# OVERFØRSEL AF PERSONOPLYSNINGER TIL USIKKERT TREDJELAND

KANDIDATSPECIALE VED AALBORG UNIVERSITET

ASBJØRN VOLLMER JEPPESEN

19. maj 2022

# Titelblad

**Universitet:** Aalborg Universitet

**Uddannelse:** Jura

**Opgave:** Kandidatspeciale

**Fagområde:** GDPR

**Dansk titel:** Overførsel af personoplysninger til usikkert tredjeland

**Engelsk titel:** Transfer of personal data to unsecure third countries

**Forfatter:** Asbjørn Vollmer Jeppesen (studie nr. 20173058)

**Vejleder:** Marie Jull Sørensen

**Afleveringsdato:** 19. maj 2022

**Antal anslag:** 133.420

# Indholdsfortegnelse

# Abstract

In an increasingly globalized world where participation in the digital world is largely becoming a necessity in much of the world, data – particularly personal data – and the access thereto and protection thereof, is simultaneously becoming of increasing importance in the legal community. The European Union (hereinafter, 'EU') is a frontrunner in this field with its General Data Protection Regulation (hereinafter, 'GDPR'). However, as the world is globalizing, data is not only transferred within one region's territory, but also across borders. Therefore, the transfer of data to third countries, namely countries outside of the EU, must also be considered within the legal framework dealing with personal data.

When transferring data to third countries, one must differentiate between what the European Commission has deemed secure and unsecure third countries, respectively. Such categorization is based on an adequacy decision and whether the national laws of the respective third country provide a level of protection comparable to EU law. As a result, the transfer of data to unsecure third countries, where such comparable level is not provided, is greatly important. However, this is often not an aspect of GDPR of great focus, thus the present contribution aims to provide an assessment of such.

According to EU law, the processing of personal data must always adhere to fundamental principles of transparency, legitimate purpose, and proportionality. The principle of proportionality is, for the purposes of the present contribution, considered as fundamental to ascertain with respect to the processing of personal data. The responsible for this lies with the data controller. This principle will be dealt with through the lens of unsecure third countries and via a comparative analysis of selected EU case law, particularly Schrems II and La quadrature du net.

Additionally, in 2021, the European Data Protection Board (hereinafter, 'EDPB') adopted its finalized recommendations on supplemental transfer tools ensuring GDPR-compliance in data transfers to third countries. Such recommendations will also be considered in view of the aforementioned EU case law. Finally, the concept of consent will be dealt with in connection to the transfer of personal data to insecure third countries.

The findings of the present paper are largely threefold. Firstly, for the data controller to make a qualified determination concerning what measures to implement, a deep understanding of the legislation

pertaining to data of the unsecure third country, as well as the EU legislation and case law, is necessary. Secondly, the comparative analysis showed that the threshold for the principle of proportionality laid out in Schrems II was more restrictive than that of La quadrature du net and that data controllers, in future EU cases, ought to rely on La quadrature du need when assessing unsecure third countries legislation. Thirdly, when it comes to transferring personal data to unsecure third countries and where public authorities have access to such data, consent does not make the transfer permissible. Overall, this paper tackles a balancing act between the protection of personal data and the freedom to exchange personal data in regards to trade. The findings show that when it comes to unsecure third countries, the former, namely the protection of personal data, outweighs the latter, meaning the freedom to exchange such.

# 1. Introduktion

Internettet gjorde for alvor sit indtog i verden i løbet 1990'erne og blev indledningsvis hovedsageligt brugt af forskere i forbindelse med analyser og til deling af data[1]. I dag anslås at 3,739 milliarder mennesker til daglig har adgang til internettet,[2] og i Danmark er 95 % af befolkningen mellem 16-74 år på internettet dagligt[3].

Den digitale verden har udviklet sig markant siden 1999, hvor den daværende direktør i Pengeinstitutternes Betalingsservice (PBS) Peter Max sendte en buket blomster via internettet til den daværende erhvervsminister Pia Gjellerup[4], til nu, hvor danskere i første halvår af 2021 har købt for 93,8 mia. kr. online[5].

I 2016 blev den nationale platform sundhed.dk, hvor alle sundhedsoplysninger kan tilgås etableret. Det var dengang det største statslige it-projekt, og det blev udarbejdet i samarbejde med den amerikanske softwareleverandør Epic[6]. I dag foregår al kommunikation med offentlige myndigheder via digitale løsninger som Digital Post, Kørekort-app, Sundhedskort-app, Borger.dk, NemID – listen er lang, og medmindre borgeren er fritaget fra at modtage digital post, hvilket 338.000 borgere er pr. marts 2022[7], modtager alle andre danske borgere al offentlig post digitalt.

Alle disse handlinger efterlader et digitalt fodspor, der alle skal opbevares på datacentre. Disse digitale fodspor og indeholder alle personoplysninger, både som enkeltstående data og ved automatisk og manuel sammenføring. De kan spores tilbage til den enkelte person, både til gavn og skade for borgerne.

Med andre ord er både borgere, virksomheder og offentlige institutioner afhængige af at kunne bruge personoplysninger i forskellige sammenhæng.[8] Dette behov skaber grundlag for en hensynsafvejning mellem retten til det private liv, som er sikret i Den Europæiske Menneskerettighedskonventions art.

---

[1] https://www.skjoldby.com/www-historie/, tilgået den 17.05.2022
[2] https://www.netkablet.dk/internet-sociale-medier-youtube-facebook-saa-meget-ser-vi/, tilgået den 17.05.2022
[3] https://www.dst.dk/da/Statistik/nyheder-analyser-publ/Publikationer/VisPub?cid=39431, tilgået den 17.05.2022
[4] https://samvirke.dk/artikler/dankortets-historie, tilgået den 17.05.2022
[5] https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2021/september/e-handelsanalysen-forbruget-pa-nettet-vokser-markant-og-slar-ny-rekord/, tilgået den 17.05.2022
[6] https://www.regionh.dk/presse-og-nyt/pressemeddelelser-og-nyheder/Sider/Sundhedsplatformen-i-luften.aspx
[7] https://digst.dk/tal-og-statistik/, tilgået den 17.05.2022
[8] Udsen, *It-Ret*, 2021, 5 udgave, s 262

8, og den absolutte nødvendighed af at kunne behandle personoplysninger for at kunne opretholde den verden, som vi alle lever i idag.

I dette krydsfelt af hensyn indførte den Europæiske Union (EU) den 27. april 2016 lovgivning om General Data Protection Regulation og lovgivningen trådte i kraft i alle medlemslande 25. maj 2016[9] Formålet med lovgivningen var at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder og samtidig skulle lovgivningen ikke udgøre en indskrænkning af den frie udveksling af personoplysninger på tværs af landegrænser[10].

Dette giver åbenlyse problemer for dataansvarlig og databehandler, i særdeleshed når personoplysninger ikke holdes inden for unionens grænser. Ofte deles personoplysninger med lande uden for EU's grænser, eftersom globaliseringen fortsat er i udvikling, både i forhold til samhandel og informationsudveksling[11]. Yderligere er USA, Kina og Indien de største outsourcing-lande i verden[12].

Problematikken er yderligere tydeliggjort ved den meget omtalte Schrems I fra 16. okt. 2015, der underkendte brugen af overførselsgrundlaget Safe Harbour. Schrems II fra den 16. juli 2020, underkendte brugen af det nyindførte overførselsgrundlag Privacy Shield. Dette fik stor praktisk betydning, da disse ordninger ikke kunne anses som at være tilstrækkelige for at sikre den registreredes rettigheder og herved ikke at opfylde EU´s krav til beskyttelsesniveauet[13].

I medfør heraf skal datasvarlig foretage meget komplekse vurderinger af dels, hvilket overføringsinstrument der skal anvendes til overførsler til usikkert tredjeland og dels herefter i særdeleshed foretage en vurdering af de tekniske supplerende foranstaltninger for at sikre et *"tilstrækkeligt niveau for beskyttelse af personoplysninger"*.

[9] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_da, tilgået den. 17.05.2022
[10] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 1
[11] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel nr. 101
[12] Udsen, *It-Ret*, 2021, 5 udgave, s 397
[13] https://www.moch360.com/da/schrems-ii/ , tilgået den 01. april .2022

# 2. Problemformulering

Med baggrund i overstående introduktion er dette speciales hovedformål at klarlægge, hvilke væsentlige hensyn dataansvarlig skal iagttage i forbindelse med at overføre personoplysninger til usikkert tredjeland. Dette vil ske med naturligt afsæt i EU-baggrundsretten, samt ved analyse af relevante artikler i forordningen, vejledninger og retspraksis.

Sluttelig vil mulighederne for brug af samtykke i forbindelse med overførsel af personoplysninger analyseres og diskuteres.

Det overordnede analyseobjekt for dette speciale kan sammenfattes således:

Overførsel af personoplysninger til usikkert tredjeland.

# 3. Struktur

Dette afsnit skal indledningsvis klarlægge, hvorledes læseren af denne fremstilling skal tages igennem de forskellige afsnit, samt opbygningen af disse afsnit. Desuden skal afsnittet klarlægge generelle forhold, der giver læseren de bedste forudsætninger for forståelsen af dette speciale.

Helt overordnet kan specialet inddeles i seks hovedkategorier:

1. del omhandler de metodiske overvejelser samt fornødne afgrænsninger, specialet gør brug af, og samtidig fastlægges kernebegreber, som vil blive anvendt i løbet af de følgende afsnit.

2. del fastlægger, hvad udgangspunktet er for overførsel til usikkert tredjeland, og hernæst vil dette afsnit beskæftige sig med, under hvilke forudsætninger der kan ske overførsel til usikkert tredjeland.

3. del vil igennem komparativ analyse af Schrems II (16. juli 2020) og La quadrature du net c-511/18 konkretisere proportionalitetsprincippet i databeskyttelsesoptik.

4. del vil med afsæt i supplerende foranstaltninger fastslå effektiviteten af tekniske supplerende foranstaltninger set i lyset af Schrems II og La quadrature du net c-511/18.

5. del vil afdække mulighederne for samtykke i forbindelse med overførsel af personoplysninger til usikkert tredjeland.

6. del vil afslutningsvis konkludere, hvilke væsentligt hensyn databehandle skal iagttage i forbindes med overførsel af personoplysninger til usikkert tredjeland.

# 4. Specialets terminologi

## 4.1 Charteret

Gennem denne fremstilling vil der grundet læsevenlighed anvendes terminologien Charteret: forordningen i forskellige bøjningsformer, og såfremt andet ikke fremgår af teksten, refererer dette til Den Europæiske Unions Charter om grundlæggende rettigheder 2012/C 326/.

## 4.2 Citater

Når specialet anvender direkte citater, vil disse fremhæves, således at citatet omsluttes af apostrof og kursiveres. Hvis det ikke fremgår tydeligt i teksten, hvor der citeres fra, vil der blive anvendt fodnote.

## 4.3 General Data Protection Regulation

General Data Protection Regulation (GDPR) vil i dette projekt grundet læsevenlighed benævnes som forordningen i forskellige bøjningsformer, og såfremt andet ikke fremgår af teksten, refererer dette til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

## 4.4 Lovhenvisninger

Ved henvisninger til lovtekst vil der, første gang lovteksten anvendes, entydigt defineres, hvilken lovtekst der refereres til, herefter, såfremt samme lovtekst anvendes flere gange i den følgende tekst, og det entydigt kan udledes af læseren, at der er tale om samme lovtekst, vil der udelukkende refereres til artikel xx, paragraf xx eller præambel xx.

## 4.5 Territoriel specificering

Når der i denne fremstilling henvises til europæiske, EU eller lignende indre grænser, refererer det til EU-medlemslandene, Island, Norge og Liechtenstein, som udgør Det Europæiske Økonomiske Samarbejdsområde (EØS)[14] og Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Storbritannien og Uruguay, som alle er sikre tredjelande[15].

