at kunne udgøre et gyldigt behandlingsgrundlag. Databeskyttelseslovens udgør den supplerende nationale lov i Danmark og behandlingen af den særlige kategori af oplysninger reguleres i DBL § 7, der som følge heraf i en række tilfælde vil udgøre grundlaget for offentlige myndigheders og private virksomheders mv. behandling af de særlige kategorier af personoplysninger.[237]

I det følgende vil alene de for specialet relevante behandlingsgrundlag gennemgås, for at klarlægge, hvornår der kan foretages en legitim behandling af biometriske data, som har til formål at identificere en person. Derfor vil alene GDPR art. 9, stk. 2, litra a & g blive gennemgået yderligere.

Det følger af GDPR art. 9, stk. 2, litra a, at den registrerede kan give et udtrykkeligt samtykke til behandling af den særlig kategori af personoplysninger, medmindre denne fravigelse er blevet undtaget af national- eller EU-ret til at kunne afgive samtykke. Kravene for om der foreligger et gyldigt samtykke efter henholdsvis GDPR art. 6, stk. 1, litra a og art. 9, stk. 2, litra a er identiske på trods af ordlyden. Dette følger af, at begge samtykkekrav skal opfylde kravene efter GDPR art. 4, nr. 11 og art. 7.[238]

[237] Nielsen & Lotterup, 2025, s. 468

[238] Knobel & Udsen, 2025, s. 279

Betænkning 1565/2017 konkluderer, at GDPR art. 9, stk. 2, litra a vil være en videreførsel af gældende ret, men lovgiveren har mulighed for at begrænse dette behandlingsgrundlag.[239] I forlængelse heraf fremgår det af lovforarbejderne[240], at Danmark ikke har valgt at indføre et generelt forbud om at registrerede, kan give udtrykkeligt samtykke til behandling af den særlige kategori af personoplysninger.[241]

Ligeledes kan det være en undtagelse, såfremt behandling er betinget af væsentlige samfundsinteresser, der er fastlagt i national ret eller EU-ret, og som står i rimeligt forhold til det formål som forfølges samt respekterer retten til databeskyttelse. Efter dansk lovgivning er der hjemmel i databeskyttelseslovens § 7, stk. 4, til en fravigelse af forbuddet, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser, jf. art. 9, stk. 2, litra g. Yderligere kræver det tilladelse til behandlingen fra Datatilsynet, hvis behandlingen ikke foretages af en offentlig myndighed.

8. Væsentlige samfundsinteresser

Som anført i afsnit 7.3., kan forbuddet om behandling af biometriske data med henblik på entydig identifikation af den registrerede, fraviges, hvis behandling er nødvendig i henhold til en væsentlig samfundsinteresse, som er fastlagt i national ret eller EU-ret, står i rimeligt forhold til det forfulgte formål, og respekterer retten til databeskyttelse, jf. GDPR art. 9, stk. 2, litra g. Derfor kan det udledes af bestemmelsen, at behandlingsgrundlaget for væsentlig samfundsinteresse skal tolkes restriktivt.[242]

Grundet kravet om at behandlingen skal være fastlagt i national ret eller EU-ret forudsætter det, at der sker en supplerende udfyldning i EU-retten eller national ret, hvorfor bestemmelsen ikke uden videre kan anvendes som direkte behandlingsgrundlag.[243]

GDPR præambelbetragtning 41 uddyber, at når GDPR henviser til, at der skal fastsættes en nationalt supplerende ret, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament. Men et sådant retsgrundlag bør imidlertid være klart og præcist, og anvendelse heraf bør være forudsigelig for personer, der er omfattet af dets anvendelsesområde. Hvorimod den analyserede retspraksis fra EUD, der fremgår af afsnit 5.4 i specialet, fastsætter

[239] Betænkning 1565/2027, s. 210 f
[240] Lovforslag L 68 FT 2017-18
[241] Lovforslag L 68 FT 2017-18, s. 176
[242] Lovforslag L 68 FT 2017-18, s. 177
[243] Betænkning nr. 1565/2017, s. 223

at anvendelsen af et "bør" må forstås som et "skal", når der foretages et alvorligt indgreb i retten til privatliv.
DBL § 7, stk. 4, er den danske generelle nationale bestemmelse, der giver hjemmel til en fravigelse af forbuddet i art. 9, stk. 1. og aktiverer GDPR art. 9, stk. 2, litra g. Denne bestemmelse fastslår, at der kan ske behandling af den særlige kategori af personoplysninger, hvis det er nødvendigt af hensyn til væsentlige samfundsinteresser i Danmark.[244]

DBL § 7, stk. 4 forudsætter desuden, at tilsynsmyndigheden, hvilket i Danmark er Datatilsynet, giver tilladelse hertil, såfremt der er tale om en ikke-offentlig myndighed. Datatilsynet kan endvidere fastsætte nærmere vilkår for behandlingen, men det er dog op til Datatilsynet at vurdere, om sådanne vilkår bør stilles. Datatilsynets tilladelse til behandlingen skal dog ikke indhentes, såfremt anden lovgivning indeholder bestemmelser, der udgør det nødvendige retlige grundlag for behandling af oplysninger af hensyn til væsentlige samfundsinteresser.[245]

Der kan dog opstå en usikkerhed for, om der skal foreligge et nationalt supplerende retsgrundlag til DBL § 7, stk. 4., da det er en generel bestemmelse og muligvis ikke opfylder GDPR art. 9, stk. 2's krav om at bestemmelsen skal *stå i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesse.*

> Af *Tele2 Sverige* fremgår det, at indførelsen af en generel ordning vil tilsidesætte de rettigheder, som er sikret ved Chartrets art. 7 og 8, medmindre ordningen suppleres af bestemmelser, der fastsætter tilstrækkelige garantier for beskyttelsen af disse rettigheder. Disse skal udgøres af klare og præcise regler, som regulerer adgangen til dataene, rækkevidden og anvendelsen af en sådan foranstaltning samt mulighed for kontrol ved en domstol eller uafhængig administrativ enhed. I forlængelse heraf skal bestemmelserne navnlig angive, under hvilke omstændigheder og på hvilke betingelser indgrebet kan finde sted. Herved sikres det, at indgrebet er begrænset til det strengt nødvendige.[246]

Argumentet for hvorfor det ikke nødvendigt at indføre yderligere specifikke foranstaltninger end DBL § 7, stk. 4, der aktiverer anvendelsen af væsentlige samfundsinteresser er, at

[244] Motzfeldt & Næser 2025, s. 230
[245] Nielsen & Lotterup, 2025, s. 1077
[246] *Tele2 Sverige,* præmis 51, 109

proportionalitetsprincippet i GDPR art. 9, stk. 2 litra g, svarer til dataminimeringsprincippet indeholdt i GDPR art. 5, stk. 1, litra c. Derudover er det en betingelse for, at behandlingen kan finde sted, at Datatilsynet giver tilladelse hertil, medmindre der er tale om offentlige myndigheder. Dette er med til at sikre, at private dataansvarlige ved behandlinger af den særlige kategori af personoplysninger overholder de strenge krav.[247] Betænkning 1565/2017 konkluderer ligeledes at proportionalitetsprincippet i GDPR art. 9, stk. 2 litra g, svarer til dataminimeringsprincippet.[248]

Men derimod konkluderer Betænkning 1565/2017 også, at det er et krav for den supplerende nationale lov, at denne skal sikre passende og specifikke foranstaltninger. Derudover vurderes det, at foranstaltningerne skal være klare og præcist afgrænset i forhold til beskyttelse af den registrerede grundlæggende rettigheder. Selvom GDPR indeholder en række bestemmelser, der specifikt beskytter den registreredes grundlæggende rettigheder, bør en national lov fastsætte yderligere foranstaltninger udover dem, der fremgår af GDPR.[249] I forlængelse heraf har EDPB i deres seneste retningslinjer[250] fastslået, at det ofte vil kræve en specifik særskilt lov, der præcist beskriver betingelserne for dens anvendelse. Ligeledes understreges det heri, at behandlingen først vil være forenelig med Chartret art. 52, stk. 1, hvis loven er tilstrækkeligt klar og præcis. Derfor vil specialet undersøge om praksis uddyber, hvilke nationalt supplerende lovgivninger, der finder anvendelse ved de enkelte afgørelser.

For at vurdere, om der er en sammenhæng mellem GDPR's væsentlige samfundsinteresser og Chartrets mål af almen interesse, der er anerkendt af Unionen, skal der ses på EU's retlige hierarki. Som tidligere anført i afsnit 5.5, skal GDPR overholde alle de grundlæggende rettigheder og følge de principper, der er fastlagt i Chartret, hvorfor bestemmelserne i GDPR skal udgøre et mål af almen interesse. GDPR fortolker kravet om væsentlige samfundsinteresser mere restriktivt end Chartret, da væsentlige samfundsinteresser stiller krav til bl.a. behandlingens nødvendighed, hvorimod der ved Chartrets mål af almen interesse blot stilles et krav om, at behandlingen forfølger et mål af almen interesse, der er anerkendt af Unionen. Det ses f.eks. i *Digital Rights Ireland*, hvor der forelå et mål af almen interesse[251]i direktivet, at indgrebet opfyldte interesse-kravet, men derimod ikke proportionalitetsprincippet, hvorfor direktivet var ugyldigt. Hvis direktivet afledte sin ret af

[247] Nielsen & Lotterup, 2025, s. 1077
[248] Betænkning 1565/2017, s. 218
[249] Betænkning 1565/2017, s. 218
[250] EDPB Guideline 05-2022, præmis 43-44,
[251] Digital Rights Ireland, præmis 42

GDPR, ville det ikke have opfyldt nødvendighedskravet for at kunne udgøre en væsentlig samfundsinteresse, jf. GDPR art. 9, stk. 2, litra g.[252]
Det må derfor antages, at det er nemmere at opfylde Chartrets krav om mål af almen interesse end GDPR's krav om væsentlig samfundsinteresse, hvorfor det kan lægges til grund, at hvis der foreligger en væsentlig samfundsinteresse, vil det også udgøre et mål af almen interesse.

8.1 Forebyggelse af utryghedsskabende adfærd

Når det skal vurderes, om der kan foretages overvågning med henblik på forebyggelse af utryghedsskabende adfærd, skal indgrebets proportionalitet vurderes i henhold til Chartrets art. 52, stk. 1 og GDPR art. 5, stk. 1, c, hvori det fastslås, at et indgreb skal være proportionalt og ikke mere vidtgående, end hvad der er nødvendigt for at opfylde formålet. Hvis der sker behandling af biometriske persondata af private aktører til identifikation og behandlingsgrundlaget er, at det er nødvendigt af hensyn til væsentlige samfundsinteresse, skal Datatilsynet give tilladelse hertil, jf. DBL § 7, stk. 4., 2. pkt.