[14] EDPB, *Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger*, Version 2.0, Vedtaget den 18. juni 2021, s. 28
[15] Datatilsynet, *Vejledning Overførsel af personoplysninger til tredjelande*, juli 2021, 3. udgave, s. 13

# 5. Afgrænsning

Specialet har til formål at fastlægge, hvilke væsentlige hensyn dataansvarlig skal iagttage i forbindelse med at overføre personoplysninger til usikkert tredjeland. Derfor vil specialet kun gå i dybden med udvalgte bestemmelser, retspraksis og litteratur.

Til trods for at specialet kun vil beskæftige sig med udvalgte bestemmelser i forordningen samt Charteret, bliver disse nødvendigvis ikke gennemgået udtømmende eller udførligt, men vil blive analyseret, systematiseret og vurderet ud fra det afgrænsede fokusområde og med fokus på at skabe de bedste forudsætninger for et videnskabeligt speciale. Dette tillader samtidig, at med de udvalgte bestemmelser er der mulighed for en mere dybdegående og fyldestgørende besvarelse på det overordnede spørgsmål.

Yderligere er området for overførsel af personoplysninger særligt præget af meget tekniske og komplekse it-løsninger, som varierer alt efter tredjelandenes lovgivning, og praksis i forbindelse med håndtering af personoplysninger. Det vil ligge uden for specialets rammer at beskæftige sig med alle disse variabler, og derfor vil specialet fortrinsvis beskæftige sig med lovgivning, hvor myndigheder kan pålægge dataimportøren at udlevere personoplysninger på europæiske borgere.

På grund af den ovenstående afgrænsning er det uundgåeligt, at der er øvrige emner, som ville være nærliggende at beskæftige sig med helt eller delvist for at opnå en bredere og mere fyldestgørende beskrivelse af retstilstanden. Hertil kan følgende emner nævnes: samtykkeerklæringer fra umyndige, dataoverførsel til sikre tredjelande, korrekt behandlingsgrundlag.

# 6. Retsdogmatisk metode

Specialet vil beskrive de gældende retsregler (de lega lata)[16] for at kunne klarlægge, hvilke væsentlige hensyn dataansvarlig skal iagttage i forbindelse med overførelse af personoplysninger ud af EU. Såfremt der ikke fremgår andet, vil den retsdogmatiske metode anvendes, hvorved beskrivelse, analyse og systematisering[17] bruges til fastlægning af de gældende retsregler.

Specialets retskildedefinition følger det traditionelle retskildehierarki: grundloven, Folketingets lov/ EU-forordninger[18], retspraksis, sædvaner og forholdets natur[19]. De skrevne retsregler følger lex superior-princippet, hvilket betyder at de underliggende retsregler naturligt har et hjemmelskrav opad i hierarkiet[20].

## 6.1 Retskildevurdering

### 6.1.1 Den Europæiske Unions Charter om grundlæggende rettigheder

Charteret er ikke underlagt traktaterne, men skal anses for at have samme juridisk værdi som traktaterne, jf. TEU's art. 6, 1. Charteret er som udgangspunkt retlig bindende over for medlemsstaterne, jf. Charterets art. 51, 1. Retspraksis har ved flere tilfælde tilladt, at private kunne påberåbe bestemmelser i Charteret, og yderligere har EU-domstolen fastslået, at Charterets art. 21, art 31, 2 og art 47 kan påberåbes horisontalt og herved af private[21]. For denne fremstilling er særlig Charterets art. 7, art 8, art 47 og art 52 relevant for det overordnede analyseobjekt.

### 6.1.2 Forordningen

Det følger af TEUF's art. 288, 2, at forordninger er "*almengyldige og bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat*". Forordninger skal sikre, at alle medlemslande har ens lovgivning på et specifikt område, og de skal ses som en del af gældende ret i hvert enkelt medlemsland. Derfor er der en snæver tilgang for medlemslandene i forhold til at udfylde eller fortolke på forordningens bestemmelser, og der skal ikke foretages nogen gennemførselsforanstaltninger, før

[16] Munk-Hansen, *Den juridiske løsning,* 2 udgave, 2021, s. 11
[17] Madsen, *Retsdogmatisk forskning 2022*, Build 20211228 s. 2
[18] Munk-Hansen, *Den juridiske løsning,* 2 udgave, 2021, s. 24
[19] Munk-Hansen, *Den juridiske løsning,* 2 udgave, 2021, s. 15
[20] Tvarnø og Nielsen, *Retskilder og retsteorier,* 6 udgave, 202, s. 35
[21] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 185

forordningen er gyldig.[22] Som beskrevet i tidligere afsnit trådte GDPR forordningen nr. 2016/679 af 27. april 2016, i kraft i alle EU´s medlemslande den 25. maj 2018. Det fremgår af art. 1, at det er en forordning, hvorfor lovgiveren har ønsket, at lovgivningen skal være identisk, altså en "totalharmonisering" i alle medlemslandene. Dette giver medlemslandene en meget indskrænket mulighed for at fortolke ud fra et nationalt perspektiv[23]. Det fremgår af art. 51,1, at der nationalt skal oprettes en tilsynsmyndighed, i Danmark er dette Datatilsynet, som vil blive behandlet i nedenstående afsnit. Forordningen er den primære retskilde i specialet og tillægges den retskildeværdi.

I denne fremstilling behandles retspraksis afsagt på basis af Direktiv 95/46 (databeskyttelsesdirektivet), som blev erstattet af forordningen. Direktivet anses derfor for at være henvisning til forordningen, jf. forordningens art. 94, 2. Det følger af TEUF's art. 288, 3, at "Et direktiv er med hensyn til det tilsigtede mål bindende for enhver medlemsstat, som det rettes til, men overlader det til de nationale myndigheder at bestemme form og midler for gennemførelsen."[24].

### 6.1.3 Præambel

Dette er et fortolkningsbidrag[25], som ikke er bindende, jf. TEUF's art. 288, 5. Derfor kan private ikke påberåbe sig en ret, som er fremført i en præambel. Gennem domstolspraksis udviklet en praksis, hvor EU-domstolen og nationale domstole skal tage hensyn til præambelbidrag[26]. I den første del af GDPR er der opgivet 173 præambelbetragtninger. Disse kan sidestilles med de danske lovforarbejder. Disse betragtninger bidrager som et nødvendigt fortolkningsbidrag til forordningens artikler. Præambelbetragtningerne giver indsigt i, hvad den endelige grundtanke er, og hvilket beskyttelsesbehov lovgiver ønsker at ramme med de forskellige artikler, samt giver en nærmere forståelse der kan anvendes som fortolkningsbidrag [27] [28]. Disse præambelbidrag vil i specialet tillægges en betragtelig retskildeværdi.

[22] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 104-105
[23] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 92
[24] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 105
[25] Blume, *Den nye persondatarets aktører,* 1 udgave, 2018, s. 165
[26] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 112
[27] Blume, *Den nye persondatare,* 2 udgave, 2018, s. 25
[28] Blume, *Den nye persondatarets aktører,* 1 udgave, 2018, s. 131

### 6.1.4 EU-retspraksis

Den retspraksis, som skabes gennem afgørelser afsagt af EU-Domstolen tillægges i EU-retten en høj præjudikatsværdi, idet EU-Domstolen nærmere har defineret ydergrænserne af traktatens bestemmelser gennem fortolkning og udfyldning. Ydermere er det sjældent, at Domstolen ændrer sin praksis, og ofte henviser nye afgørelser til tidligere retspraksis[29]. Retspraksis afsagt efter skæringspunktet er medtaget, såfremt den omhandler dataoverførsel til tredjelande, og vil i denne fremstilling tillægges en betragtelig retskildeværdi.

### 6.1.5 Databeskyttelsesloven

Som beskrevet i afsnittet om GDPR er det legitimeret, at nationale lovgivere kan udøve en vis form for national udfyldning. Denne mulighed har Danmark udnyttet og har udarbejdet databeskyttelseslov nr. 502 af 23/05/2018 (herefter DBL). Denne er mindre relevant for denne fremstilling, som beskæftiger sig med databehandling i tredjelande. Ikke desto mindre, som det fremgår af § 2, stk.2. pkt., har Datatilsynet tilsyns- og håndhævelsesbeføjelsen (Datatilsynet vil blive behandlet nedenfor), og DBL-regulering af nationale forhold er derfor ikke underlagt forordningens mekanismer eller EU-Domstolens kompetence. DBL må anses for at være relevant for databehandling inden for det fælleseuropæiske indre marked[30].

### 6.1.6 Datatilsynet

Legitimationen for Datatilsynet findes som tidligere omtalt i præambel nr. 8. Datatilsynets opgaver er udførligt fremsat i forordningens art. 57. Grundlæggende kan det sammenfattes, at tilsynet skal føre tilsynsvirksomhed, afsige afgørelser og "afkode" den tunge og til tider uklare forordning og herved tilgængeligøre, hvilke rettigheder relevante myndigheder, virksomheder og borgere har.[31]
Datatilsynets arbejde som afgørelsesvirksomhed og den beføjelse der medfølger, er reguleret nærmere i forordningens art. 58. Området, som Datatilsynet beskæftiger sig med, stiller store krav til teknisk indsigt, grundet at persondataområdet er under hastig og konstant udvikling og derfor hele tiden skaber og bruger nye tekniske løsninger. Datatilsynet er placeret i Justitsministeriet[32], men skal

[29] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 115
[30] Blume, *Den nye persondatare,* 2 udgave, 2018, s. 30 ff.
[31] Blume, *Den nye persondatarets aktører,* 1 udgave, 2018, s. 88
[32] Blume, *Den nye persondatarets aktører,* 1 udgave, 2018, s. 89

være politisk og økonomisk uafhængig, jf. forordningens art. 52. Datatilsynets vejledninger og afgørelser vil i specialet opfattes som vægtige bidrag til udfyldelsen af analyseobjektet.

### 6.1.7 Vejledninger

Vejledninger er ikke-bindende retsakter, som udstedes af EU-institutionerne. Disse er ikke bindende for modtageren, men binder som udgangspunkt afsenderen, idet de udgør en berettiget forventning til, at der i konkrete sager vil blive fortolket i overensstemmelse med den udstedte retsakt.[33]

Specialet vil anvende vejledninger som "soft law"[34] til fortolkningsbidrag. Som tidligere anført, er området præget af at have særdeles teknisk karakter, hvorved følgende specialenheder har mere specifik viden om området end domstolene. Specialenheder inkluderer EDPB som er lovfastsat i forordningens art. 68, tilsynsmyndigheden i forordningens art. 51 og slutteligt Artikel 29-Gruppe, som erstattes af EDPB. Artikel 29-Gruppe udtagelser er blevet godkedet af EDPB, og kan herfor anvendes på lige fod som udtagelser fra EDPB[35]. Disse publiceres for at tilstræbe en ensartet sagsbehandling og tillige for at klarlægge, hvorledes aktører skal tolke og handle efter gældende lovgivning. Derfor er vejledninger en form for "best practice" og må formodes at skabe en form for praksis for udøvelsen uden at være en bindende retskilde, blandt andet fordi skøn ikke kan sættes under regel og herved udgøre et lovbestemt skøn[36] [37].

### 6.1.8 Generaladvokaterne

Generaladvokaten består af otte generaladvokater, jf. TEU art. 19,3, og TEUF art. 252. Fra 2015 og frem har EU-domstolen besluttet at supplere med yderligere syv generaladvokater.

Den centrale opgave for generaladvokaten er at udarbejde forslag til afgørelser i sager, som er anbragt for EU-domstolen. EU-domstolen er ikke forpligtet til at følge de anbringelser eller konkrete forsalg til afgørelsen[38]. Denne fremstilling vil kun anvende generaladvokatens forslag til afgørelsen i det omfang, de anvendes af EU-domstolens afgørelse.