Brøndbyernes I.F. Fodbold A/S (herefter Brøndby) ønskede at anvende ansigtsgenkendelse på deres stadion som en tryghedsskabende foranstaltning, hvorfor de anmodede Datatilsynet om at få tilladelse hertil. En sådan ansigtsgenkendelse ville udgøre en indskrænkning i retten til privatliv, hvorfor Datatilsynet i afgørelsen skulle vurdere, om behandlingen af særlige kategorier af personoplysninger ville være lovlig.[253]

> Datatilsynet meddelte tilladelse til Brøndby's brug af ansigtsgenkendelse, under forudsætning af, at visse vilkår blev overholdt. Tilladelsen gjaldt kun ved afvikling af fodboldkampe, hvoraf omfattet er træningskampe med deltagelse af hold fra superligaen, 1. og 2. division, landskampe samt ved fodboldkampe i UEFA-regi[254] på Brøndby Stadion. Meddelelse af karantæne forudsatte endvidere, at dette skete på et sagligt og proportionalt grundlag for Brøndby og Superligaen.
>
> Derudover måtte de personoplysninger, der blev behandlet som følge af ansigtsgenkendelsessystemet, og som ikke stemte overens med oplysninger fra karantænelisten, ikke lagres. I forlængelse af dette skulle personoplysninger, der blev behandlet som led i ansigtsgenkendelsessystemet, og som stemte overens med oplysninger fra karantænelisten, slettes umiddelbart efter hver kamp. Yderligere forudsatte det,

[252] Digital Rights Ireland, præmis 62
[253] DT j.nr. 2018-51-0332
[254] Internationalt udbudte fodboldkampe

at der blev foretaget klar skiltning om, at der blev behandlet biometriske data ved hjælp af et automatisk ansigtsgenkendelsessystem.

Princippet om opbevaringsbegrænsning i henhold til GDPR art. 5, stk. 1, litra e, overholdes af Brøndby, fordi der ved behandling af biometriske data, ikke sker oplagring af de ikke-relevante personoplysninger, mens personoplysninger, der stemmer overens med karantænelisten, bliver slettet umiddelbart efter hver kamp.[255] Datatilsynet kommenterer, at tilladelse til anvendelse af ansigtsgenkendelsessystemet gives, under forudsætning af, at meddelelse af karantæne sker på et sagligt og proportionalt grundlag.[256] Derimod oplyser Datatilsynet ikke, at de har behandlet, hvorvidt indgrebet i retten til privatliv er nødvendigt for at forfølge formålet, hvilket er et krav efter GDPR art. 5, stk. 1, litra c, for at opfylde dataminimering.

Derudover, som beskrevet i afsnit 7.3, er det en forudsætning for at kunne behandle særlige kategorier af personoplysninger, at der identificeres en tydelig lovhjemmel hertil, kommer Datatilsynet ikke videre ind på, i deres offentliggørelse, hvilken hjemmel der legitimerer dette indgreb udover DBL § 7, stk. 4. Dette skal dog tages med forbehold for, at Datatilsynet kan have drøftet det internt, selvom det ikke er noget, der kan udledes af deres offentliggjorte afgørelse.

Brøndby ønsker herefter at udvide deres tilladelse til ansigtsgenkendelse, så det også kan finde anvendelse til deres udebanekampe. Det bliver derfor forelagt Datatilsynet til at træffe afgørelse, om Brøndby kunne få tilladelse til behandling af biometriske data ved andre kampe end på Brøndby Stadion.[257]

Brøndby erfarede, at personer, som fremgik af karantænelisten, formåede at skaffe sig ulovlig adgang til deres udebanekampe, hvilket resulterede i fortsat vold, hærværk og utryghedsskabende adfærd, blot på andre stadioner.

Brøndby ønskede derfor at anvende mobil ansigtsgenkendelse ved kampe på andre stadions, hvilket blev begrundet med, at mobil ansigtsgenkendelse ville forebygge den utryghedsskabende adfærd, der kunne opstå, hvis en person på karantænelisten skulle pågribes af kontrollører under kampen, da dette kunne medføre betydelig gene for de andre tilskuere. Derudover ville der ikke eller i et beskedent omfang blive behandlet særlige kategorier af personoplysninger, af andre personer, f.eks. hjemmeholdets tilhængere, hvilket ikke ville være i overensstemmelse med

[255] DT j.nr. 2018-51-0332, punkt 4 i tilladelsen
[256] DT j.nr. 2018-51-0332, punkt 2 i tilladelsen
[257] DT j.nr. 2022-51-0375

> formålet. Efter Datastyrelsen interesseafvejning var dette dog ikke til hinder for at meddele tilladelse til Brøndby i medfør af DBL § 7, stk. 4.

Det kan udledes af afgørelsen, at den utryghedsskabende adfærd kan udgøre en væsentlig samfundsinteresse, hvorfor behandlingen af den særlige kategori af personoplysninger er lovlig, jf. GDPR art. 9, stk. 2, litra g, jf. DBL § 7, stk. 4.[258] Imidlertid foreskriver Chartrets art. 52, stk. 1., 1. pkt. og GDPR art. 9, stk. 2, litra g, at der skal foreligge et lovgrundlag, der bestemmer, at begrænsningen i retten til privatliv og bestemmelsen skal respektere denne rettigheds væsentligste indhold. Ligesom i den tidligere afgørelse[259], kan det ikke udledes på hvilket retsgrundlag denne tilladelse baseres på. Det ses dog, at Datatilsynet afvejer om behandlingen opfylder dataminimeringsprincippet, ved at vurdere, om risikoen for indgrebet i andre personer, f.eks. hjemmeholdets tilhængere ville forhindre en tilladelse, fordi behandlingen ville ligge uden for formålet og indgrebet derfor ikke ville være proportionalt. Datatilsynet vurderer, at eftersom behandlingen slet ikke, eller kun i et beskedent omfang, finder sted, er indgrebet fortsat begrænset til, hvad der er relevant og nødvendigt for at sikre de tryghedsskabende foranstaltninger, hvorfor disse går forud for de andre personers ret til privatliv. Dette er også i overensstemmelse med princippet om dataminimering, jf. GDPR art. 5, skt. 1 litra c.[260] Behandlingen vil være lovlig, fordi det ikke er muligt at opnå det tiltænkte formål om tryghedsskabende foranstaltninger med mindre indgribende midler.

I forlængelse af dette ønsker F.C. København (FCK) også at få implementeret ansigtsgenkendelse på deres stadion og udebanekampe, og ansøger Datatilsynet om tilladelse hertil.[261]

> FCK fik tilladelse til ansigtsgenkendelse på samme vilkår som Brøndby, hvorfor denne tilladelse kun omfattede fodboldkampe på stadionet. Derimod fik FCK ikke tilladelse til at anvende ansigtsgenkendelse til øvrige arrangementer, der bl.a. omfattede koncerter.

Afgørelsen fastslår, at Datatilsynet afvejer nødvendigheden for at behandle biometriske data ved overvågning, og i hvilken sammenhæng det kan begrundes i at udgøre en væsentligt samfundsinteresse.[262] Samtidig klarlægges det, at det er den dataansvarlige, der skal

[258] DT j.nr. 2022-51-0375, afsnit 3
[259] DT j.nr. 2018-51-0332
[260] DT j.nr. 2022-51-0375, afsnit 3.1.
[261] DT j.nr. 2024-51-0012
[262] DT j.nr. 2024-51-0012, afsnit 3.

bevise, at der foreligger en nødvendighed for et alvorligt indgreb, og dette vil blive sammenlignet med andre mindre indgribende foranstaltninger.[263] Derudover viser afgørelsen, at der ikke foreligger den samme utryghedsskabende adfærd, som gør sig gældende ved fodboldkampe, ved andre arrangementer hos FCK, da der ikke udstedes karantæner i samme omfang.[264] Ligesom i de to tidligere afgørelser, kommer Datatilsynet ikke videre ind på, i deres offentliggørelse, hvilken hjemmel der legitimerer dette indgreb udover DBL § 7, stk. 4. Dette skal dog tages med forbehold for, at Datatilsynet kan have drøftet det internt. Endelig viser afgørelsen, at selvom formålet hver gang har været at skabe tryghedsskabende foranstaltninger, er nødvendigheden heraf afgørende for, om der kan gives tilladelse og antallet af registrerede der er blevet sanktioneret til en pågældende begivenhed er afgørende.[265]

I forlængelse af de givne tilladelser til Brøndby og FCK, anmodede Divisionsforeningen i denne afgørelse, om at få tilladelse til, at klubberne i henholdsvis Superligaen[266] og 1. Divisionen[267] kunne behandle biometriske data ved brug af automatisk ansigtsgenkendelse med henblik på at håndhæve karantæner og forebygge utryghedsskabende adfærd.[268]

> Ligesom tidligere ansøgninger vedr. ansigtsgenkendelse bestod der i denne afgørelse et ønske om at behandle biometriske data, med det formål entydigt at identificere en person ved brug af dennes biometriske data, idet de daværende foranstaltninger ikke var tilstrækkelige. Divisionsforeningen anså derfor ansigtsgenkendelse som et nødvendigt og sagligt middel, der på en effektiv måde skulle understøtte bekæmpelsen af uro og utryghedsskabende adfærd ved fodboldkampene.
>
> Datatilsynet gav tilladelse til, at klubberne i Superligaen kunne foretage denne ansigtsgenkendelse, hvilket var begrundet i bl.a. mængden af igangværende karantænesager, overtrædelser af ordensreglementet samt mængden af fremmødte tilskuere, hvilket førte til utryghedsskabende adfærd.
>
> Derimod fik klubberne i 1. Divisionen afslag, da de foreliggende omstændigheder, der gjorde at Superligaklubberne fik tilladelse, ikke forelå i samme grad for klubberne i 1. Divisionen, da bekæmpelsen af uro og utryghedsskabende adfærd ved fodboldkampene ville kunne opnås ved mindre indgribende midler.

[263] DT j.nr. 2024-51-0012, afsnit 2.1
[264] DT j.nr. 2024-51-0012, afsnit 2.1
[265] DT-j.nr. 2024-51-0012, afsnit 3
[266] Superligaen er den øverste liga i Dansk Fodbold
[267] 1. Divisionen er Danmarks næstøverste fodboldliga
[268] DT j.nr. 2024-51-0014

> Dette betød, at hvis den pågældende klub rykkede ned til 1. Division, ville dette resultere i, at tilladelsen ville blive ophævet.