---

[33] Sørensen og Nielsen, *EU-retten,* 2022, 8. udgave, s. 112
[34] Hamer & Müller, *Juraens verden*, 2020, 1 udgave, 1 oplag, s. 269.
[35] Hamer & Müller, *Juraens verden*, 2020, 1 udgave, 1 oplag, s. 270
[36] https://pav.medst.dk/forvaltningsret-persondataloven-mv/andre-forvaltningsretlige-grundsaetninger/skon-under-regel/ tilgået den 22.marts 2022)
[37] Munk – Hansen, *den juridiske løsning*, 2021, 2. udgave, s. 85
[38] Udsen, *It-Ret*, 2021, 5 udgave, s. 93

### 6.1.9 Litteratur

Specialet vil inddrage faglitteratur, videnskabelige artikler, samt rapporter i det omfang, at det kan bidrage som fortolkningsbidrag. Litteratur anvendes, således at den ikke får altovervejende betydning.[39] Derfor vil der løbende blive foretaget en vurdering af, om det anvendte materiale er fyldestgørende, og om det kan verificeres[40]. Hertil, hvis det er relevant, vil der blive suppleret med flere kilder omhandlende det specifikke område for at kunne sammenligne kvaliteten af materialet.

### 6.1.10 Online-artikler

Artikler, som udelukkende er offentliggjort på online, vil anvendes i et meget sparsomt omfang i denne fremstilling. Når online-artikler anvendes, vil dette ske med det samme vurderingsgrundlag som for litteraturen.

[39] Munk – Hansen, *den juridiske løsning*, 2021, 2. udgave, s. 80
[40] Madsen, *Retsdogmatisk forskning 2022,* Build 2021128, s. 2

# 7. Begrebsdefinitioner

I det nærværende afsnit vil centrale begreber blive afklaret, hvilket gøres for at give læseren den nødvendige baggrundsviden for at drage nytte af de følgende afsnit.

## 7.1 Personoplysninger

I forordningens art. 4, 1 fremgår følgende definition af personoplysninger: *"enhver form for information om en identificeret eller identificerbar fysisk person"*. Det kan heraf udledes, at alle oplysninger, der kan tilbageføres til en fysisk person, er omfattet. Dette spænder naturligt over en lang række informationer, fra de ikke følsomme oplysninger omkring navn, adresse, alder, stilling osv. til de følsomme personoplysninger, der er underlagt forordningens art. 9, herunder genetiske data, race, helbredsoplysninger osv. Yderligere er subjektive vurderinger ang. fysiske personer også inkluderet i definitionen.[41]

Ofte vil dataansvarlig sikre, at der i et nødvendigt omfang sker en pseudonymisering eller kryptering af de informationer, der indhentes. Disse informationer er fortsat omfattet af definitionen i art. 4,1 til trods for denne efterbehandling, jf. præambel nr. 26.

Herefter skal der anvendes krypteringsnøgle, såfremt personoplysningen ønskes at gøres identificerbar. Dette giver anledning til at specificere, hvornår en fysisk person er identificerbar, såfremt det er teknisk og/eller økonomisk muligt, jf. præambel nr. 83, og ved sammenføringer af personoplysninger eller viderebehandling af de krypterede personoplysninger m.m. skal være muligt at identificere en fysisk person, jf. præambel nr. 26, 3. pkt.

## 7.2 Behandling

Af forordningens art. 4,2 fremgår definitionen af *"behandling af personoplysninger"* er "*enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse*".

[41] Udsen, *It-Ret*, 2021, 5. udgave, s 287

Ud fra ovenstående må det konkluderes, at der fra lovgiveres side ikke er ønsket en snæver, men nok nærmere en bred definition af begrebet, hvilket ses ved bugen af ordet "*enhver*" og "*enhver anden form*". Hertil kommer der, at der foreligger undtagelser til udgangspunktet, og disse forefindes i forordningens art. 2, 2. Disse undtagelser vil ikke blive nærmere behandlet i denne fremstilling.

### 7.3 Den registrerede

I forordningen anvendes terminologien "den registrerede" om den person, hvis oplysninger behandles[42]. Forordningen art. 1,1 specificerer, at den registrerede er en fysisk person.

### 7.4 Den dataansvarlige

Modsat ovenstående kan den dataansvarlige både være en "en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger", jf. art. 4, 7. Det er med andre ord den eller de, som beslutter at optage, behandle eller slette personoplysninger, der er ansvarlige for, at dette sker i overensstemmelse med forordningen. Derfor vil det også være den dataansvarlige, som vil blive mødt med sanktioner, såfremt behandling af personoplysninger ikke er forenelig med forordningen. Den dataansvarlige er altså det primære pligtsubjekt[43]. Eksempel på en dataansvarlig kan være AAU, Sundhedsstyrelsen eller online-tjenesteydelser.

### 7.5 Databehandler

Ligeledes som ovenstående kan databehandleren være en "*fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ",* jf. forordningens art. 4, 8. Endvidere fremgår det af denne artikel, at databehandler varetager behandling af personoplysninger på vegne af den dataansvarlige. Herved foreligger der et forhold, hvor dataansvarlig giver databehandler instruktion i hvorledes personoplysninger skal behandles. Forholdet cementeres ved, at såfremt der skal foreligge et databehandlerforhold, skal der indgås en retlig bindende aftale, der lever op til de nærmere fastsatte formkrav i forordningens art. 28, 3[44]. Heri fremgår også de selvstændige forpligtelser, som databehandler, er underlagt. Hertil kan særligt, men ikke udtømmeligt, fremhæves litra e, hvor

[42] Udsen, *It-Ret*, 2021, 5. udgave, s 277
[43] Udsen, *It-Ret*, 2021, 5. udgave, s 278
[44] Udsen, *It-Ret*, 2021, 5. udgave, s. 280

databehandler skal bistå dataansvarlig i at vælge "*forsvarlige passende tekniske og organisatoriske foranstaltninger"* i forhold til at opretholde det fornødne beskyttelsesniveau.

Ovenstående beskriver kortfattet de forhold, hvor der er en dataansvarlig og en databehandler. Dette udgangspunkt bliver dog ofte udfordret i praksis, hvor et fælles dataansvar er relevant. når begge parter behandler personoplysninger[45]. Denne relation ses blandt andet ved Facebook, når individuelle brugere uploader, lagrer og videregiver personoplysninger på Facebooks platform, dette udgør en databehandling. I forhold til de personoplysninger, Facebook behandler om brugerne, bliver Facebook dataansvarlig herfor. Der er altså tale om den samme type stamdata, men anvendelsen er forskellig[46].

## 7.6 Dataeksportør samt dataimportør

Disse udtryk anvendes, når personoplysninger behandles uden for de europæiske grænser. Begreberne er ikke nærmere defineret i forordningen, men er blevet nærmere defineret af henholdsvis Det Europæiske Databeskyttelsesråd og Datatilsynet.

Dataeksportør er den dataansvarlige eller den databehandler, der befinder sig inden for Det Europæiske Økonomiske Samarbejdsområdes (EØS) grænser, og som overfører personoplysninger ikke-EØS-lande og EU. Forpligtelserne er identiske med de forpligtelser, som er fastsat i forordningen omkring dataansvarlig og databehandler og nærmere beskrevet ovenfor.[47] [48]
Dataimportør er en dataansvarlig eller databehandler, som befinder sig uden for EØS-samarbejdet, og som modtager eller får adgang til personoplysninger overført fra EØS-lande[49] [50].

## 7.7 Tredjeland

Med forordningen har EU- og EØS-landene i en vis grad lukket sig om sig selv i beskyttelsen af personoplysninger. Det har af samme grund ikke været lovgiverens intention, at dataansvarlig kunne

[45] Datatilsynet, Vejledning om dataansvarlige og databehandlere, november, 2017, s. 15
[46] Udsen, *It-Ret*, 2021, 5. udgave, s. 279
[47] EDPB, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0, Vedtaget den 18. juni 2021, s. 28
[48] Datatilsynet, Vejledning Overførsel af personoplysninger til tredjelande, juni 2019, s. 11
[49] EDPB, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0, Vedtaget den 18. juni 2021, s. 28 1
[50] Datatilsynet, Vejledning Overførsel af personoplysninger til tredjelande, juni 2019, s. 11

flytte de indhentede personoplysninger til et tredjeland og herved kunne undgå at skulle leve op til forordningens beskyttelsesniveau. Derfor er der i forordningens art. 44 til 50 isat en række bestemmelser, der skal anvendes, når der overføres til tredjeland.[51] Disse er isat, da det ikke praktisk er muligt eller ønskeligt fuldstændig at stoppe overførslen til tredjeland, da dette vil betyde, at international samhandel og samarbejde med stor sandsynlighed ville ophøre, jf. forordningens præambel nr. 101. Endvidere er USA, Kina og Indien nogle af de største udbydere af it-løsninger og løsninger til opbevaring af personoplysninger[52].

I art. 45, 1 findes hjemmelsgrundlaget for Kommissionen i forhold til at godkende "*tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation*". Såfremt Kommissionen finder, at de førnævnte kan sikre et beskyttelsesniveau, der tilnærmelsesvis minder om det beskyttelsesniveau, der er for personoplysninger inden for forordningens territoriale anvendelsesområde, tildeles der status som "*sikker"* tredjeland. Der kan herefter overføres personoplysninger uden forhåndsgodkendelse. Når Kommissionen foretager denne vurdering, sker det som udgangspunkt efter art. 45, 2. Denne oplistning skal ikke anses for udtømmelig. Men nærmere hvad lovgiver *"navnlig"* skal tillægge vægt ved vurderingen.[53]

Følgende er pr. 24.03.2022 sikre tredjelande: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Storbritannien og Uruguay. Hertil er en række områdesektorer i Australien, Canada, Færøerne og Japan, som anses som sikre inden for specifikke områder af overførsler.[54] Modsætningsvis er alle tredjelande eller områder, specifikke sektorer og internationale organisationer uden for EU/EØS, der ikke er sikre tredjelande, pr. definition "*usikkert*" tredjelande. Hvordan der kan ske overførsel til usikkert tredjeland, vil blive behandlet nærmere i afsnittet nedenfor.

# 8. Grundrettigheder

Med forordningens ikrafttrædelse sikres endnu en gang de grundlæggende rettigheder, som i 1950 trådte i kraft med Den Europæiske Menneskerettighedskonvention. Hertil kan særligt nævnes konventionens art. 8,1: *"Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin*

[51] Udsen, *It-Ret,* 2021, 5 udgave, s. 394
[52] Udsen, *It-Ret*, 2021, 5. udgave, s. 397
[53] Datatilsynet, Vejledning Overførsel af personoplysninger til tredjelande, juli, 2021, 3. udgave, s.12
[54] Datatilsynet, Vejledning Overførsel af personoplysninger til tredjelande, juli, 2021, 3. udgave, s.13

*korrespondance."* Særlig relevant for denne fremstilling er "*korrespondance*", som bliver uddybet i Traktaten om Den Europæiske Union (TEU) art. 286 fra 1958 og videreført til Traktaten om Den Europæiske Unions Funktionsmåde (TEUF), art. 16,1 og fastslår, at *"Enhver har ret til beskyttelse af personoplysninger om vedkommende selv."*

Netop disse to artikler er citeret i forordningens præambel nr. 1. Navnlig beskyttelse af personoplysninger fremhæves i forordningens præambel nr. 2 over for de andre grundrettigheder og frihedsrettigheder efter Den Europæiske Menneskerettighedskonvention.

Balancen mellem de ovenstående tunge hensyn og beskyttelsesbehov stillet over for behovet for at kunne behandle personoplysninger i forskelligt omfang[55] har skabt en meget kompleks retsdisciplin for dennes udøver. Kompleksiteten mindskes blandt andet gennem forordningens art. 5, der omfatter en række principper for behandlingen af personoplysninger, der altid skal følges[56]. Helt overordnet er der art. 5, 1, litra a, hvor det fremgår, at behandling skal foregå på en *"lovlig, rimelig og på en gennemsigtig måde".* Disse tre overordnede ord skal uddybes for at give en klarere definition.

### 8.1 Lovlighed

Lovligheden er nærmere reguleret i forordningens art. 6, 1, litra a-f, hvoraf mindst en de nævnte forhold skal være opfyldt. Oplistninger er således ikke kumulative. Særlig relevant for denne fremstilling er litra a, der foreskriver, at den registrerede samtykker til *"et eller flere specifikke formål."* Og der foreligger herved en lovlig behandling af dennes personoplysninger. Begrebet samtykke behandles dybdegående i senere afsnit. Relevant for denne fremstilling er også opsamlingsbestem-melsen i litra f [57], som indeholder en adgang til lovligt at behandle efter en interesseafvejning mellem en legitim interesse og den registreredes interesse og grundlæggende rettigheder og frihedsrettigheder, som er behandlet ovenfor.