Ligesom tilfældet er i de tidligere afgørelser, kan det udledes, at behandling af biometriske data, ved brug af ansigtsgenkendelse, kan finde sted, når der er tale om forebyggelse af utryghedsskabende adfærd, da Datatilsynet vurdere at det er at betegne som en væsentlig samfundsinteresse, jf. GDPR art. 9, stk. 2, litra g, jf. DBL § 7, stk. 4.[269] GDPR art. 9, stk. 2, litra g., forudsætter et nationalt supplerende retsgrundlag, hvilket ikke fremgår af den offentliggjorte meddelelse af Datatilsynet. Imidlertid er det kun Superliga klubberne, der får tilladelse til behandle biometriske data til brug af automatisk ansigtsgenkendelse, hvilket er begrundet i, at der eksisterer et større antal karantænesager i Superligaen og der er generelt et større tilskuerantal[270], modsat 1. Divisionen, hvorfor 1. Divisionen får afslag. Det kan udledes af afgørelsen, at bekæmpelsen af uro og utryghedsskabende adfærd ved fodboldkampene udgør en væsentlig samfundsmæssig interesse, der legitimerer et indgreb i retten til privatliv, men det er en konkret vurdering om proportionalitetsprincippet er opfyldt. Ligesom i de tre tidligere afgørelser, behandler Datatilsynet ikke i deres offentliggørelse, om der er andre hjemler end DBL § 7, stk. 4, der legitimerer indgrebet. Dette skal dog tages med forbehold for, at Datatilsynet kan have drøftet det internt.

Det Spanske Datatilsyn (AEPD) skulle behandle en lignende sag i Spanien[271] om brug af ansigtsgenkendelse med henblik på entydig identifikation på fodboldstadioner.[272]

> Den Spanske Kommission mod vold, racisme, xenofobi og intolerance (Kommissionen) anmodede om tilladelse til et ansigtsgenkendelsessystem ved indgangen til stadionerne, der skulle behandle tilskuernes biometriske data af hensyn til sikkerheden og integriteten for personer på stadionet samt forebyggelse af "hatecrimes" og diskrimination. Kommissionen mente, at de i national lovgivning[273] havde hjemmel til at implementere sikkerhedsforanstaltninger for begivenheder og konkurrencer med en høj risiko.
>
> AEPD meddelte Kommissionen, at hvis der skulle behandles biometriske data, skulle der identificeres en væsentlig samfundsinteresse og ikke blot en samfundsinteresse. AEPD vurderede, at den spanske lov ikke identificerede en væsentlig

[269] DT j.nr. 2024-51-0014, afsnit 3.
[270] DT j.nr. 2024-51-0014, afsnit 3
[271] Grundet totalharmonisering kan praksis fra andre medlemsstater i EU anvendes, jf. afsnit 4.2.4.
[272] GDPRhub AEPD (Spain) - 0098/2022
[273] Artikel 13, stk. 1 i den spanske lov mod vold, racisme, xenofobi og intolerance i sport

samfundsinteresse eller indeholdt specifikke regler, der kunne have gjort behandlingen lovlig. Loven indeholdt mulighed for at foretage identitetskontrol, men dog ikke mulighed for at anvende biometriske systemer. Derudover indeholdt den ikke tilstrækkelige garantier, der kunne beskytte den registreredes grundlæggende rettigheder. På den baggrund afslog AEPD Kommissionens anmodning om anvendelse af ansigtsgenkendelse på stadioner.

AEPD fastslår indledningsvis, at der er tale om særlige kategorier af personoplysninger der bliver behandlet ved henholdsvis biometrisk identifikation- og verifikationssystem.[274] I den forbindelse vurderer de, at anvendelsen af ansigtsgenkendelse udgør et biometrisk identifikationssystem. I forlængelse heraf fastslår AEPD, at anvendelsen af biometriske identifikationssystemer anses for at være særlig indgribende i den registrerede grundlæggende rettigheder.[275] Dette kan sidestilles med følelsen af konstant overvågning, og kan derfor være i strid med Chartrets art. 7 og 8. Yderligere fastslår APED, at ud fra ordlyden i GDPR art. 9, stk. 2, litra g, kræver *væsentlig* samfundsmæssig interesse i modsætning til en almen samfundsmæssig interesse, før den kan finde anvendelse. Dette understreger betydningen af samt nødvendigheden for en stærkere beskyttelse af de oplysninger, der bliver behandlet.[276]

Ved behandling af biometriske oplysninger i henhold til GDPR art. 9, stk. 2, litra g, er det forudsat, at behandlingen er fastsat i en retsregel på enten EU-retligt eller nationalt niveau. Loven skal endvidere præcisere den væsentlige offentlige interesse, der begrunder indgrebet i retten til beskyttelse af personoplysninger, samt angive under hvilke omstændigheder dette indgreb kan foretages. Den skal fastsætte regler, der gør det forudsigeligt for den registrerede, at en sådan begrænsning kan blive pålagt, samt hvilke konsekvenser dette kan have. En generel henvisning til en offentlig interesse er i den forbindelse ikke tilstrækkelig. Endelig skal loven under alle omstændigheder respektere proportionalitetsprincippet, således som det er understreget i Domstolens praksis.[277]

Derudover følger det af fast retspraksis på det forfatningsretlige område, at lovforbeholdet ikke kun er begrænset til at kræve, at der i loven er hjemmel til foranstaltninger, der foretager et indgreb i de grundlæggende rettigheder. Det er endvidere påkrævet, at lovgiver fastslår de situationer, betingelser og garantier, der gælder for at kunne foretage indgreb i de grundlæggende rettigheder.[278]

[274] GDPRhub AEPD (Spain) - 0098/2022, overskrift 3
[275] GDPRhub AEPD (Spain) - 0098/2022, overskrift 5
[276] GDPRhub AEPD (Spain) - 0098/2022, overskrift 6
[277] GDPRhub AEPD (Spain) - 0098/2022, overskrift 14
[278] GDPRhub AEPD (Spain) - 0098/2022, overskrift 13

AEPD fastslår, at den spanske nationale lov giver mulighed for at der kan anvendes systemer til identitetskontrol, men det fremgår dog ikke af loven, at der kan anvendes biometriske data med det formål entydigt at identificere en fysisk person. Idet den nationale lov ikke eksplicit har taget stilling til de særlige risici, der gælder ved behandling af biometriske data eller fastsat specifikke garantier, vil denne ikke udgøre et tilstrækkeligt nationalt supplerende retsgrundlag til art. 9, stk. 2, litra g.[279]
I modsætning til det danske Datatilsyn, indeholder AEPD's afgørelse således en identifikation af, om det nationalt supplerende retsgrundlag indeholder mulighed for en implementering af ansigtsgenkendelse. Det er fastslået, at behandling af personoplysninger kan udgøre et lovligt indgreb i retten til privatlivet, hvis dette udgør en væsentlig samfundsinteresse. Førend en sådan behandling kan foretages, er det betinget, at denne sker i overensstemmelse med lov, forfølger et legitimt formål, respekterer det væsentligste indhold af de grundlæggende rettigheder og er nødvendig for at opnå et legitimt mål. Dette er udtryk for undtagelsesbestemmelsen i Chartrets, art. 52, stk. 1.[280] Anvendelsen af ansigtsgenkendelse vil derfor udgøre et ulovligt indgreb, da det nationalt supplerende retsgrundlag ikke opfylder kravene i henhold til GDPR og Chartret.

Med afsæt i ovenstående afgørelser, kan det indledningsvist fastslås, at forebyggelse af utryghedsskabende adfærd kan udgøre en væsentlig samfundsmæssig interesse og derved udgøre et lovligt indgreb i retten til privatliv. Det vil altid være en konkret vurdering, om interessen er væsentlig og heri indgår elementer såsom sikkerhedsbehov, formålets samfundsmæssige betydning, indgrebets påvirkning i forhold til målet samt problemets alvor og omfang.
Hertil skal der dog, i henhold til proportionalitetsvurderingen, identificeres visse parametre, der kan legitimere et indgreb, da retten til privatliv vægtes højt. Dette forstærkes af det faktum, at der skal foreligge tilstrækkeligt klare garantier for den registreredes grundrettigheder. Derudover skal der foreligge et nationalt supplerende retsgrundlag, der tydeligt tillader behandlingen af særlige kategorier af personoplysninger førend behandlingsgrundlaget efter GDPR art. 9, stk. 2, litra g, er opfyldt. I forlængelse heraf kræver det, at de bestemmelser, der muliggør indgrebet i retten til privatliv, er tilstrækkelig klare og præcise, så indgrebets rækkevidde er anskueliggjort for den registrerede, jf. Chartrets art. 52, stk. 1. En generel henvisning til en offentlig interesse vil ikke være tilstrækkelig i denne henseende. En manglende identifikation af dette vil være i strid med Chartret.

[279] GDPRhub AEPD (Spain) - 0098/2022, overskrift 15
[280] GDPRhub AEPD (Spain) - 0098/2022, overskrift 6

8.2 Supplerende national lov

Væsentlige samfundsinteresser udgør et af behandlingsgrundlagene, hvortil der bl.a. stilles krav om, at indgrebet har et nationalt supplerende retsgrundlag. Fodboldstadions-afgørelserne fra Datatilsynet viser, at Datatilsynet anvender DBL § 7, stk. 4, som det nationalt supplerende retsgrundlag, der kræves i henhold til GDPR art. 9, stk. 1. Der er dog usikkerhed, om Datatilsynet har anvendt andre supplerende retsgrundlag. Hvis dette ikke er tilfældet, tyder det på, at DBL § 7, stk. 4 legitimerer en bred fortolkning for anvendelsen GDPR art. 9, stk. 2, litra g.

Det fremgår af *Chromebook*-afgørelsen[281], at der tillægges en bred fortolkning af formålet til folkeskoleloven[282] (FSL), hvorved den dataansvarlige, i henhold til denne lov, kan behandle personoplysninger.[283]

> I den foreliggende sag vurderede Datatilsynet, at formålet med behandling var at eleverne skulle undervises i EDB[284] i forskellige anvendelsessituationer. Formålet om EDB-undervisning fremgik kun af lovforarbejderne, men ikke bestemmelsernes ordlyd. Alligevel forelå der et gyldigt behandlingsgrundlag for videregivelse af elevernes oplysninger til levering, sikkerhed og drift af tjenesterne. Men formålet var ikke foreneligt med behandling af videregivelse af oplysninger til udvikling af nye produkter mv. af Google.

Derfor foretager Datatilsynet en bred fortolkning af det formål, der hverken fremgår af ordlyden eller forarbejderne.[285] Det er vigtigt at understrege, at der sker behandling af almindelige personoplysninger, hvorfor det vil udgøre et mindre indgreb i retten til privatliv, end hvis der skete behandling af den særlige kategori af personoplysninger.

Hvis DBL § 7, stk. 4 sambehandles med en anden national lov, som udgør behandlingsgrundlaget for GDPR art. 9, stk. 2, litra g., vil det være nærliggende at antage at det fremgår af hooliganloven[286] (HGL). Denne lov forholder sig dog kun til, at der kan ske videregivelse af lister til kontrollører, og at kontrollørerne kan behandle de personoplysninger, der er nødvendige for at håndhæve karantæner. HGL indeholder dog ingen specifik hjemmel for behandlingen af den særlige kategori af personoplysninger. I Chromebook-sagen tillægges

---

[281] DT j.nr. 2023-431-0001

[282] Lovbekendtgørelse nr. 1086 af 15. august 2023 om folkeskolen (FSL) - obs. historisk lovbekendtgørelse

[283] Jf. GDPR art. 6, stk. 1, litra e, jf. art. 6, stk. 3, og FSL § 2, stk. 1, og § 18, stk. 1.

[284] Systematisk bearbejdning af data ved hjælp af computere

[285] DT j.nr. 2023-431-0001, afsnit 4.2.3 & 4.2.5

[286] Lovforslag L 38 Forslag til lov om sikkerhed ved bestemte idrætsbegivenheder. Folketinget 2007-08 2-samling, 12. oktober 2007.

forarbejderne til loven en bred fortolkning, og det fremgår af lovforslaget[287] til HGL at der ved behandling af oplysninger også kan ske videregivelse af følsomme oplysninger[288] til kontrollører.[289] Formålet med behandling er at varetage sikkerheden ved afholdelse af større idrætsbegivenheder, hvilket udgør en væsentlig samfundsinteresse.[290] I forlængelse heraf fremgår det af AI-genoptræning afgørelsen[291], at behandlingsgrundlaget efter GDPR art. 9, stk. 2, litra g, ikke var opfyldt. Det blev begrundet i, at hverken i serviceloven[292] eller dens forarbejder var der taget tilstrækkelig stilling til behandling af personoplysninger, men derimod alene hjemmel til behandling af almindelige personoplysninger.[293] Ud fra ovenstående udlægning vil behandlingsgrundlaget i medfør af DBL § 7, stk. 4, jf. formålet i HGL's lovforslag, være i overensstemmelse med GDPR art. 9, stk. 2, litra g.
Dette vil dog ikke stemme overens med det, der fremgår af den Spanske stadions-afgørelsen[294], som foreskriver at loven skal være tilstrækkeligt klar og præcis, så den registrerede kan forudsige sin retsstilling, og der skal fremgå en tydelig hjemmel til behandling af den særlige kategori af personoplysninger. Ligeledes har EUD i dommen *C-143/83 Kommissionen mod Danmark*[295] slået fast, at bemærkningerne til lovforslaget ikke sikrer en hensigtsmæssig information til de berørte personer.[296] Endvidere fremgår det tydeligt af både Chartrets art. 8, stk. 2 og 52, stk. 1 samt GDPR art. 9, stk. 2, litra g, at behandlingen skal være fastsat i lov, hvoraf det følger at muligheden for indgreb ikke må fremgå af forarbejderne, men derimod skal fremgå klart og præcist af loven for at sikre forudsigelighed i den registreredes retsstilling.

Det er derfor fortsat uklart, hvad der udgør det fornødne nationalt supplerende retsgrundlag. Spørgsmålet bliver i henhold til Fodboldstadions-afgørelserne, om DBL § 7, stk. 4, udgør det nationalt supplerende retsgrundlag, eller om denne suppleres af en anden lov. Da der ikke foreligger praksis fra EUD på området, er det usikkert, hvilke krav EUD ville stille til et nationalt supplerende retsgrundlag, hvis de skulle træffe afgørelse herom.

[287] Lovforslag L 38 Forslag til lov om sikkerhed ved bestemte idrætsbegivenheder.
[288] Adækvat til særlig kategori af personoplysninger
[289] Lovforslag L 38, s. 1736 f
[290]Lovforslag L 38, s. 1735
[291] DT j.nr.: 2023-212-0015
[292] Lovbekendtgørelse nr. 1089 af 16/08/2023 om social service - obs. historisk lovbekendtgørelse
[293] DT j.nr.: 2023-212-0015, afsnit 3.3 & 3.4.2
[294] GDPRhub AEPD (Spain) - 0098/2022
[295] Kommissionen mod Danmark, C-143/83, EU:C:1985:34
[296] Kommissionen mod Danmark, præmis 11

9. Samtykke til behandling af biometriske data

Det fremgår af Chartrets art. 8, stk. 2, at samtykke kan anvendes til behandling af personoplysninger, hvis disse behandles rimeligt og til et udtrykkeligt angivne formål. Dette behandlingsgrundlag er eksplicit fastsat i art. 9, stk. 2, litra a, men det fremgår ikke af denne bestemmelse, hvad der udgør et gyldigt samtykke. I denne sammenhæng skal det fastslås, at GDPR art. 7 præciserer betingelserne for samtykke, og skal ses i sammenhæng med GDPR art. 4, nr. 11, der indeholder den legale definition på, hvad der skal forstås ved begrebet "samtykke":[297]

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

Ud fra ovenstående bestemmelse kan samtykke derfor deles op i 4 krav: Krav om ***frivilligheden***, ***specifikationskravet***, ***informationskravet*** og ***utvetydig viljestilkendegivelse***. Før der gås i dybden med disse krav, skal det dog klarificeres, at det som udgangspunkt skal være den registrerede selv, der afgiver sit samtykke, medmindre denne ikke i en fysisk eller juridisk sammenhæng kan afgive sit samtykke.[298]
Meningen i denne sammenhæng er derfor at undtage de tilfælde, hvor den registrerede som følge af sygdom eller på grund af en foretagen rejse ikke kan afgive et gyldigt samtykke.[299]

Når GDPR fastslår, at samtykke skal være afgivet ***frivilligt***, menes der at den registrerede ikke må være forhindret i at have haft et reelt eller frit valg, eller ikke kan afvise eller trække sit samtykke tilbage, uden at det vil være til skade for vedkommende.[300]
Derudover skal et samtykke også være ***specifikt***, hvis det skal leve op til kravene i GDPR art. 4, nr. 11. I henhold til dette krav skal det klart og utvetydigt fremgå, hvad der gives samtykke til, dvs. det skal gøres klart, hvilke oplysninger, der må behandles som følge af samtykket, af hvem og til hvilke formål. Såfremt der er flere behandlingsformål, skal det fremgå, hvilke oplysninger der vil blive behandlet til hvert formål. Samtykket skal derfor

[297] Spiecker gen. Döhmann et al., 2023, s. 377
[298] Nielsen & Lotterup, 2025, s. 294
[299] Nielsen & Lotterup, 2025, s. 294
[300] Trzaskowski et al., 2025, s. & Lotterup, 2025, s. 299

granuleres, dvs. der skal kunne gives separat samtykke til de individuelle behandlingsformål, så den registrerede har mulighed for at afvise andre behandlingsformål.[301]
Samtykket skal yderligere være ***informeret***, hvormed menes, at den registrerede skal oplyses om, hvad det er denne giver sit samtykke til. Et informativt samtykke forudsætter bl.a. at den dataansvarlige oplyser, hvem den dataansvarlige er, formålet med behandlingen, hvilke oplysninger der vil være omfattet af behandlingen og retten til at trække samtykke tilbage.[302]
Endeligt er det forankret i bestemmelsen, at samtykket skal være udtryk for en ***utvetydig viljestilkendegivelse***, hvorom dette krav fastslår, at den registrerede aktivt skal tilvælge samtykke som behandlingsgrundlaget og forudfyldte erklæringer fra den dataansvarlige vil ikke udgøre et gyldigt samtykke.[303]
Såfremt et behandlingsgrundlag baseres på samtykke, så skal det af den dataansvarlige påvises, at den registrerede har givet samtykke til behandling af sine personoplysninger, jf. GDPR art. 7, stk. 1. Derudover fremgår det af GDPR art. 7, stk. 2., at hvis den registrerede giver sit samtykke via en skriftlig erklæring, der også angår andre forhold, skal anmodningen udarbejdes på en måde, der klart kan skelnes fra andre forhold, i en letforståelig og lettilgængelig og i et klart og enkelt sprog. Hvis erklæringen ikke opfylder disse krav, vil den ikke være bindende, da det er en overtrædelse af GDPR.
Dernæst har den registrerede ret til altid at trække sit samtykke tilbage, hvilket den registrerede også skal oplyses om, inden denne afgiver sit samtykke, jf. art. 7, stk. 3. Hvis samtykke trækkes tilbage, vil dette ikke påvirke lovligheden af den behandling, der er foretaget på baggrund af samtykket før tilbagetrækningen af samtykke.
At kunne trække sit samtykke tilbage skal være lige så nemt, som det var at give det, jf. GDPR art. 7, stk. 3.
Ved vurdering af om et samtykke er givet frit, skal der tages størst muligt hensyn til, om bl.a. om opfyldelse af en kontrakt er gjort betinget af at der givet samtykke til en behandling, der er mere omfattende end nødvendigt for at opfylde kontrakten, jf. GDPR art. 7, stk. 4. Hvis samtykket er mere omfattende end nødvendigt, er det tvivlsomt om dataminimeringsprincippet er opfyldt, hvorfor samtykket ikke vil være frivilligt afgivet og derved være ugyldigt.[304] EDPB har i deres vejledning[305] præciseret, hvornår der alligevel kan foreligge et samtykke, på trods af at GDPR art. 7, nr. 4 ikke er opfyldt. Der kan således stadigvæk

[301] Motzfeldt & Næser, 2025, s. 191 f
[302] Motzfeldt & Næser, 2025, s. 194
[303] Christensen & Sørensen, 2024, s. 188
[304] Nielsen & Lotterup, 2025, s. 455
[305] EDPB's Retningslinjer 05/2020, præmis 32- 37

afgives et gyldigt samtykke til behandlingen, hvis der foreligger et reelt alternativ, som ikke er mere vidtgående end nødvendigt og medfører yderligere omkostninger for den registrerede.

Det følger heraf i henhold til præambelbetragtning 43, at et samtykke må vurderes ikke at være afgivet frivilligt, såfremt der er en klar skævhed mellem den registrerede og den dataansvarlige, og samtykke bør anvendes til behandling, hvis den dataansvarlige er en offentlig myndighed.

9.2 Samtykke til behandling af biometriske data

Igennem årene har samtykkets betydning i databeskyttelsesretten udviklet sig, hvilket især har vist sig ved, at reguleringens fokus har bevæget sig fra en regulering af computerteknologi og de hertil knyttede risici til et øget fokus på den registrerede selvbestemmelse.[306]

Den registreredes ret til selvbestemmelse, hvoraf må formodes at være en ret til at bestemme, om ens personoplysninger bliver behandlet, kom bl.a. til udtryk i denne afgørelse, hvor FysioDanmark havde opstillet et overvågningssystem, som medførte, at kunders personoplysninger blev behandlet, selvom de havde nægtet at give samtykke.[307]

> Et fitnesscenter, FysioDanmark, ønskede at opstille et kamera ved deres indgang, som via ansigtsgenkendelse kunne identificere kunder ved at sammenligne med billeder lagret i en database. Systemet ville være online uafbrudt. Kunder, der ikke ønskede at give samtykke, kunne i stedet bruge adgangskort eller kode.
>
> Datatilsynet vurderede, at der var tale om behandling af særlig kategori af personoplysninger, fordi formålet med behandlingen var entydig identifikation. Det var derfor uden betydning, om der faktisk skete et match, eller om behandlingen alene var kortvarig. Samtykket til selve adgangskontrollen opfyldte kravene i GDPR. Men fordi ansigtsgenkendelse også blev anvendt til at indsamle oplysninger om mødetider, krævede det en separat behandlingsaktivitet, hvilket igen krævede et særskilt samtykke. Endelig lagde Datatilsynet vægt på, at det konstant aktive kamera indebar, at også kunder, der ikke havde givet samtykke til behandlingen, fik behandlet deres biometriske data, hvis de bevægede sig inden for kameraets rækkevidde, hvilket udgjorde et uretmæssigt indgreb.