### 8.2 Rimelighed

Overordnet skal personoplysninger behandles med minimum og med mindst mulige indgriben i den registreredes grundrettigheder og frihedsrettigheder, jf. forordningens præambel nr. 39.

---

[55] Udsen, *It-Ret*, 2021, 5. udgave, s. 363
[56] Udsen, *It-Ret,* 2021, 5. udgave, s. 281
[57] Udsen, *It-Ret*, 2021, 5. udgave, s. 321

Særligt offentlige myndigheder foretager i stigende grad afgørelser på bagrund af personoplysninger, der er hentet fra forskellige registre, for eksempel oplysninger fra arbejdsgiveres lønsystem til skatteväesenet i forbindelse med årsopgørelser og sundhedsoplysninger, der videregives mellem forskellige hospitalssektorer i forbindelse med sygdomsbehandling. Det er åbenlyst relevant og nødvendigt, at de registre har adgang til at få rettet eller fjernet urigtige oplysninger vedrørende dem. Denne ret er sikret i forordningens art. 5, 1, litra d samt i forordningens art. 16, som omhandler retten til berigtigelse, og forordnings art. 17 om retten til sletning[58].

### 8.3 Gennemsigtig

Princippet sikrer, at den registrerede uden videre kundskaber eller indsigt kan få adgang til enhver form for information, som vedrører den registrerede selv. Dette stiller krav til den dataansvarlige eller databehandleren for at gøre disse informationer *"lettilgængelige og letforståelige"* [59] for den registrerede. Særlige oplysninger om identitet på den dataansvarlige, samt hvorledes, hvordan og i hvilket omfang den registreredes personoplysninger behandles, er relevant for den registrerede, jf. præambel nr. 39.

# 9. Overførsler til usikkert tredjeland

Den centrale problemstilling i dette speciale er, hvorledes overførsel af personoplysninger mest sikkert kan overføres til usikkert tredjeland. Derfor vil denne fremstilling ikke beskæftige sig med overførsler til sikre tredjelande, der er defineret i forordningens art. 45. Det nedenstående afsnit vil indledningsvis beskæftige sig med forordningens art. 46 og det heri nævnte overføringsgrundlag, og herefter vil relevante præmisser for Schrems ll-dommen (C-311/18) gennemgås for at fastslå retstilstanden for anvendelsen af forordnings art. 46.

Forordningens art. 46 tilsigter at give dataansvarlig/dataeksportør det fornødne hjemmelsgrundlag til overførsler af personoplysninger til usikkert tredjeland. Under henvisning til tidligere afsnit i denne fremstilling er et usikkert tredjeland ethvert land eller enhver organisation, som ikke er forhåndsgodkendt af EU-Kommissionen som sikre tredjelande/organisationer.

---

[58] Udsen, *It-Ret*, 2021, 5. udgave, s. 316
[59] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel nr. 39

Udgangspunktet er, at der kun må ske overførsel til usikkert tredjeland og derfor behandling af personoplysninger, såfremt dataansvarlig/dataeksportør kan stille fornødne garantier, samt at disse kan håndhæves, gennem effektive retsmidler i det usikkert tredjeland, jf. art. 46,1. Vurderingen, om der er stillet fornødne garantier, skal foretages ud fra samme grundlag, som er oplistet i forordningens art. 45, jf. Schrems II, præmis nr. 96.

Garantierne er opdelt således, at i forordnings art. 46, 2 kræves der ikke forudgående godkendelse fra nationale tilsynsmyndigheder, før personoplysninger kan overføres til usikkert tredjeland. Modsætningsvis kræves der forudgående godkendelse fra nationale tilsynsmyndigheder ved anvendelse af forordningens art. 46,3.[60] Overførselsværktøjer som adfærdskodekser, certificeringsmekanismer og ad hoc-kontraktbestemmelser vil ikke blive nærmere behandlet i denne fremstilling.

## 9.1 Forordningens art. 46, 2, litra c og d (standardkontrakter)

Der er overordnet to typer af standardkontrakter, den ene er med hjemmel i forordningens art. 46, 2, litra d, hvor nationale tilsynsmyndigheder kan udarbejde egne standardbestemmelser, hvilket det danske datatilsyn har afholdt sig fra.

Det andet og mere praktisk anvendelige instrument til at opfylde de nødvendige garantier i forordningens art. 46,1 er EU-Kommissionens standardbestemmelser (L199/31) eller "Standard Contractual Clauses" (SCC), som er offentliggjort den 4. juli 2021, og som pr. den 27. september 2021 ophæver tidligere afgørelser, der er foretaget efter det daværende gældende persondatadirektiv, jf. L199/31[61], art. 4, 2 art. 4, 3. EU-Kommissionens standardbestemmelser vil blive analyseret i det følgende afsnit.

Standardbestemmelser skal overordnet tilsikre et beskyttelsesniveau i tredjelandet, som tilnærmelsesvis svarer til det beskyttelsesniveau, den registrerede kan forvente inden for de europæiske grænser. Dette fremgår af forordningens præambel 108 og 114 samt af L199/31 præambel nr. 1. Ved vurdering af beskyttelsesniveauet skal der anvendes samme vurderingsgrundlag som i forordningens art. 45 *(Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet),* jf. Schrems II, præmis nr. 96.

---

[60] Udsen, *It-Ret*, 2021, 5. udgave, s 400

[61] Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021, om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679

Det følger af L199/31 præambel nr. 10, at standardkontraktbestemmelserne er opbygget således, at dataansvarlig/databehandler udover at overholde de generelle bestemmelser også skal tage stilling til, hvilket behandlerforhold der foreligger, og herudfra foretage valg af et "modul". Dette giver dataansvarlig/databehandler mulighed for at individualisere standardkontraktbestemmelserne i en større grad end hidtil uden at ændre i kontekst og indhold. Herved bibeholder standardkontraktbestemmelserne deres gyldighed som fornøden garanti, jf. art. 46, 1[62].

Modul 1 regulerer overførsler fra dataansvarlig til dataansvarlig. Modul 2 regulerer overførsler fra dataansvarlig til databehandler. Modul 3 regulerer overførsler fra databehandler til databehandler. Det sidste modul regulerer overførsler fra databehandler til dataansvarlig.

For at kunne anvende det rigtige modul er det nødvendigt at fastlægge, hvem af parterne der er dataansvarlig og databehandler, samt såfremt der er flere dataansvarlige og databehandlere, er det relevant at fastlægge, i hvilket led den enlige overførsel til usikkert tredjeland udføres.

Definitionen af henholdsvis dataansvarlig og databehandler er identisk med definitionen i forordningens art. 4,7 og art. 4, 8 og kan ikke fortolkes i strid med denne forordning, jf. L 199 /31, bestemmelse 4, litra a og c.

EU-Kommissionens standardbestemmelser, L 199 /31, opfylder efter Schrems II-dommen fortsat bestemmelsen om fornødne garantier efter forordningens art. 46,1[63], jf. Schrems II, præmis nr. 27.

## 9.2 Forordningens art. 46,2, litra b (bindende virksomhedsregler)

Brugen af de ovennævnte standardformularer vil i multinationale koncerner eller virksomheder, som har fælles økonomisk aktivitet[64] (i det følgende koncern), være særdeles byrdefuld, når den berørte koncern skal overføre personoplysninger internt i koncernen i forbindelse med administrativt brug, for eksempel ved ansættelse, lønafvikling eller mellem forskellige fagområder.

[62] Udsen, *It-Ret*, 2021, 5. udgave, s 402
[63] Udsen, *It-Ret*, 2021, 5. udgave, s 402
[64] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 47,1, litra a

Det vil kræve, at der ved hver behandling skal anvendes en standardbestemmelse for at stille den fornødne garanti efter forordningens art. 46,1. Dette forhold må anses for at være problematisk i forhold til blandt andet forordningens præambel nr. 6, 5. pkt. samt forordningens præambel nr. 101, der begge fremhæver nødvendigheden af at kunne overføre personoplysninger til tredjeland, såfremt beskyttelsesniveauet opretholdes. Med afsæt heri har lovgiver muliggjort, at der internt i koncernen kan vedtages bindende virksomhedsregler (Binding Corporate Rules (BCR)), der tilsikrer et tilstrækkeligt beskyttelsesniveau for behandlingen af personoplysninger.

Når koncernen har udarbejdet de bindende virksomhedsregler, der som minimum skal indeholde de oplistede krav, jf. forordningens art. 47, 2, litra a-k, skal disse godkendes af den kompetente tilsynsmyndighed, jf. forordningens art. 46, 3. Vurderingsspørgsmålet afgøres efter den meget nuancerede art. 47 i forordningen. Såfremt de internt bindende virksomhedsregler godkendes af den nationale tilsynsmyndighed, opfyldes kravet til fornødne garantier efter forordningens art. 46, 1.

### 9.3 Forordningens art. 46,3, litra a og b (individuelle kontraktbestemmelser)

Formålet med de individuelle kontraktbestemmelser er fortsat at tilsikre et beskyttelsesniveau og håndhævelse, som i det *"væsentligste svarer til"* [65] de rettigheder, den registrerede har som følge af forordningen. Dette hensyn skal derfor inkorporeres i de individuelle kontraktbestemmelser, der regulerer forholdet mellem dataansvarlig og databehandler, databehandler og databehandler eller tredjepart, for at bestemmelserne udgør den fornødne garanti, jf. forordningens art. 46, 3 samt forordningens art. 46,1, hvis den nationale tilsynsmyndighed skal godkende brugen heraf.[66]

Den praktiske anvendelighed af individuelle kontraktbestemmelser må anses som begrænset, grundet at det administrativt er meget byrdefuldt dels at kontrahere og dels at få godkendelse fra den nationale tilsynsmyndighed. Yderligere må det også antages, at udformningen og omfanget af de individuelle kontraktbestemmelser i store træk skal være identiske med EU-Kommissionens standardbestemmelser, grundet at beskyttelseshensynet er ens, og der er tale om ens typer overførsler og aktører. Derfor

[65] C-311/18, Schrems II, præmis 64
[66] Udsen, *It-Ret*, 2021, 5. udgave, s 400-401

må det formodes at være mindre byrdefuldt for aktører at anvende de på forhånd definerede og godkendte standardbestemmelser[67] frem for at anvende individuelle kontraktbestemmelser.

### 9.4 Del konklusion

De ovenstående standardbestemmelser kan fortsat anvendes som overførselsgrundlag, når der ikke foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for det pågældende tredjeland i henhold til forordningens art. 45,3, 1. pkt., og når dataansvarlig eller databehandler kan give de *"fornødne garantier", og* kan sikre *"rettigheder, som kan håndhæves"* og med *"effektive retsmidler".* De to sidste forhold behandles nedenfor. I forhold til "*fornødne garantier"* fastslår Den Europæiske Domstol, at de fortsat kan opretholdes ved brugen af forordningens art. 46,2, litra a.[68] [69]

Schrems II fastslår, at "*fornødne garantier"* fortsat kan sikres gennem brugen af de overførselsinstrumenter, som er angivet i forordningens art. 46. Brugen af disse er betinget af, at der sker effektiv håndhævelse. Derfor skal dataansvarlig og databehandler sikre, at lovgivningen i usikkert tredjeland ikke krænker den registreredes grundrettigheder og frihedsrettigheder, jf. Schrems II, præmis nr. 92[70].

# 10. Vurdering af lovgivningen i usikkert tredjeland

De ovenstående overførselsinstrumenter sikrer fornødne garantier gennem en kontraktlig forpligtelse, jf. Schrems II, præmis nr. 133. Denne forpligtelse består selvsagt udelukkende mellem følgende konstellationer: dataansvarlig og databehandler, dataansvarlig og dataansvarlig eller databehandler og databehandler og forpligter ikke udefrakommende tredjemand, og særlig problematisk heller ikke i forhold til offentlige myndigheder i tredjelande, jf. Schrems II, præmis nr. 125. Det er helt centralt, at de fornødne garantier i forordningens art. 46,1 kan *"håndhæves"* og med *"effektive retsmidler"* i usikkert tredjeland, ellers vil de fornødne garantier i forordningens art. 46, 1 ikke være effektive i praksis[71], og herved vil beskyttelsesniveauet blive undermineret, hvilket ikke er foreneligt med forordningens art. 44.

---

[67] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 46, 2, litra a
[68] C-311/18, Schrems II, præmis nr. 27
[69] Udsen, *It-Ret*, 2021, 5. udgave, s 403
[70] Udsen, *It-Ret*, 2021, 5. udgave, s 404
[71] EDPB, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, s.13 nr. 29

Offentlige myndigheders adgang til data er historisk set blevet kvalificeret som et indgreb i de grundlæggende rettigheder. Dette princip følger af en fast EU-domspraksis, jf. den Europæiske Menneskerettigheds Domstol (EMD) EMD, Leander, præmis nr. 48; EMD, Rotaru præmis nr.46; EU-Domstolen, Digital Rights Ireland, præmis nr. 35[72]. Denne domspraksis ses ligeledes i Schrems I og Schrems II, hvor den amerikanske efterretningstjenestes adgang til personoplysninger om europæiske borgere er uforenelig med Charter art. 7, art. 8 og art. 47 og dermed hele forordningens kapitel V[73].

Derfor skal dataeksportør, før der kan overføres personoplysninger til usikkert tredjeland, vælge korrekt overførselsinstrument, men i særdeleshed foretage en vurdering af det usikkert tredjelands lovgivning eller praksis for at sikre, at særligt offentlige sektorer og efterretningstjenester ikke krænker Charters art. 7, art. 8 og art. 47[74].

Ved denne vurdering skal dataeksportør inkludere alle aspekter angående de involverede aktører, der kan få tilgang til personoplysningerne, og kompleksiteten af denne vurdering stiger naturligvis med antallet af aktører.[75] Dette følger også af ældre EMD-domstolspraksis, at en "*vurdering beror på alle forhold i en sag, såsom eventuelle foranstaltningers art, rækkevidde og varighed, årsager til at kræve dem iværksat, de myndigheder med kompetence til at godkende, udføre og føre tilsyn med dem samt typen af retsmidler i national lovgivning" [76]*.

Hertil kan dataeksportør fastlægge usikkert tredjelands myndigheders "eventuelle adgang"[77] til de personoplysninger, der ønskes overført. I Schrems II-dommen fremgår følgen af præmis nr. 105: "for så vidt angår en eventuel adgang for dette tredjelands offentlige myndigheder til de således overførte personoplysninger – til de relevante forhold i dettes retssystem, herunder navnlig de elementer, som er opregnet i den nævnte forordnings art. 45,2."

[72] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020
[73] C-311/18, Schrems II, præmis 92, 93
[74] Udsen, *It-Ret*, 2021, 5 udgave, s 404
[75] EDPB, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, s. 13 nr. 31
[76] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 15 nr. 50

Det kan herudfra konkluderes, at en del af dataeksportørs vurdering skal klarlægge, om en offentlig myndighed i et tredjeland har mulighed for at få adgang til personoplysninger, frem for om myndighederne behandler eller planlægger at foretage en behandling af personoplysninger. Dette forhold er mere vidtgående og kræver en mere kompleks vurdering af usikkert tredjelands retsforhold og håndhævelse af principperne i forordningens art. 44, hvor der skal foreligge en reel behandling, eller der planlægges at behandle personoplysninger efter overførslen til usikkert tredjeland.

Yderligere kan det udledes af Schrems II-dommens præmis nr. 105, at dataeksportør *"navnlig"* skal basere vurdering af usikkert tredjelands retsforhold, og om et tilstrækkeligt beskyttelsesniveau kan opnås og håndhæves ud fra de samme oplistede elementer som i forordningens art. 45,2, der omhandler EU-Kommissionens godkendelse af tredjelande, som opnår status som sikre tredjelande.

Denne bestemmelse er formuleret særdeles bredt og kræver, at dataeksportøren har omfattende og indsigtsfuldt kendskab til lovgivning og praksis i det usikkert tredjeland [78]. Yderligere kan oplistningen ikke opfattes som udtømmelig, grundet at der *"navnlig"* skal lægges vægt på de oplistede forhold, men ikke udelukkende. For yderligere at konkretisere vurderingen af offentlige myndigheders adgang til personoplysninger og herved indgreb i de grundlæggende menneskerettigheder og frihedsrettigheder har Det Europæiske Databeskyttelsesråd udarbejdet fire europæiske væsentlige garantier.

## 10.1 De fire europæiske væsentlige garantier

A. Behandling baseret på klare, præcise og tilgængelige regler
B. Nødvendighed og proportionalitet, hvad angår de legitime mål, der forfølges og godtgøres
C. En uafhængig tilsynsmekanisme
D. Effektive retsmidler til rådighed for de enkelte personer[79].

Nærværende fremstilling vil ikke gå i dybden med alle facetter af de fire ovenstående garantier men fremhæve det, som har størst relevans i forhold til problemformuleringen.

[78] Udsen, *It-Ret,* 2021, 5. udgave, s 404
[79] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 8 nr. 24

### 10.1.1 A: Behandling baseret på klare, præcise og tilgængelige regler

Denne garanti følger af Charterets art. 8, 2, hvor der i forhold til behandlingen af personoplysninger er angivet på *"grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag",* jf. Schrems II, præmis nr.173. Charterets art. 8, 2 skal læses i sammenhæng med Charterets art. 52,1, som fastlægger, at enhver begrænsning i udøvelse af de i Charteret fastsatte bestemmelser kun må foretages ved fastsat lovgivning. Dette betyder, at den pågældende lovgivning, som tillader indgreb i den registreredes grundrettigheder og frihedsrettigheder, af egen drift skal klarlægge, i hvilket omfang bestemmelsen kan anvendes, og under hvilke mindstekrav bestemmelsen kan realiseres. Dette er for at give den registrerede garantier for, at behandling kun foretages i det strengt nødvendige omfang, jf. Schrems II, præmis nr. 176.

Denne garanti var ikke forenelig med den amerikanske lovgivning, Foreign Intelligence Surveillance Act, sektion 702 samt bekendtgørelsen[80] E.O. 12333, grundet at der ikke indgår nogen begrænsninger eller minimumskrav for behandling af personoplysninger tilhørende registret i EU, jf. Schrems II, præmis nr. 180.

### 10.1.2 B: Nødvendighed og proportionalitet, hvad angår de legitime mål, der forfølges og godtgøres

Gennem Schrems ll og La quadrature du net c-511/18 kan rækkevidden af denne garanti nærmere fastlægges og klarlægges i forhold til, hvad dataansvarlig navnlig skal tillægge værdi i forbindelse med vurdering af tredjelands lovgivning.

Dette princip udspringer af Charterets art. 52,1 og indebærer, at enhver begrænsning skal være proportionel i forhold til, hvad der er nødvendigt og modsvarer mål for almene interesser. Det er selvsagt en meget bred formulering. Bestemmelsen kan deles op i to overordnede hensyn. Det første er proportionalitetsprincippet. og det andet er princippet om nødvendighed.

Det følger af fast EU-Domstolen praksis, at ethvert indgreb i de grundlæggende rettigheder og frihedsrettigheder, og i særdeleshed når indgrebet behøver personoplysninger, skal holde sig til det strengt nødvendige[81]. Dette princip er også forankret i forordningens art. 5,1, litra c, d og e, hvor der

[80] https://www.archives.gov/federal-register/codification/executive-order/12333.html, tilgået d. 2022
[81] C-511/18, La quadrature du net, præmis nr.130

stilles krav om dataminimering, og omfanget af denne bestemmelse er derfor relevant for denne fremstilling at fastlægge nærmere.

Det er fastsat i dommen La quadrature du net c-511/18, præmis nr.132:

"for at opfylde kravet om proportionalitet skal en lovgivning fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning".

I forbindelse med princippet om nødvendighed fremgår det af samme præmis:

"Denne lovgivning skal være retligt bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige".

I det følgende afsnit vedrørende den ovenstående præmis om proportionalitet og nødvendighed bliver den behandlet for at klarlægge dens omfang, når forholdet omfatter et medlemslands (Frankrig) lovgivning over for den amerikanske lovgivnings adgang til brugen af *"generel og uddifferentieret lagring af trafikdata og lokaliseringsdata"*[82].

Den overordnede tvist i dommen La quadrature du net c-511/18 omhandler, hvorvidt den franske regering kunne pålægge et kommunikationsnetværk et påbud om *"generel og uddifferentieret lagring af trafikdata og lokaliseringsdata"*[83].

Dette påbud minder om den førnævnte Foreign Intelligence Surveillance Act, sektion 702, der giver den amerikanske efterretningstjeneste adgang til ubegrænset og uddifferentieret at masseovervåge ikke-amerikanske borgeres personoplysninger, såfremt disse persondata kan klassificeres som *"foreign intelligence*[84]. Dette omfatter enhver oplysning om udenlandske magter, organisationer eller personers hensigter, aktiviteter og kapaciteter. [85]

Begge bestemmelser tilsiger, at der kan foretages en vis form for masseovervågning af personoplysninger med henblik på at forebygge og bekæmpe grov kriminalitet og trusler mod den offentlige

[82] C-511/18, La quadrature du net, præmis nr. 229, 1
[83] C-511/18, La quadrature du net, præmis nr. 229,1
[84] https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf , tilgået den.16.03.2022
[85] https://www.intelligence.senate.gov/laws/united-states-intelligence-activities , tilgået den. 16.03.2020

sikkerhed, begge gennem anvendelse af "*generel og uddifferentieret lagring af trafikdata og lokaliseringsdata".*

I dommen La quadrature du net c-511/18 er der til dette udgangspunkt fastsat begrænsninger i forhold til både, hvilken type trusselsbillede der kan legitimere et indgreb, og i hvilket omfang der kan ske indgreb.

10.1.2.1 Målrettet lagring af trafikdata og lokaliseringsdata

Hvad angår målrettet lagring af trafikdata og lokaliseringsdata, kan dette indgreb bruges i forbindelse med grov kriminalitet og til beskyttelse af den offentlige sikkerhed, såfremt der sker en objektiv og ikke-diskriminerende afgrænsning af, hvilke personer som berøres af indgrebet, og at dette indgreb tidsmæssigt holdes til et minimum, jf. La quadrature du net c-511/18, præmis nr.168.

Endvidere kan et nærmere geografisk defineret område, som ud fra en objektiv og ikke-diskriminerende vurdering også legitimere et indgreb i privatlivets fred, såfremt der foreligger et forhøjet niveau eller risiko for kriminalitet, og disse områder er større offentligt tilgængelige steder, såsom lufthavne, togstationer og andre strategiske steder, jf. La quadrature du net c-511/18, præmis nr.150.

10.1.2.2 Brugen af IP-adresser

Angående brugen af IP-adresser, kan disse data anvendes til at skabe et ganske detaljeret billede af enkelte individer ud fra deres søgemønster online. Brugen af IP-adresser er begrænset til, at der kun kan foretages sporing af, hvem der lægger noget ud, men ikke, hvem der modtager, jf. La quadrature du net c-511/18, præmis nr.152 samt 153 En generel og uddifferentieret brug af IP- adresser kan resultere i, at personer, som ikke er relevante for det forfulgte mål, og deres personoplysninger blotlægges. Dette skal undgås ved at fastsætte *"strenge betingelser og garantier for så vidt angår brugen af disse data, bl.a. ved hjælp af sporing, med hensyn til de kommunikationer og de aktiviteter, som de berørte personer foretager online*", jf. La quadrature du net c-511/18, præmis nr.156.

Derfor må brugen af generel og uddifferentieret lagring af IP-adresser kun foretages, når det omhandler beskyttelse af offentlig sikkerhed og til forebyggelse af grov kriminalitet, jf. La quadrature du net c-511/18, præmis nr.168.