[306] Christensen & Sørensen, 2024, s. 162

[307] DT j. nr. 2021-431-0145

Indledningsvist skal det gøres klart, at der foreligger en behandling af biometriske data, hvorfor der skal identificeres en undtagelse til forbuddet i art. 9, stk. 1., hvilket i dette tilfælde er den registreredes samtykke i henhold til art. 9, stk. 2., litra a. Den samtykkeerklæring, kunderne bliver præsenteret for, opfylder kravene i henhold til GDPR art. 7, stk. 1-4 og art. 4, nr. 11.[308] Ligeledes bliver de præsenteret for mindre indgribende alternativer, hvorefter de fortsat kan benytte fitnesscentrets faciliteter, i form af fysiske adgangskort og koder.[309]

Derimod vil selve overvågningen være problematisk, da kunder som ikke har afgivet samtykke til behandlingen af deres biometriske data, alligevel kan få behandlet disse, fordi systemet er online uafbrudt. Datatilsynet fastslår, at det er selve formålet med behandlingen, der er afgørende, hvilket i dette tilfælde er *med henblik på entydig identifikation*. Derfor er det uden betydning, om der faktisk sker en entydig identifikation, og om behandlingen alene er at betegne som ganske kortvarig.[310] Dette er ligeledes i overensstemmelse med EDPB's retningslinjer, hvorefter behandling af biometrisk data med formål at identificere i sig selv altid vil udgøre et alvorligt indgreb. Dette er uafhængigt af behandlingens endelige resultat, herunder om behandlingen resulterer i et no-hit, eller om den biometriske skabelon slettes øjeblikkeligt.[311]

Ansigtsgenkendelse som adgangskontrol vil dog ikke i sig selv være i strid med proportionalitetsprincippet. Hvis brugen af systemet forudsætter en form for aktivering, f.eks. tastetryk[312], ville dette medføre, at systemet ikke er online uafbrudt, hvorfor behandlingen af personers data, der ikke giver samtykke, ville kunne begrænses til alene at angå registrerede, der har afgivet samtykke. De mindre indgribende alternativer i form af adgangskort og adgangskode kunne derved siges at være blevet illusoriske, idet systemet fortsat ville være online uafbrudt, hvorfor kundernes oplysninger alligevel ville blive behandlet, selvom de gjorde brug af de mindre indgribende alternativer, hvilket ville kunne bidrage til en følelse af konstant overvågning. Derudover viser afgørelsen også, at retten til privatliv vægter højt, da fitnesscentret ikke kan foretage en overvågning over for registrerede, der ikke har givet samtykke til behandlingen af deres data.

[308] DT j. nr. 2021-431-0145, Afsnit 3.2.1
[309] DT j. nr. 2021-431-0145, Afsnit 3.2.1
[310] DT j. nr. 2021-431-0145, Afsnit 3.4
[311] EDPB retningslinjer *05/2022, præmis 36*
[312] DT j. nr. 2021-431-0145, Afsnit 3.4

Kravet om mindre indgribende alternativer i et fitnesscenter var ligeledes et fokusområde i denne afgørelse, hvor Datatilsynet skulle vurdere, om de i sagens udbudte alternativer til ansigtsgenkendelse konstituerede reelle alternativer.[313]

> Den registrerede ville ikke give samtykke til Sporting Health Club Scandinavia ApS's (SHC) behandling af dennes biometriske data via ansigtsgenkendelse, og derudover mente han ikke, at der forelå reelle alternativer til ansigtsgenkendelse. SHC erklærede sig uenige hermed, da de anførte, at generering af kode, adgang via receptionen og adgang via døgnsupport udgjorde alternative adgangsmuligheder. Datatilsynet vurderede, at receptionen ikke udgjorde ifølge et reelt alternativ, da det begrænsede adgangen. De andre alternativer blev dog anset som tilstrækkelige, forudsat at disse ikke var forbundet med lang ventetid.
>
> Ansigtsgenkendelsessystemet foretog kun behandling af dem, som havde afgivet samtykke hertil, da behandlingen hver gang forudsatte en aktiv handling fra den registrerede, hvorfor Datatilsynet vurderede, at dataminimeringsprincippet var overholdt. Slutteligt fastslog Datatilsynet, at samtykke kun er gyldigt afgivet, hvis det er opdelt efter hvert af de enkelte formål dataene behandles til.

Det følger af ovenstående afgørelse, at der ved vurderingen af, om et samtykke er frivilligt afgivet, skal foreligge alternativer, der er mindre indgribende, end den forudsatte brug af automatisk genkendelse. Derudover behøver alternativet ikke være identisk med ansigtsgenkendelse, men det må dog ikke indebære begrænsninger eller omkostninger for den registrerede. Det foreliggende alternativ for at tjekke ind i receptionen via personlig betjening i receptionens åbningstid, vil dog ikke udgøre et tilsvarende alternativ, da den registrerede begrænses i sin adgang til at opnå adgang til centeret sammenholdt med ansigtsgenkendelse.[314] Derimod vil det udgøre tilstrækkelige alternativer, hvis den registrerede i stedet for adgang via ansigtsgenkendelse, kan opnå adgang til centeret ved hjælp af adgangskode og adgangskort, da disse alternativer ikke er forbundet med meromkostninger eller nævneværdige begrænsninger. Dette vil dog ikke være tilfældet, hvis alternativerne ikke udgør reelle alternativer, f.eks. hvis disse er forbundet med urimelig lang ventetid for at få adgang til centeret.[315]

Imidlertid ville SHC ikke opfylde frivillighedskravet, hvis den registrerede blot ville blive henvist til at træne i den åbnede bemandingstid, hvis ikke denne ønskede at give samtykke

[313] DT j.nr. 2023-31-0028

[314] DT j.nr. 2023-31-0028, afsnit 3.4.1

[315] DT j.nr. 2023-31-0028, afsnit 3.4.1

til ansigtsgenkendelse. Dette vil begrænse dem, som ikke giver samtykke til behandling adgang til fitnesscentret modsat dem, der har afgivet samtykke til ansigtsgenkendelse.[316]
Derudover fremgår det af afgørelsen, at behandlingen af biometriske data via ansigtsgenkendelse opfylder kravet om dataminimering, jf. GDPR art. 5, stk. 1, litra c, da det forudsætter en aktiv handling, så kun den, der har afgivet samtykke til ansigtsgenkendelse får behandlet sine biometriske data.[317]
Ligeledes vil samtykke ikke opfylde frivillighedskravet, hvis ikke der kan gives samtykke til hvert af de enkelte behandlingsformål. Samtykke skal derfor granuleres, da et af den registrerede afgivet samtykke i henhold til én behandlingsaktivitet ikke vil udgøre et gyldigt samtykke i henhold til en anden behandlingsaktivtet.[318]
Modsat den sidste afgørelse ville der derfor ikke i denne afgørelse foreligge en følelse af konstant overvågning, da systemets overvågning forudsætter en aktiv handling, og systemet er derfor ikke online uafbrudt.

Datatilsynet fik en forespørgsel fra BornholmsTrafikken i 2003, som er en statsvirksomhed, der har til formål at transportere mennesker, gods etc. til og fra Bornholm.[319]

> Virksomheden ønskede at ændre deres billigste pendlerkort, så det fremadrettet ikke længere indeholdt et billed-id, men derimod et personligt chipkort, der indeholdt pendlerens fingeraftryk. Formålet var, at det skulle formindske muligheden for misbrug med pendlerkortet, så det ikke længere var muligt at andre kunne låne pendlerkortet. Fingeraftrykket ville kun blive opbevaret på det udleverede kort, og der var ikke nogen central database, og efter scanning af fingeraftrykket ved check-in ville alle ikke-relevante oplysninger slettes.
>
> Datatilsynet kom frem til, at de biometriske oplysninger efter den daværende persondatalov ikke udgjorde en følsom personoplysning, hvorfor det alene skulle reguleres efter behandlingen af ikke-følsomme personoplysninger. Datatilsynet vurderede, at virksomhedens interesse i at sikre entydig identifikation af pendlerne vejede tungere end pendlernes interesse i, at oplysningerne ikke blev behandlet, hvorfor der blev givet tilladelse til behandling af biometriske data.

Det skal understreges, at Datatilsynet har behandlet sagen efter de daværende regler, hvorfor en afgørelse efter *de lege lata* formentlig vil få et andet udfald. For det første følger

316 DT j.nr. 2023-31-0028, afsnit 3.4.2
317 DT j.nr. 2023-31-0028., afsnit 3.4.1
318 DT j.nr. 2023-31-0028., afsnit 3.4.1
319 DT j.nr.: 2003-212-0143 - afgørelsen er ikke inddelt i afsnit, hvorfor analysen ikke indeholder en reference til afsnittene.

det af GDPR art. 9, stk. 1, at behandlingen af et system, som anvender biometrisk verifikation, vil være omfattet af behandling af særlige kategorier af personoplysninger, hvorfor behandlingen vil være forbudt, medmindre der foreligger hjemmel hertil i GDPR, art. 9, stk. 2.

Det er relevant at diskutere om dataminimeringsprincippet stadigvæk er opfyldt, jf. GDPR art. 5, stk. 1, litra c, idet fingeraftrykket nu udgør en behandling af særlige kategorier af personoplysninger, hvorimod f.eks. et pendlerkort med billede eller krav om at have et id-kort med, ville udgøre en personoplysning.

Datatilsynet er af den opfattelse, at behandlingen af oplysningerne var nødvendig af hensyn til opfyldelse af en kontrakt ved check-in, hvorfor virksomheden har hjemmel hertil. Yderligere kommer Datatilsynet frem til, at der efter en interesseafvejning er hjemmel til formålet med behandlingen af biometriske oplysninger, idet virksomhedens interesse i at sikre entydig identifikation af pendlerne vejer tungere end pendlernes interesse i, at oplysningerne ikke behandles, hvilket også bliver sammenholdt med, at pendlerne frivilligt køber pendlerkortet. Endelig fastslår Datatilsynet at proportionalitetsprincippet er opfyldt, idet oplysningerne er relevante og tilstrækkelige og er ikke mere omfattende, end hvad der kræves til opfyldelse af formålet, hvortil oplysningerne indsamles, og derfor opfylder persondatalovens bestemmelser.

Verifikationssystemet vil efter de nugældende regler i GDPR, vurderes at være meget indgribende i den registreredes ret til privatliv end kort med billed-id. Hvis indgrebets behandlingsgrundlag udgøres af væsentlig samfundsinteresse, jf. GDPR art. 9, stk. 2, litra g, kræver det, at indgrebet er nødvendigt, hvorfor der ikke må foreligge mindre indgribende alternativer, som kan opfylde formålet med behandlingen. Selvom virksomheden oplever misbrug med deres pendlerkort, kan det ikke berettige, at der foretages et så alvorligt indgreb, idet der foreligger mindre indgribende alternativer, f.eks. ID-rabatkort med billede. Anvendelsen af et verifikationssystem vil derfor ikke opfylde dataminimeringspricippet, hvorfor der ikke kan ske en behandling ud fra væsentlige samfundsinteresser.

Endelig kan det diskuteres, om anvendelsen af verifikationssystemet kan anvendes med samtykke som behandlingsgrundlag, jf. GDPR art. 9, stk. 2, litra a. For at den registrerede kan give et gyldigt samtykke til behandling, kræver det, at samtykket er givet frivilligt, specifikt, informeret og er en utvetydig viljestilkendegivelse af den registrerede, jf. GDPR art. 4, nr. 11. Der kan opstå en problematik for, om samtykket er frivilligt, nu hvor det er den eneste mulighed for at erhverve et billigt pendlerkort og om der reelt findes alternativer i et tilsvarende prisleje, eller om der er ulighed i styrkeforholdet mellem virksomheden og den registrerende.

Virksomheden har monopol på transporten til og fra øen, og et alternativt pendlerkort kan kun erhverves mod en merpris. Endvidere fremgår det af GDPR præambelbetragtning 43, at samtykke til behandling ikke bør anvendes, hvis der foreligger en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed. Alt dette taler for, at der ikke kan indhentes et gyldigt samtykke for behandlingen af biometriske data. EDPB har i deres guidelines [320] præciseret, hvornår der alligevel kan foreligge et samtykke, på trods af at GDPR art. 7, nr. 4 ikke er opfyldt. Der kan således stadigvæk afgives et gyldigt samtykke til behandlingen, hvis der foreligger et alternativ, som ikke indebærer behandlingen af biometriske oplysninger til identifikation og ikke medfører ekstra omkostninger for den registrerede.
Virksomheden har mulighed for at anvende et verifikationssystem, hvortil behandlingsgrundlaget er samtykke, hvis der foreligger et reelt tilsvarende alternativ, som er mindre indgribende. Hvis ikke dette er tilfældet, vil et pendlerkort med krav om biometriske data være ulovligt.

I et spansk fitnesscenter blev der ligeledes anvendt ansigtsgenkendelse som adgangskontrol. Det Spanske Datatilsyn (AEPD) skulle afgøre, om der forelå et gyldigt behandlingsgrundlag hertil.[321]

> Fitnescenterkæden SIDECU S.A. valgte at erstatte deres adgangskontrol fra både at tilbyde identifikation med magnetkort eller fingeraftryk til nu kun at omfatte ansigtsgenkendelse, uden at den registrerede blev informeret herom eller afgav samtykke hertil. AEPD vurderede, at der ikke kunne gives samtykke til ansigtsgenkendelse, hvis der ikke forelå mindre indgribende alternativer.
>
> Ligeledes vurderede AEPD, at fingeraftryk alene som alternativ til ansigtsgenkendelse heller ikke udgjorde et reelt alternativ.

AEPD vurderer, ligesom Datatilsynet, at samtykke ikke kan finde anvendelse til behandling af biometriske data med det formål entydigt at identificere en fysisk person, hvis det ikke er nødvendigt for formålet med behandling, medmindre der foreligger et reelt alternativ, som er mindre indgribende.[322]

[320] EDPB's Retningslinjer 03/2019, s. 14
[321] GDPRhub AEPD (Spain) - EXP202313347
[322] EXP202313347, s 56

SIDECU S.A. begrunder anvendelsen af ansigtsgenkendelse med, at de vil sikre rigtigheden af de personoplysninger, der behandles, fordi de oplever tekniske fejl med det andet system. AEPD konkluderer, at tekniske fejl ikke kan begrunde et mere vidtgående indgreb, men de skal anvende andre foranstaltninger, der løser problemet.[323]
AEPD fastslår, at biometriske data, med det formål entydigt at identificere en fysisk person, kan anvendes som adgangskontrol i fitnesscentre, hvis dets behandlingsgrundlag udgør en væsentlig samfundsinteresse. Dette forudsætter, at der sker en vurdering af de fordele, der følger af foranstaltningen, og at de ikke overstiges af de ulemper, den medfører i forhold til udøvelsen af retten til privatliv. En afgørende faktor for vurderingen er, om der allerede findes foranstaltninger med et lignende eller identisk formål, som skal tages i betragtning, hvorefter den mindst indgribende foranstaltning skal anvendes.[324]

Behandlingsgrundlaget for overvågning kan være samtykke, men hvis der foreligger mindre indgribende alternativer, som den registrerede ikke er blevet præsenteret for, vil der ikke foreligge et gyldigt samtykke.
Ligeledes vil det afgørende for, om GDPR art. 9, stk. 1., finder anvendelse, være om behandlingen sker med henblik på entydig identifikation, hvorfor det er uden betydning, om behandlingen resulterer i et no-hit, da det er formålet, der er det essentielle. Behandling af biometriske data vil derfor i sig selv udgøre et alvorligt indgreb.
Det er essentielt, at der ikke foretages overvågning af de personer, der ikke har afgivet samtykke til behandling af deres personoplysninger, da dette vil medføre, at der fortsat sker en behandling af deres personoplysninger, hvorfor alternativerne derved bliver illusoriske.
I forlængelse af dette skal alternativerne ikke blot være alternativer, men derimod reelle alternativer, da de ikke skal være forbundet med f.eks. lang ventetid eller forøgede omkostninger, da de derved ikke vil udgøre tilsvarende alternativer til ansigtsgenkendelse.
For at sikre, at der foreligger et gyldigt samtykke af den registrerede, kan dette opfyldes ved, at den registrerede hver gang foretager en aktiv handling, før behandlingen finder sted, f.eks. et tastetryk, som aktiverer ansigtsgenkendelsessystemet.

[323] EXP202313347, s. 69
[324] EXP202313347, s. 74

9.3 Fremmødekontrol med ansigtsgenkendelse

Ansigtsgenkendelse har vist sig at være et effektivt værktøj til at identificere registrerede hurtigt og effektivt, hvilket f.eks. ansigtsgenkendelse på fodboldstadioner har vist.[325] Derfor vil det ikke være utænkeligt, at f.eks. en administrativ medarbejder på en uddannelsesinstitution foreslår, at der anvendes et ansigtsgenkendelsessystem, som automatisk registrerer, når elever møder op i klassen. Dette er begrundet i, at formålet er at lette arbejdet med fraværsregistrering, samtidigt med at det sikrer mere præcise data.[326]

En netop sådan sag skulle det Svenske Datatilsyn (Datainspektionen, i 2021 ændret navn til Integritetsskyddsmyndigheten (IMY)) afgøre om anvendelsen af ansigtsgenkendelse på et svensk gymnasium[327] var lovligt.[328]

> Gennem medierne blev IMY gjort opmærksom på, at et svensk gymnasium anvendte ansigtsgenkendelse for at kontrollere fravær i klasserne. Gymnasiet havde indhentet samtykke fra samtlige elever for at behandle biometriske personoplysninger for at identificere deres tilstedeværelse på skolen. Ifølge svensk lovgivning var gymnasier forpligtet til at føre tilsyn med de fremmødte elever, hvorfor formålet med behandlingen var at lette arbejdet med fraværsregistrering.
>
> IMY vurderede, at samtykket fra eleverne ikke var afgivet frivilligt, grundet de reelt ikke havde haft et frit valg samt der forelå en magtubalance mellem gymnasiet og eleverne. Ligeledes vurderede IMY, at behandlingen ikke kunne begrundes i at være nødvendigt af hensyn til væsentlige samfundsinteresser, fordi formålet ville kunne opnås ved mindre indgribende alternativer i elevernes ret til privatliv, på trods af at gymnasiet ved lov var forpligtet til at føre tilsyn med eleverne. IMY konkluderede, at ansigtsgenkendelse var ulovligt, idet gymnasiet ikke havde noget behandlingsgrundlag for at behandle biometriske personoplysninger med det formål at identificere elevernes fravær på skolen.

For det første viser afgørelsen problematikken ved anvendelsen af samtykke som behandlingsgrundlag, jf. GDPR art. 9, stk. 2, litra a, hvis der er magtubalance mellem den registrerede og den dataansvarlige. IMY vælger i den konkrete afgørelse at henvise til GDPR præambelbetragtning nr. 43, der netop uddyber, hvordan det sikres, at samtykket er blevet afgivet frivilligt. På den baggrund skal vurderingen af, om et samtykke er afgivet frivilligt,

---

[325] Samvirke s. 46 f

[326] Tillæg til "Vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne" s. 21

[327] De omhandlende personer der fremgår af afgørelsen er både myndige og umyndige, men IMY har ikke valgt at differentiere muligheden for anvendelsen af samtykke som behandlingsgrundlag.

[328] Integritetsskyddsmyndigheten, REf. no. DI-2019-2221

tillige omfatte en vurdering af forholdet mellem den registrerede og den dataansvarlige. Muligheden for at den registrerede kan afgive et samtykke over for den offentlige aktør, vil ofte være begrænset. I det konkrete tilfælde vurderer IMY, at eleverne er i et tydeligt afhængighedsforhold til gymnasiet med hensyn til karakter, studiemidler, videreuddannelsesmuligheder etc., hvorfor samtykke ikke kan anvendes som behandlingsgrundlag.[329] Den gensidige anerkendelse mellem medlemsstaternes datatilsyn kommer også her til udtryk, ved at vurderingen fra IMY stemmer overens med Datatilsynets og EDPB's vurdering for, hvornår et samtykke ikke er givet frivilligt.[330]

Yderligere behandler IMY, om behandlingsgrundlaget kunne være væsentlige samfundsinteresser, idet den svenske lov kræver, at gymnasiet foretager en fraværsregistrering af eleverne. IMY vurderer, at den svenske lov medfører, at behandling er nødvendig af hensyn til udførelse af en opgave i *samfundets interesse*, hvorfor behandlingen kan finde sted på baggrund af et behandlingsgrundlag i GDPR art. 6, stk. 1, litra e, jf. stk. 3.[331] Derimod vurderer IMY ikke, at fraværsregistreringen udgør en *væsentlig samfundsinteresse* med nationalt supplerende retsgrundlag, hvorfor gymnasiet ikke kan anvende GDPR art. 9, stk. 2, litra g som behandlingsgrundlag for anvendelsen af ansigtsgenkendelse.[332] Yderligere vurderer IMY, at fraværsregistreringen med ansigtsgenkendelse vil være mere omfattende, end hvad der kræves for at opfylde formålet, på trods af, at den er mere sikker og effektiv end de hidtidige metoder. Derfor vil det være i strid med dataminimeringsprincippet, hvorfor det er ulovligt. Derfor skal gymnasiet anvende andre mindre indgribende måder, som f.eks. en manuel håndtering af fraværsregistreringen.[333] Afgørelsen viser, at retten til privatliv vægtes højere, selvom ansigtsgenkendelsen er en mere sikker og effektiv metode for fraværsregistrering end de hidtidige metoder. Netop fordi overvågning kan skabe en følelse af konstant overvågning, hvilket EUD vurderer udgør et vidtgående indgreb i retten til privatliv, kræves det, at nødvendighedskriteriet er opfyldt, hvilket ikke var tilfældet i denne sag. Derfor ville overvågningen også have været i strid med de 4 kumulative betingelser i Chartret art. 52, stk. 1.