10.1.2.3 Uddifferentieret lagring af trafikdata og lokaliseringsdata

Hvad angår brugen af *"uddifferentieret lagring af trafikdata og lokaliseringsdata*", fremgår det af La quadrature du net c-511/18, præmis nr.139, at brugen af *"uddifferentieret lagring af trafikdata og lokaliseringsdata"* udelukkende kan bruges i forbindelse med en foreliggende alvorlig trussel mod national sikkerhed, heriblandt trussel mod *"væsentlige funktioner og grundlæggende samfundsinteresser"* samt *"forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed"*[86].

Dette princip følges også i La quadrature du net c-511/18, præmis nr. 141, hvor det fremgår, at såfremt en medlemsstats lovgivning i forbindelse med bekæmpelse af grov kriminalitet gør brug af *"generel og uddifferentieret lagring af trafikdata og lokaliseringsdata",* kan dette ikke legitimeres som at være strengt nødvendigt, og det kan derfor ikke anses for at være proportionelt. Ydermere vil en *"generel og uddifferentieret lagring af trafikdata og lokaliseringsdata"* også kunne involvere personer, som udelukkende bruger elektroniske kommunikationsmidler i lovligt medfør, og som ikke i sig selv udgør et strafsubjekt. Dette forhold kan heller ikke anses for at være begrænset til det nødvendige omfang, der i sig selv kunne legalisere et indgreb, jf. La quadrature du net c-511/18, præmis nr. 143 samt præmis nr.145.

Den ydre grænse, over for hvem denne foranstaltning kan anvendes, er fastlagt således, at det skal baseres på objektive forhold, der direkte eller indirekte kan afsløre eller forhindre grov kriminalitet, som udgør en alvorlig sikkerhedstrussel for offentligheden eller nationen, jf. La quadrature du net c-511/18, præmis nr.140 og præmis nr.148. Endvidere kan geografisk nærmere definerede områder, som ud fra en objektiv og ikke-diskriminerende vurdering også være underlagt dette indgreb i privatlivets fred, såfremt der foreligger et forhøjet niveau eller risiko for kriminalitet, og disse områder er større offentligt tilgængelige steder, såsom lufthavne, togstationer og andre strategiske steder jf. La quadrature du net c-511/18, præmis nr.150.

[86] C-511/18, La quadrature du net, præmis nr.135

Indgreb som de ovennævnte skal anses for at være af alvorlig karakter i forhold til grundlæggende rettigheder og frihedsrettigheder. Derfor skal disse indgreb ledsages af *"strenge betingelser og garantier",* der sikrer, at de data, som indhentes via personers brug af online-tjenester og færden i offentlige rum, videre hen behandles, jf. La quadrature du net c-511/18, præmis nr.156.

10.1.2.4 Automatiserede analyser

Såfremt persondata er indhentet på baggrund af overstående eller andre grundlag, hvor der efterfølgende anvendes *"automatiseret analyse*"[87], opfatter EU-retten det som et *"særligt alvorligt indgreb"*[88] og kan kun legitimeres gennem proportionalitetsprincippet, såfremt der foreligger en alvorlig trussel mod den nationale sikkerhed, der kan defineres til at*" være reel og aktuel eller forudsigelig og på betingelse af, at varigheden af denne lagring er begrænset til det strengt nødvendige."*[89] Det kan herudfra udledes, at forebyggelse eller opklaring af grov kriminalitet ikke kan opfattes som proportionelt over for det indgreb, der foretages i henhold til Charterets art. 7, 8 og 52,1.

10.1.2.5 Lagring af personoplysninger

Lagring af personoplysninger skal være begrænset til det absolut nødvendige tidsrum, og der kan derfor ikke ske ubegrænset lagring. Såfremt det findes nødvendigt, kan lagringens periode forlænges, når hensyn taler herfor, jf. La quadrature du net c-511/18, præmis nr. 151 samt 176. Lagring skal derfor altid kunne opfylde objektive kriterier for, hvad der opbevares, og hvad det forfulgte mål udgør, jf. La quadrature du net c-511/18, præmis nr. 133.

10.1.2.6 Hurtig lagring af trafikdata og lokaliseringsdata

I praktisk har virksomheder, som udbyder elektroniske kommunikationstjenester, behov for at behandle og lagre personoplysninger i forbindelse med deres virke. Herefter skal personoplysninger enten slettes eller anonymiseres efter de på området lovbestemte fristelser. Der kan undertiden være et behov fra myndighedernes side at forlænge disse frister for at kunne opklare angreb på den offentlige sikkerhed eller grov kriminalitet, jf. La quadrature du net c-511/18, præmis nr. 161. Dette indgreb skal nødvendigvis ikke begrænset til kun at omhandle personoplysninger om den eller dem, som er mistænkt i forbindelse med en grov kriminel handling eller angreb mod den offentlige sikkerhed, men

[87] C-511/18, La quadrature du net, præmis nr. 177
[88] C-511/18, La quadrature du net, præmis nr. 177
[89] C-511/18, La quadrature du net, præmis nr. 177

skal for så vidt begrænses til det strengt nødvendige, jf. La quadrature du net c-511/18, præmis nr. 165. Dette indgreb kan ikke foretages uden forudgående domstolsprøvelse af en uafhængig kompetent myndighed, jf. La quadrature du net c-511/18, præmis nr. 168.

10.1.2.7 Trafikdata og lokaliseringsdata i realtid

Denne type indgreb udgør i særdeleshed et indgreb i den personlige frihed, idet der kan foretages "kontinuerligt og i realtid at overvåge de personer, som de berørte personer kommunikerer med, de midler, som de anvender, varigheden af deres kommunikation og disse personers opholdssted og færden"[90]. Derfor kan denne type indgreb ikke foretages uden forudgående prøvelse hos enten en kompetent domstol eller en administrativ uafhængig instans. Denne tilladelse kan kun gives, såfremt der kan fremlægges en meget velbegrundet mistanke om tilknytning til terrornetværk, og at indgrebet kan begrænses til at være det strengt nødvendige, jf. La quadrature du net c-511/18, præmis nr. 192.

10.1.2.8 FISA's sektion 702 og E.O. 12333 sammenholdt med PPD-28

Den amerikanske lovgivning er ikke lige så detaljeret på området for statslige indgreb i personoplysninger. Derfor er det ikke muligt med lige så detaljeret grad at fastslår, hvilke begrænsninger der kan gøres gældende i forbindelse med indgreb, som er underlagt Charterets art. 7, art. 8 og art. 52,1.

Den tidligere beskrevne Foreign Intelligence Surveillance Act Section 702 (i det følgende FISA) er dog begrænset således, at den kun kan anvendes, såfremt den overholder det udstedte præsidentielle dekret PPD-28, jf. PPD-28, sektion 1, litra a. Brugen af indsamlet personoplysninger, der sker gennem FISA, må ikke bruges til at diskriminere eller inkriminere på baggrund af etnicitet, race, køn, seksuel orientering eller religion, jf. PPD-28, sektion 1, litra b. Behandlingen af denne type personoplysninger er i GDPR-forordningen reguleret i art. 9.

Yderligere må indsamlet personoplysninger ikke videregives med henblik på kommercielle interesser, men kun bruges til at beskytte den nationale sikkerhed for amerikanske allierede, jf. PPD-28, sektion 1, litra c.

[90] C-511/18, La quadrature du net, præmis nr. 184

Brugen af indsamling og behandling af personoplysninger skal være så *"så målrettet som muligt« (as tailored as feasible)",* jf. PPD-28, sektion 1, litra c. Dette udgør ikke en tilstrækkelig begrænsning og anses i Schrems II, præmis nr. 64 for at udgøre en generel tilgang for amerikanske myndigheder til at behandle massedata om europæiske borgere uden begrænsninger.

I forbindelse med behandlingen af personoplysninger, der optages gennem *"Bulk"*[91]*,* der skal sidestilles med *"Uddifferentieret lagring af trafikdata og lokaliseringsdata"*[92]*,* er det nødvendig grundet en stigende grad af kommunikation på medier, som kan tilgås af alle personer. Derfor sker der en sammenblanding af personoplysninger, som kan være relevante for efterretningstjenesten, men også personoplysninger, der ikke er relevante for efterretningstjenesten. Med henblik på at overholde de i Charterets art. 7 og art. 8 grundrettigheder og frihedsrettigheder er der i PPD-28 foretaget en begrænsning i indgrebsmulighederne. Derfor må personoplysninger, som er behandlet i forbindelse med bulk, kun anvendes i forbindelse med trusler mod national sikkerhed, allieret national sikkerhed, it-sikkerhed og kriminalitet generelt, jf. PPD-28, sektion 2.[93]

Denne brede tilgang for en offentlig myndighed findes ikke i Schrems II for at være begrænset i tilstrækkelig grad til, at det kan anses for at være proportionelt eller være begrænset til det strengt nødvendige i forhold til det indgreb, der lovmæssigt kan foretages i grundrettigheder og frihedsrettigheder.[94]

### 10.1.3 C: En uafhængig tilsynsmekanisme

Nedstående afsnit vil indledningsvis behandle de to sidste europæiske væsentlige garantier samlet. Herefter vil afhængig tilsynsmekanisme og effektive retsmidler til rådighed for de enkelte personer blive behandlet selvstændigt, og afslutningsvis vil der være en delkonklusion.

Behovet for at sikre, at de grundlæggende rettigheder og frihedsrettigheder i Charterets art. 7 og art. 8 håndhæves af effektive og uafhængige instanser og er til rådighed for den enkelte person, hvis

[91] PPD-28, sektion 2
[92] C-511/18, La quadrature du net, præmis nr.139
[93] https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities , tilgået den 19.04.2022
[94] C-311/18, Schrems II, præmis nr. 184

personoplysninger som er blevet gjort til genstand for behandling, er en af grundstenene i Den Europæiske Unions værdisæt.[95]

Den Europæiske Menneskerettighedsdomstol har tidligere belyst de hensyn, der er i forbindelse med de indgreb, som kan defineres som overvågningsforanstaltninger. Sådanne indgreb bør være baseret på forudgående retlige afgørelser, og dette hensyn opvejes over for *"faktiske funktion af systemet, herunder kontroller og afvejninger af udøvelse af beføjelser, og om der forekommer reelt misbrug"*.

Samme instans har ved flere domsafsigelser præciseret, at et indgreb i privatlivets fred, herunder personoplysninger, skal være *"underlagt en effektiv, uafhængig og upartisk tilsynsmekanisme, der skal oprettes enten af en dommer eller et andet uafhængigt organ."*[96]

Dette hensyn er yderligere fremhævet i forordningens præambel nr. 104: "Tredjelandet bør navnlig sikre et effektivt uafhængigt databeskyttelsestilsyn og bør fastlægge samarbejdsmekanismer med medlemsstaternes databeskyttelsesmyndigheder, og de registrerede bør have effektive rettigheder, som kan håndhæves, og adgang til effektiv administrativ og retslig prøvelse."

Dette er selvsagte en bred formulering, der skal konkretiseres, for at dataansvarlig kan foretage en valid vurdering af det usikkert tredjeland lovgivning på området.

I forhold til konkretisering af omfanget af en uafhængig tilsynsmyndighed skal denne øjensynlig holdes op mod de i forordningen kapital VI nærmere fastsatte bestemmelser som følge af Schrems II, præmis nr. 96, der fastlægger, at lovgivningen i usikkert tredjeland i "*det væsentlige svarer til det niveau, der er sikret inden for Unionen"*.

I forordningens art. 52 er uafhængigheden af tilsynsmyndighed nærmere fastlagt. Det følger heraf, at tilsynsmyndighed ikke kan underlægges nogen former for direkte eller indirekte kontrol eller instruks af udefrakommende enhed, jf. forordningens art. 52,2. Derfor er det også nødvendigt, at tilsynsmyndigheden selv udpeger og afskediger medarbejdere, jf. forordningens art. 52, 5, men det pålægges

[95] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel 104
[96] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 12 nr. 39

medlemsstaterne at udnævne hvert medlem af tilsynsmyndigheden. Den pågældende udnævnelse skal være transparent, og det forudsættes, at udnævnelsen sker på grundlag af medlemmers konkrete kompetencer i særdeleshed på feltet omkring beskyttelse af personoplysninger, jf. forordningens art. 53.

For at sikre, at den fornødne uafhængighed kan opretholdes, skal den nationale stat tilsikre, at tilsynsmyndigheden råder over kompetente og de nødvendige medarbejdere, at der stilles de nødvendige tekniske løsninger samt lokaler til rådighed, og at der tilføres de nødvendige finansielle ressourcer for at sikre en velfungerende tilsynsenhed, jf. forordningens art. 52,3. Det er også en afgørende forudsætning, at tilsynsorganet har adgang til alle relevante dokumenter for at kunne udøve sit erhverv i det nødvendige omfang[97].

I forbindelse med revision skal denne foretages således, at dens uafhængighed ikke påvirkes. Yderligere skal der føres offentligt og særskilt budget, som om nødvendigt kan indgå som den del af statsbudgettet eller det nationale budget, jf. forordningens art. 52, 6.

EMD har udvist en præference forstået på den måde, at der er juridiske dommere, der er ansvarlige for tilsynsmyndigheden, og særligt for håndhævelsen af forordningen. Dog udelukker dette ikke muligheden for, at tilsynsmyndigheden kan bestå af et administrativt organ[98]. Dette forhold er yderligere behandlet i Schrems II, præmis. nr. 197, hvor det specifikke ord "organ" anvendes i forbindelse med den amerikanske ombudsmandsmekanisme. Hovedelementerne er, at den kan opretholde en *"tilstrækkelig uafhængighed af det udøvende"*[99].

Med udgangspunkt i de ovenstående parametre vil hovedsageligt Schrems II blive nærmere analyseret for at fastlægge den praktiske anvendelse af bestemmelserne og yderligere konkretisere deres rækkevidde.

[97] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 13 nr. 42
[98] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 13 nr. 42
[99] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s.13 nr. 42

I Schrems I fandt Kommissionen, at Amerika kunne "anses for at sikre et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er garanteret i Charterets art. 47" [100], såfremt den amerikanske regering med de retlige anliggender, som var opgivet i Office of the Director of National Intelligence (ODNI) ville oprette en ombudsmand, der skulle håndhæve de grundlæggende regler og frihedsrettigheder, som findes i Charterets art. 7 og art. 8 og være uafhængig af de amerikanske efterretningstjenester, jf. Schrems II, præmis nr. 43, 2. pkt.

I Schrems II bliver ODNI efterbehandlet, og den findes ikke at udgøre et tilstrækkeligt grundlag ved ikke at opstille fornødne garantier, der tilskikker ombudsmandens uafhængighed. Navnlig er det uforeneligt med forordningens art. 52, 2 at uafhængigheden af ombudsmanden ikke er fuldstændig, grundet at ombudsmanden *"indberetter direkte til den amerikanske udenrigsminister, der sørger for, at ombudsmanden udøver sin funktion på objektiv vis og fri for indflydelse, som kan påvirke de svar, der skal gives."*[101] Dette er ikke foreneligt med førnævnte bestemmelse i forordningens art. 52, 2, grundet at Udenrigsministeriet udøver en form for kontrol, til trods for at denne kontrol skal sikre objektive og uafhængige processer. Hos ombudsmanden skal det opfattes som et indgreb i ombudsmandens uafhængighed.[102]

Yderligere er det Udenrigsministeriet, som udpeger en seniorkoordinator, som blandt andet skal varetage dialog med regeringer uden for Amerika. Omfanget af, hvilken adgang Udenrigsministeriet har til at nedlægge ombudsmandens funktion eller fjerne medarbejdere, er ikke nærmere afgrænset i ODNI[103], men bør ikke findes foreneligt med forordningens art. 52,5 samt forordningens art. 53,4. Ydermere i forbindelse med indsættelse af medarbejdere er dommen Roman Zakharov mod Rusland, 04.12.2015 relevant. Heraf fremgår det, at udvælgelsesprocessen til tilsynsmyndighedens medlemmers juridiske status skal ses i tæt sammenhæng med omfanget af deres uafhængighed. Den ydergrænse er tildelt og defineret ved, at der i domme ikke kunne statueres fuldstændig uafhængighed hos en *"indenrigsminister — som ikke alene var politisk udpeget og medlem af det udøvende organ, men som også var direkte involveret i bestilling af særlige overvågningsmetoder"*[104].

[100] C-311/18, Schrems II, præmis nr.193
[101] C-311/18, Schrems II, præmis nr. 195
[102] C-311/18, Schrems II, præmis nr. 195
[103] C-311/18, Schrems II, præmis nr. 195
[104] EDPB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 13 nr. 42

Opgaverne, som en tilsynsmyndighed skal varetage, er ligeledes nærmere beskrevet i kapitel IV, artikel 57, heriblandt skal tilsynsmyndighed *"føre tilsyn med og håndhæve anvendelsen af denne forordning"*[105] og *"behandle klager, der indgives af en registreret eller af et organ, en organisation eller en sammenslutning i overensstemmelse med artikel 80."*[106] Det kan heraf fastslås, at en af opgaverne med tilsynsmyndighed er at føre et enligt tilsyn, der kan håndhæves, og at varetage indkomne klager i forbindelse med forordningen. Dette kan anses for at være en af hovedopgaverne for tilsynsmyndigheden. Det er særligt i den henseende ikke foreneligt med forordningens art. 57, at det i ODNI ikke nærmere defineres eller nævnes, hvilke beføjelser ombudsmanden har over for særligt den amerikanske efterretningstjeneste. Ligeledes er det ikke oplyst, hvilke adgange registret har for at påberåbe lovbestemte garantier[107].

### 10.1.4 D: Effektive retsmidler til rådighed for de enkelte personer

Det enkelte individs adgang til en effektiv og retfærdig domsstolsbeskyttelse er en forudsætning for en retsstat[108]. Dette udgangspunkt opretholdes i forbindelse med overførsel af personoplysninger gennem en *"effektiv administrativ og retslig prøvelse for de registrerede, hvis personoplysninger overføres"*[109]. Der skal således være en lovbestemt adgang for det enkelte individ for at få håndhævet rettigheder gennem adgang til egne oplysninger, som herefter kan berigtiges eller slettes[110]. Dette grundlæggende princip skal tilsikres gennem de fornødne beføjelser hos tilsynsrådet, som kan foretage en enlig retlig bindende afgørelse, som i væsentlighed modsvarer de garantier, som forefindes i Charterets art. 47[111]. Disse garantier er i særdeleshed vigtige, når det omhandler overførsler af personoplysninger til usikkert tredjeland, jf. Schrems II, præmis nr.189.

I Schrems II, præmis nr. 181 samt præmis nr. 192 bekræfter amerikanske myndigheder, at hverken den førnævnte FISA´s artikel 702, PPD-28 eller E.O 12333 indeholder bestemmelser, som sikrer den registrerede rettigheder, der kan håndhæves over for amerikanske myndigheder. Dette er ikke

[105] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 57, 1, litra a
[106] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 57, 1, f
[107] C-311/18, Schrems II, præmis nr. 196
[108] C-311/18, Schrems II, præmis nr. 187
[109] C-311/18, Schrems II, præmis nr. 188
[110] C-311/18, Schrems II, præmis nr. 194
[111] EPDB, Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, Vedtaget den 10. november 2020, s. 15, nr. 47

foreneligt med Charterets art. 7, art. 8 og art. 47 og er derfor per definition ikke foreneligt med forordningens art. 45, 2, litra a.[112]

I modsætning hertil er der i den tidligere benævnte dom La quadrature du net c-511/18, hvor der fremgår en nærmere og fastlagt praksis for den registreredes adgang til enten en domstolsprøvelse eller prøvelse ved en uafhængig administrativ enhed. I forbindelse med indsamling af data i realtid skal der forelægge en forudgående domstolsprøvelse eller bindende afgørelse fra en uafhængig enhed, for at indgrebet kan foretages. I de tilfælde, hvor omstændighederne grundet tidsmæssige årsager ikke tillader tid til forudgående bindende afgørelse, skal en bindende afgørelse indhentes uden ugrundet ophold, jf. La quadrature du net c-511/18, præmis nr. 189.

Yderligere skal individer, som har været genstand for optagelse af data i realtid med brug af automatiseret analyse, informeres, så snart det ikke kompromitterer at opnå målet med indgrebet. Denne underretning giver den registrerede mulighed for at kunne anvende sine rettigheder, heriblandt indsigt i egne oplysninger samt berigtigelse og sletning og domstolsprøvelse, jf. La quadrature du net c-511/18, præmis nr. 190.

### 10.2 Del konklusion

Dette afsnit skal drage overordnede konklusioner af vurderingerne ang. usikkert tredjelands lovgivning, der skal foretages af dataeksportøren, efter det er fastlagt, hvilket overførselsværktøj der ønskes anvendt. Den konkrete vurdering skal i hovedtræk følge forordningens art. 45, 2, jf. Schrems II, præmis nr. 104. Denne artikel anvendes af Kommissionen i forbindelse med vurdering af, om et usikkert tredjeland kan opnå status som sikkert tredjeland. Yderligere bør dataeksportøren iagttage de fire europæiske væsentlige garantier, som er fastsat af Det Europæiske Databeskyttelsesråd.[113]

Det må forudsættes, at ovenstående analyse samt tilhørende konklusioner kan anvendes universelt og ikke kun er begrænset til vurdering af amerikansk lovgivning.

Både Charterets art. 7, art. 8 og art. 47, forordningens art. 45, 2 samt de fire europæiske væsentlige garantier udgør de centrale elementer i forbindelse med dataeksportørens vurdering usikkert

[112] C-311/18, Schrems II, præmis nr.181
[113] Udsen, *It-Ret*, 2021, 5. udgave, s 404

tredjelands lovgivning. De kan derfor ikke behandles enkeltvist eller uafhængigt af hinanden. Disse centrale elementer udgør ikke det eneste grundlag for vurdering, alle relevante forhold hos et usikkert tredjeland bør og skal inkluderes i helhedsbedømmelsen.

Resultatet af denne helhedsvurdering skal ikke nødvendigvis vise, at lovgivningen er identisk med europæisk lovgivning, hvilket i praktisk nok også ville være umuligt. Dette skyldes, at der i forordningen og i Schrems II-afgørelsen stilles krav om, at lovgivningen i et usikkert tredjeland i forhold til beskyttelsesniveau i det væsentlige svarer til europæiske standarder og garantier.

Bestemmelserne og de fire europæiske væsentlige garantier formuleret så bredt, at fortolkning er nødvendig. Udgangspunktet for fortolkning er at klarlægge, hvilke adgang offentlige myndigheder har til EU-borgeres personoplysninger. Det er i den forbindelse irrelevant, om den offentlige myndighed anvender denne adgang, eller om det blot foreligger som en mulighed for adgang. Herefter skal indgrebet vurderes ud fra proportionalitetsprincippet, som er lovbestemt i Charterets art. 52,1. Et af hovedformålene har i henholdsvis c-511/18, La quadrature du net og C-311/18, Schrems II, været beskyttelse af den offentlige og nationale sikkerhed, hvoraf det fremgår af amerikanske lovbestemmelser er formuleret bredere ved at anvende termer som ”så målrettet som muligt”, hvor den franske lovgivning er begrænser til det ”strengt nødvendige”.

I La quadrature du net c-511/18 fandt EU-domstolen, at grove indgreb i Charterets art. 8 og art. 7 legitimeres gennem proportionalitetsprincippet, såfremt indgrebet er begrænset til det strengt nødvendige for at sikre offentlig og national sikkerhed og som værn med grov kriminalitet. I forhold til overvågningsmiddel kunne det samme ses i FISA´s artikel 702, PPD-28 og E.O 12333, men her var tilgangen til indgrebet i Charterets art. 8 og art. 7 ikke begrænset til det strengt nødvendige, men til at være så målrettet som muligt. Forholdet mellem de to domme er ikke blevet behandlet hos en relevant domstol endnu, men efter denne fremstillings opfattelse, bør dataeksportøren inddrage dommen c-511/18 La quadrature du net, som et vigtigt fortolkningsbidrag til vurdering af usikkert tredjelands lovgivning. Dommen statuerer, at der også indenfor europæiske grænser foreligger vidtrækkende indgreb i Charterets art. 8 og art. 7 i forhold til myndighedernes adgang til personoplysninger.