---

329 Integritetsskyddsmyndigheten, REf. nr. DI-2019-2221, kap. Samtycke som rättslig grund

330 Christensen & Sørensen, 2024, s. 177f

331 Integritetsskyddsmyndigheten, REf. nr. DI-2019-2221, kap. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse

332 Integritetsskyddsmyndigheten, REf. nr. DI-2019-2221, kap. Känsliga personuppgifter (artikel 9)

333 Integritetsskyddsmyndigheten, REf. nr. DI-2019-2221, kap. Grundläggande principer för behandling av personuppgifter (artikel 5)

Et lignende tilfælde[334] blev forelagt en fransk forvaltningsdomstol, der, ligesom det svenske Datatilsyn, skulle vurdere, om et ansigtsgenkendelsessystem kunne implementeres på skolen.[335]

> Regionen Provence-Alpes-Côte d'Azur (PACA) havde autoriseret et ansigtsgenkendelsessystem, der skulle kontrollere samt sikre sikkerheden i to gymnasier. Dette blev dog aldrig implementeret, men dette medførte ikke, at retten derfor ikke ville vurdere, hvorvidt ansigtsgenkendelsessystemet var gyldigt. Herefter skulle den franske ret vurdere, hvorvidt der forelå et gyldigt samtykke. Dernæst skulle den franske forvaltningsdomstol vurdere, om ansigtsgenkendelsessystemet var gyldigt efter væsentlige samfundsinteresser. Ansigtsgenkendelsessystemet ville blive sat op ved gymnasiernes indgange, og ville både behandle elevernes samt besøgendes særlige kategorier af personoplysninger. Formålet med systemet var at identificere identitetstyveri samt uønskede bevægelsesmønstre. Ansigtsgenkendelsessystemet angik derfor ikke blot identifikation til adgangskontrol, men også bevægelsessporing. Forvaltningsdomstolen konkluderede, at behandlingen udgjorde hverken et gyldigt samtykke eller en væsentlig samfundsinteresse.

Indledningsvist pointerer retten, at ansigtsgenkendelsessystemet behandler biometriske data, hvilket forudsætter et gyldigt behandlingsgrundlag, før disse oplysninger kan behandles. Derudover er det ikke regionen, men derimod skolerne, der har autoritet til at implementere et sådant ansigtsgenkendelsessystem, hvorfor regionen overskrider sine beføjelser, idet tilsyn og overvågning af eleverne ikke falder ind under regionens beføjelser. Dette er derimod beføjelser, der er underlagt skolen.[336] Forvaltningsdomstolen adresserer dog alligevel, hvorvidt indgrebet udgør et gyldigt behandlingsgrundlag. I henhold til GDPR art. 4, nr. 11, skal samtykke bl.a. være frivilligt afgivet, hvilket ikke var tilfældet i denne sag, da der foreligger et ulighedsforhold mellem skolen og eleverne, hvorfor samtykke var ugyldigt.[337]

Formålet med behandlingen af de særlige kategorier af personoplysninger var at hjælpe personalet, der skulle kontrollere adgangen til skolen, effektivisere kontrollen samt forhindre identitetssvindel og opdage uønskede bevægelser. Ingen af disse formål udgør væ-

[334] De omhandlende personer, der fremgår af afgørelsen, er både myndige og umyndige, men den franske forvaltningsdomstol har ikke valgt at differentiere mellem disse gruppers muligheder for anvendelsen af samtykke som behandlingsgrundlag.

[335] GDPRhub TA Marseille - N°1901249.

[336] GDPRhub TA Marseille - N°1901249, præmis 8

[337] GDPRhub TA Marseille - N°1901249, præmis 12

sentlige samfundsinteresser. I denne forbindelse har regionen tillige ikke godtgjort, at formålet kunne nås med mindre indgribende alternativer, herunder f.eks. adgangskort og videoovervågning.[338] Der foreligger derfor ikke en væsentlig samfundsinteresse, der kan medføre, at forbuddet i GDPR art. 9, stk. 1, fraviges.

Det kan på baggrund af ovenstående retspraksis derfor fastslås, at vurderingen af om et samtykke kan anses for frivilligt afgivet, beror på, om der foreligger en magtubalance mellem den registrerede og den dataansvarlige, hvilket typisk vil foreligge, når der er tale om forholdet mellem en skole og dens elever. , Dette da eleverne er i et tydeligt afhængighedsforhold til skolerne med hensyn til karakter, studiemidler og videreuddannelsesmuligheder.
Derudover kan fraværsregistrering ikke udgøre væsentlige samfundsinteresser, selvom dette ville øge effektiviteten af frarværsregistreringen. I forlængelse af dette kan det heller ikke udgøre væsentlige samfundsinteresser, at effektiviteten ved adgangskontrollen bliver øget ved ansigtsgenkendelsessystemet, hvilket igen fastslår, at siden privatlivet vægtes højt, skal indgrebet begrænses til det strengt nødvendige.
Ligeledes tillægges det en vis værdi i vurderingen af, om et samtykke er gyldigt, om der foreligger mindre indgribende alternativer, såsom adgangskort og videoovervågning, idet en mangel på alternativer vil indikere et ufrivilligt samtykke.

[338] GDPRhub TA Marseille - N°1901249, præmis 13

10. Konklusion

Dette speciale har undersøgt, hvornår overvågning, der behandler biometriske data med det formål entydigt at identificere den registrerede (biometrisk overvågning), kan legitimeres i henhold til Chartret og Databeskyttelsesretten.

Retten til privatliv er en grundlæggende rettighed, som beskyttes af Chartret indenfor EU-retten anvendelsesområde, men det er ikke en absolut rettighed. Derfor kan der foretages indgreb heri, hvis indgrebet opfylder de 4 kumulative betingelser i undtagelsesbestemmelsen, der fremgår af Chartrets art. 52, stk. 1. Indledningsvis skal indgrebet have hjemmel i lov. Dernæst skal indgrebet respektere det væsentligste indhold af rettighederne i Chartret. Derudover skal indgrebet forfølge et mål af almen interesse, der er anerkendt af Unionen. Slutteligt skal indgreb være begrænset til det nødvendige.

Det følger af EUD's praksis, at undtagelsesbestemmelsen er af afgørende betydning, når det skal vurderes, om der foreligger et legitimt indgreb i retten til privatliv, så den registrerede har mulighed for at vurdere rækkevidden af et muligt indgreb. Det indebærer, at reglerne skal udformes, så det ikke overlades til myndighederne at fastlægge rækkevidden af indgrebet gennem et ubegrænset skøn. Særligt vigtig i denne sammenhæng er proportionalitetsprincippet, hvoraf det følger, at behandling alene må ske, hvis den er begrænset til det strengt nødvendige for at opnå det legitime formål. I denne vurdering inkluderes det, om mindre indgribende alternativer kan anvendes. Alternativerne skal endvidere udgøre reelle alternativer, hvorfor de ikke må være forbundet med ekstra ulemper for den registrerede, f.eks. begrænset adgang eller meromkostninger, hvorved de anførte alternativer vil blive illusoriske. Yderligere indgår der et krav om opbevaringsbegrænsning i vurderingen, hvilket sikrer at personoplysninger kun opbevares i det nødvendige tidsrum. Der skal foretages en løbende revurdering af om gyldigheden for opbevaringen fortsat forfølger formålet med behandlingen.

For at der kan foretages overvågning, der behandler biometriske data med det formål at identificere en fysisk person, er der forskellige fremgangsmåder, hvorpå det legitimeres i henhold til chartret og databeskyttelsesretten. Indledningsvist følger det af GDPR art. 9, stk. 1, at denne type overvågning udgør en behandling af den særlige kategori af personoplysninger, hvorfor det udgør et alvorligt indgreb i retten til privatliv. De behandlingsgrundlag, der er undersøgt i specialet, er væsentlige samfundsinteresser og samtykke, som muliggør biometrisk overvågning under bestemte forudsætninger.

Ved anvendelsen af væsentlige samfundsinteresser som behandlinsgrundlag, er der tilknyttet krav, før dette kan legitimeres, jf. GDPR art. 9, stk. 2, litra g. For det første skal behandlingen være nødvendig af hensyn til væsentlige samfundsinteresser, hvilket antages at kunne rummes inden for Chartrets mål af almen interesse. De analyserede afgørelser viser, at det er den dataansvarlige, der skal bevise, at behandlingen er nødvendig af hensyn til en væsentlig samfundsinteresse. Heri ligger der et krav om, at behandlingen netop er en *væsentlig* samfundsinteresse, hvorfor en almindelig samfundsinteresse ikke vil være tilstrækkelig. Det vil altid være en konkret vurdering, om interessen er væsentlig og heri indgår elementer såsom sikkerhedsbehov, formålets samfundsmæssige betydning, indgrebets påvirkning i forhold til målet samt problemets alvor og omfang. Derudover skal indgrebet stå i rimeligt forhold til det forfulgte formål, og respektere det væsentligste indhold af retten til databeskyttelse, hvilket udtrykker et nødvendighedskrav. I denne vurdering indgår det, om behandlingen er tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til det forfulgte behandlingsformål. Slutteligt skal der foreligge en klar og præcis aktiveringslov, der sikrer passende og specifikke foranstaltninger. Herved vil betingelserne for Chartrets art. 52, stk. 1 være opfyldt, hvorfor et indgreb kan legitimeres.
Den danske aktiveringslov fremgår af DBL § 7, stk. 4., hvorefter ikke-offentlige databehandlere skal have tilladelse til biometrisk overvågning. Bestemmelsens ordlyd er bred, hvorfor det er uklart, om loven er tilstrækkelig specifik for at sikre de fornødne garantier.
Det andet behandlingsgrundlag er udtrykkeligt samtykke, jf. GDPR art. 9, stk. 2, litra a. Dette behandlingsgrundlag stiller bl.a. krav til, at samtykket er frivilligt afgivet. Samtykke anses ikke for frit afgivet, hvis der er magtubalance mellem den dataansvarlige og den registrerede, f.eks. hvis der er tale om forholdet mellem en skole og dens elever. Ligeledes er det ikke muligt at anvende samtykke som behandlingsgrundlag ved en nødvendig ydelse, der anses som alment behov, og hvor der ikke foreligger et alternativ. Derudover skal samtykke også opdeles i henhold til hver af de foretagne behandlingsaktiviteter. Hvis behandlingen ikke er nødvendig for at forfølge formålet, skal der foreligge mindre indgribende alternativer, før der kan afgives et samtykke. Alternativerne skal være reelle, hvilket er i overensstemmelse med Chartrets art. 52, stk. 1.

Retten til privatliv er således til hinder for, at der kan anvendes biometrisk overvågning, medmindre der foreligger et gyldigt behandlingsgrundlag. Den teknologiske udvikling og mulighederne for biometrisk overvågning indebærer dog en stigende udfordring af

Chartret og databeskyttelsesretten, hvorfor det er nødvendigt med effektive regulering, der sikrer at retten til privatliv ikke udhules i takt med den teknologiske udvikling.

11. Litteraturliste

11.1 Lovregister

AI-Act: Forordning (EU) 2024/1689 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens)

Chartret: CHARTER OM GRUNDLÆGGENDE RETTIGHEDER af 2012/C 326/02

DBL: Lovbekendtgørelse nr. 289 af 08/03/2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

ePrivacy-direktivet: Direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved direktiv 2009/136/EF

EMRK: Lovbekendtgørelse nr. 138 af 26/01/2022 om Den Europæiske Menneskerettighedskonvention

Folkeskoleloven (Historisk**)**: Lovbekendtgørelse nr. 1086 af 15. august 2023 om Lov om folkeskolen (Folkeskoleloven)

GDPR: Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF

Hooliganloven: Lovbekendtgørelse nr. 1216 af 27/10/2015 om sikkerhed ved bestemte idrætsbegivenheder med senere ændringer

Logningsdirektivet: Direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF

Pasfordningen: Forordning (EF) nr. 2252/2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, som ændret ved Forordning (EF) nr. 444/2009

Persondatadirektivet: Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Persondataloven (Historisk): Lov nr. 429 af 31/05/2000 om behandling af personoplysninger med senere ændringer

Retshåndhævelsesdirektivet: Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med

henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA

Retshåndhævelsesloven: Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer

Serviceloven (Historisk**)**: Lovbekendtgørelse nr. 1089 af 16/08/2023 om social service

TEU: Konsoliderede udgaver af traktaten om den Europæiske Union 2008/C 115/01

TEUF: Traktaten om den Europæiske Unions funktionsmåde 2008/C 115/01

TV-overvågningsloven: Lovbekendtgørelse nr. 182 af 24/02/2023 om lov om tv-overvågning med senere ændringer

11.2 Litteratur

Blume, P. (2018) *Databeskyttelsesret* (5. udg.) Djøf Forlag

Blume, P. (2020) *Tv-overvågningsloven med kommentarer* (2. udg.) Jurist- og Økonomforbundets Forlag

Blume, P., Hermann, J., R. (2018) *Ret, privatliv og teknologi.* (4. udg.) Jurist- og Økonomforbundets Forlag

Bønsing, S. (2023) *Almindelig Forvaltningsret.* (5. udg.) Djøf Forlag

Bønsing, S., Elholm, T., Jakobsen, S., S., & Lentz, L., W. (red.) (2018) *I forskningens og formidlingens tjeneste - festskrift til professor Lars Bo Langsted.* (1. udg). Ex Tuto Publishing

Christensen, T. K. (2021). *Digital overvågning: Lovgivningens grænser i et menneskeretligt krydsfelt.* (1. udg.) DJØF Forlag.

Christensen, T. K., & Sørensen, M. J. (red.) (2024). *Samtykke*. (1. udg.) Ex Tuto Publishing.

Christoffersen, J., Christensen, L., H., Madsen, L., L., Storgaard, L., H., Skovgaard-Petersen, H., & Ventegodt, M. (2018) *EU's Charter om Grundlæggende Rettigheder med kommentarer*. (2. udg.) Jurist og Økonomforbundets Forlag

Ersbøll, E. (2016) *EU's Charter i et menneskeretligt krydsfelt.* (1. udg.) Jurist- og Økonomforbundets Forlag

Evald, J. (2023) *At tænke juridisk.* (6. udg.) Djøf Forlag.

Hamer, C. R., & Schaumburg-Müller, S. (2020) *Juraens verden - Metoder, retskilder og discipliner.* (1. udg.) Djøf Forlag

Hervey, T., Kenner, J., Peers, S., & Ward, A (2014) *The EU Charter og Fundamental Rights - A Commentary.* (First published 2014, Reprinted in 2019) Bloomsbury Publishing

Jakobsen, S., S., Andersen, M., M., Hartfield-Traun, D., Mortensen, B., O., G., & Sørensen, M., G. (2021) *Informationssikkerhedsret.* (1. udg.) Ex Tuto Publishing

Jasserand, C. (2022), *Biometric Data, Within and Beyond Data Protection*. University of Groningen, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4483962
Knobel, D., Udsen, H. (2025) *Almindelig Databeskyttelsesret.* (1. udg.) København: Ex Tuto Publishing
Motzfeldt, H., Næser, J. (2025) *Databeskyttelsesret.* (2. udg.) Djøf Forlag
Munk-Hansen, C. (2022) *Retsvidenskabsteori.* (3. udg.) Djøf Forlag
Neergaard, U., & Nielsen, R. (2024) *EU-ret* (9. udg.) Karnov Group Denmark
Nielsen, K., & Lotterup, A. (2025) *Databeskyttelsesforordningen og databeskyttelsesloven*. (2. udg.) Djøf Forlag
Nielsen, R., & Tvarnø, D. (2021) *Retskilder og retsteorier* (6. udg.) Djøf Forlag
Orwell, G. (1949) *1984.* (11. udg.) Gyldendal
Spiecker gen. Döhmann, I. Papakonstantinou, V., De Hert, P., & Hornung, G. (2023) *General Data Protection Regulation: Article-by-Article Commentary.* (bind 1) Nomos Verlagsgesellschaft
Trzaskowski, J., (red) Bergqvist, C., Jakobsen, S., Karstoft, S., Kirk, H., Lentz, L., Riis, T., Sørensen, M. (2024) *Internetretten.* (4. udg.) Ex Tuto Publishing
Trzaskowski, J., & Sørensen, M. (2022) *GDPR COMPLIANCE Understanding the General Data Protection Regulation.* (2. udg.) Ex Tuto Publishing
Trzaskowski, J. (2021) *Your Privacy Is Important to Us!- Restoring Human Dignity in Data-Driven Marketing.* (1. udg.) København: Ex Tuto Publishing

11.3 Lovforarbejder og betænkninger

Betænkning nr. 1565/2017 *Betænkning om Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning*

Lovforslag L 38 Forslag til lov *om sikkerhed ved bestemte idrætsbegivenheder*. Folketinget 2007-08 2-samling, 12. oktober 2007.

Lovforslag L 68 om *supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger* (databeskyttelsesloven), Folketinget 2017-18, 25. oktober 2017

11.4 Artikler

Andersen, K. B. H. (2023). *En fælles databeskyttelsesret: Betydningen af europæiske medlemsstaters praksis i dansk databeskyttelsesret*. UfR 2023B.51.

Samvirke (April 2026) *Vis mig dit ansigt* https://samvirke.dk/magasin/april-2026#magazine/

Bertelsmann Foundation (2016) Newpolitik: Echoes of History: Understanding German Data Protection af Alvar C.H. Freude og Trixy Freude https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Publication_Newpolitik_BFNA_2016.pdf

First Response Group (2024) *How Technology Advances Security in the Modern Age* https://issuu.com/firstresponsegroup/docs/how_technology_advances_security_in_the_modern_age?utm_medium=referral&utm_source=www.firstresponsegroup.com

11.5 Domme

EU-domme

CILFIT, C-283/81, EU:C:1982:335
Kommissionen mod Danmark, C-143/83, EU:C:1985:34
Casa Fleischhandels, C-215/88, EU:C:1989:331
Digital Rights Ireland m.fl., de forenede sager C-293/12 og C-594/12, EU:C:2014:238
Ryneš C-212/13, EU:C:2014:2427
Google Spain og Google, C-131/12, EU:C:2014:317
Schwarz, C-291/12, EU:C:2013:670
Tele2 Sverige m.fl., de forenede sager C-203/15 og C-698/15, EU:C:2016:970
Ministerio Fiscal, C-207/18, EU:C:2018:788
La Quadrature du Net m.fl., de forenede sager C-511/18, C-512/18 og C-520/18, EU:C:2020:791
TU og RE mod Google, C-460/20, EU:C:2022:962

Ugeskrift for Retsvæsen

UfR.2022.2162 H

11.6 Administrativ praksis

Praksis fra Datatilsynet **Praksis fra Integritetsskyddsmyndigheten**

Datatilsynets j.nr. 2003-212-0143
Datatilsynets j.nr. 2018-51-0332
Datatilsynets j.nr. 2018-211-0135
Datatilsynets j.nr. 2019-31-1650
Datatilsynets j.nr. 2021-431-0145
Datatilsynets j.nr. 2022-51-0375
Datatilsynets j.nr. 2023-31-0028
Datatilsynets j.nr. 2023-211-0004
Datatilsynets j.nr.: 2023-212-0015
Datatilsynets j.nr. 2023-431-0001
Datatilsynets j.nr. 2024-51-0012
Datatilsynets j.nr. 2024-51-0014

Integritetsskyddsmyndigheten, REf. no. DI-2019-2221

Praksis fra GDPRHub
GDPRhub TA Marseille - N°1901249.
GDPRhub AEPD (Spain) - 0098/2022
GDPRhub AEPD (Spain) - EXP202313347

11.7 Vejledninger og Udtalelser

EDPB Udtalelse 11/2024 om anvendelse af ansigtsgenkendelse til at strømline passagerstrømmen i lufthavne (forenelighed medart. 5, stk. 1, litra e) og f), samtart. 25 og 32 i GDPR)

EDPB Retningslinjer 05/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet

EDPB Retningslinjer 05/2020 vedrørende samtykke i henhold til forordning 2016/679

EDPB Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger

Børne- og Undervisningsministeriet, Styrelsen for It og Læring, (December 2025) Tillæg til "Vejledning om lovlig brug af kunstig intelligens for uddannelsesinstitutionerne"