Lovgivning i usikkert tredjeland skal sikre, at der er et uafhængigt organ, som kan håndhæve det enkelte individs rettigheder. Denne uafhængighed skal foreligge både direkte og indirekte. I forordningens kapitel IV er myndighedernes rolle i forhold til det uafhængigt organ, nærmere defineret som at være en faciliterende rolle, og udøvelsen af denne rolle skal ske efter armslængdeprincippet. Yderligere er det særligt relevant at tilsynsorganet har mulighed for selvstændig håndhævelse og med effektive retsmidler uden en overliggende myndigheds kontrol, som det modsætningsvis fremgives af forholdet mellem den amerikanske ombudsmandsinstitution og udenrigsministeren.

Når dataeksportøren har foretaget denne vurdering, kan der drages en af to konklusioner: Enten opfylder tredjelandet i væsentlighed forordningens art. 45, 2 og de europæiske væsentlige garantier, og der kan derfor overføres personoplysninger til tredjeland.

Den anden og nok mere øjensynlige konklusion er, at tredjeland ikke opfylder forordningens art. 45, 2 og de europæiske væsentlige garantier, og der kan derfor som udgangspunkt ikke foretages overførsel til et usikkert tredjeland.

# 11. Supplerende foranstaltninger

Anvendelse af supplerende foranstaltninger kan indledningsvis henføres til forordningens præambel nr. 109, hvor det fremgår, at *"Dataansvarlige og databehandlere bør tilskyndes til at give yderligere garantier gennem kontraktmæssige forpligtelser, der supplerer standardbestemmelserne om beskyttelse."* På denne måde pålægges dataeksportøren en generel forpligtelse til at tilskikket et meget højt beskyttelsesniveau og så i den forbindelse, at standardbestemmelserne i sig selv udgør et tilstrækkeligt beskyttelsesniveau.

I Schrems II bliver anvendelse af supplerende foranstaltninger yderligere udvidet gennem præmis nr. 133, hvoraf det fremgår, at såfremt anvendelsen af de standardbetingelser, som er oplistet i forordningens art. 46, ikke sikrer et tilstrækkeligt beskyttelsesniveau, vil der *"være behov for, at den dataansvarlige vedtager supplerende foranstaltninger for at sikre, at dette beskyttelsesniveau er overholdt."* Dette giver dataeksportøren en yderligere mulighed for at overføre personoplysninger til usikkert tredjeland, til trods for at der ikke kan sikres et tilstrækkeligt beskyttelsesniveau ved alene anvendelsen af standardbestemmelserne i forordningens art. 46.

Som beskrevet i afsnittet ovenfor vil en konkret og omhyggelig vurdering af et usikkert tredjelandslovgivning for at fastlægge, om der er et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres, ofte resultere i, at der ikke foreligger et beskyttelsesniveau, som i det væsentlige svarer til det, som er sikret inden for EU´s grænser. Dette resulterer i, at der ikke kan overføres personoplysninger uden for EU´s grænser, uden at dataeksportøren foretager supplerende foranstaltninger, der effektivt bringer beskyttelsesniveauet op til det, som der er inden for de europæiske grænser.

Supplerende foranstaltninger kan opdeles i tre hovedgrupper værende af kontraktlig, teknisk eller organisatorisk art. Disse kan anvendes individuelt, men må anses for at opnå en forstærkende effekt ved at blive kombineret. Fælles for de supplerende foranstaltninger er, uanset i hvilken konstellation de anvendes i, er de pr. definition et supplement til overførselsinstrumenterne i forordningens art. 46.[114] Det er en forudsætning, at dataeksportøren har et indgående kendskab til, hvor det er relevant og effektivt at anvende supplerende foranstaltninger. Derfor skal der for hvert anvendt overførselsinstrument foretages en konkret vurdering af, hvilke supplerende foranstaltninger der er relevante i forhold til det tredjelands utilstrækkelige lovgivning. Denne vurdering kan suppleres med de "fund", som er gjort i forbindelse med vurdering af overførselsgrundlaget og vurderingen af det pågældende usikkert tredjeland.

I det tilfælde, at dataeksportøren tidligere ved brug af supplerende foranstaltninger har overført personoplysninger til et tredjeland, og at den forstående overførsel er af samme type personoplysninger og til samme tredjeland, pålægges det ikke dataeksportøren at gentage processen igen, og tidligere anvendte overførselsinstrument samt supplerende foranstaltninger kan anvendes, såfremt de fortsat er virksomme.[115] Derfor er det en forudsætning, at dataeksportøren løbende foretager en vurdering af, om behandlingen af personoplysninger fortsat er *"lovlig, rimelig og gennemsigtig"* og herved overholder forordningens art. 5,1. Tillige er det en forudsætning, at dataeksportøren kan påvise gennem dokumentation, at ovennævnte betingelser er overholdt, jf. forordningens art. 5, 2. I forbindelse med brug af supplerende foranstaltninger er det særligt relevant at følge og vurdere udvikling af it-

[114] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 22 nr. 50
[115] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 22-23

løsninger, modtagerlandets lovgivning og retspraksis samt nødvendigheden af brug af samarbejdspartnere.[116]

Anvendelse af enhver form for supplerende foranstaltninger forudsætter, at de i realiteten har en effekt. Denne effekt kan ikke måles på generel vis, men er en specifik vurdering. De kontraktlige og organisatoriske foranstaltninger binder ikke tredjemand. Derfor forpligter de ikke tredjelands offentlige myndigheder. Dog er implementering af kontraktlige og organisatoriske foranstaltninger ikke uden relevans i forhold til dataeksportøren og dataimportøren.[117] De kontraktlige og organisatoriske foranstaltninger kan målrettes i forhold til de konkrete problematiske forhold i det usikkert tredjelands lovgivning. Eksempelvis i tilfælde, hvor dataimportøren kan blive mødt med påbud om at udlevere personoplysninger. Her kan det være relevant for dataeksportøren at have foretaget kontraktlige foranstaltninger, der tilsikrer, at dataimportøren kun udleverer den absolutte minimale mængde data. Yderligere kan det være relevant for dataeksportøren at fastlægge klare kontraktlige foranstaltninger omkring, hvilke medarbejdere hos dataimportøren der kan tilgå personoplysninger og under hvilke omstændigheder[118]. Dataeksportøren skal for hver enkelt kontraktslige og organisatoriske foranstaltning kunne påvise, at disse har en egentlig effekt i forhold til opretholdelse af det nødvendige beskyttelsesniveau[119]

## 11.1 Format af oplysninger, der skal overføres (f.eks. almindelig tekst/pseudonymiseret eller krypteret)

Det Europæiske Databeskyttelsesråd har oplistet en ikke udtømmende liste over relevante faktorer, som kan være en indikator på, om en supplerende foranstaltning ville have en reel effekt[120]. Nedenfor vil særligt den tekniske foranstaltning blive analyseret.

[116] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 26
[117] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0, Vedtaget den 18. juni 2021 s. 23, nr. 53
[118] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0, Vedtaget den 18. juni 2021 s. 43
[119] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0, Vedtaget den 18. juni 2021 s. 23, nr. 38
[120] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 23-24, nr. 54

### 11.1.1 Pseudonymisering

Pseudonymisering af personoplysninger er i forordningens art. 4,5 defineret til at være en proces, hvor personoplysninger adskilles således, at fysiske personer udelukkende kan identificeres ved brug af supplerende oplysninger. Det er en forudsætning, at de adskilte data opbevares separat og inden for de europæiske grænser og herved opretholde et tilstrækkeligt beskyttelsesniveau.[121]

I praksis er anvendelse af pseudonymisering mest brugt i forbindelse med analyse inden for sundhedsfaglig forskning, Datatilsynet har i perioden fra den 17.01.2021 til 12.01.2022 givet tilladelse til 11[122] overførsler til usikkert tredjeland af personoplysninger omfattet af forordningens art. 9 og art 10. Tilladelserne er afgivet med hjemmel i databeskyttelseslovens § 10, stk. 3, nr. 1, der tillader behandling af personoplysninger med henblik på *"statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning."* Dette statuerer et snævert anvendelsesområde, men principperne kan formentlig overføres, såfremt dataeksportøren finder, at pseudonymisering er anvendelig som supplerende foranstaltning.

Datatilsynet praksis gennem de 11 tilladelser og Det Europæiske Databeskyttelsesråds (i det følgende EDPB) henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, viser, at EDPB har en strengere vurdering af anvendelsen af pseudonymisering.

Datatilsynet fremsætter en betingelse, som foreskriver, at "Videregivelse af personoplysninger skal ske i pseudonymiseret form, således at oplysningerne ikke er umiddelbart personhenførbare for den modtagende dataansvarlige."*[123]*

Hvorimod EDPB anser pseudonymisering som en effektiv supplerende foranstaltning, såfremt personoplysninger "ikke længere kan henføres til en bestemt registreret eller bruges til at udpege den registrerede i en større gruppe uden brug af yderligere oplysninger."*[124]*

---

[121] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 32
[122] Se litteraturliste
[123] Se litteraturliste
[124] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 32

Datatilsynet anvender terminologien ”*ikke er umiddelbart”,* hvor EDPB anvender *”ikke længere”* i forbindelse med muligheden for igen at kunne identificere individer. Yderligere følger, at EDPB betinger, at pseudonymiserede oplysninger ikke kan anvendes til ”*at udpege den registrerede i en større gruppe*”, hvorimod Datatilsynet anfører *”personhenførbare”.* Der må herudfra tolkes, at Datatilsynet i et vist omfang tillader, at pseudonymiserede oplysninger kan anvendes til at identificere et individ ud fra en større gruppe.

Det skal herudfra konkluderes, at ved anvendelse af pseudonymisering som supplerende foranstaltning stilles der større tekniske krav hos EDPB end hos Datatilsynet. Ydermere er der et snævert anvendelsesområde for pseudonymisering, grundet at pseudonymisering er særdeles ressourcekrævende, og der i praksis ofte er behov for at overføre personhenførbare personoplysninger.

### 11.1.2 Kryptering

Som en supplerende foranstaltning kan personoplysninger overføres til usikkert tredjeland ved brug af kryptering. Ved anvendelse af kryptering kan dataeksportøren nedbringe risici for, at usikkert tredjeland myndigheder kan anvende personoplysninger, da disse over for myndigheder og andre, der ikke har adgang til krypteringsnøgler, vil fremstå i en uforståelig tekst, jf. forordningens præambel nr. 83. Ligeledes er det også fast praksis i de 11 tilladelser afgivet af Datatilsynet, at ”Ved transmission af fortrolige og følsomme personoplysninger over internettet eller eksterne netværk skal den dataansvarlige som minimum anvende passende kryptering.”[125]

Kryptering af personoplysninger kan være relevant i forbindelse med datalagring hos dataimportøren, hvor dataimportøren ikke har behov for at behandle personoplysninger i klar tekst. Det er en forudsætning, at kryptering kan modstå forsøg på kryptering af uautoriserede personer eller instanser. Derfor skal krypteringen til hver en tid leve op til det tekniske niveau og være af en robusthed, som kan modstå kryptoanalyse foretaget af myndigheder i modtagerlandet.

[125] Se litteraturliste under ”Tilladelser”

Krypteringsnøglen skal opbevares inden for de europæiske grænser eller i sikre tredjelande, som har tilstrækkeligt beskyttelsesniveau, dog fortsat under fuld kontrol af dataeksportøren, men kan udledes enten ved at give adgang eller ved at lagre krypteringsnøglen ved betroet tredjemand.[126]

Denne krypteringsløsning er anvendelig i de tilfælde, hvor personoplysninger udelukkende skal opbevares og ikke behandles af dataimportøren. Her skal behandling ikke forstås som i forordningens art. 4,2. Denne type af overførsler er i forordningen defineret som en behandling. Men behandlingen i den forståelse, at dataimportøren ikke rent forretningsmæssigt skal yde en service, for eksempel håndtering af forespørgsler eller applikationer[127].

### 11.1.3 Cloudservices

Behovet for cloudservices er over kort tid blevet meget stor, hvilket indebærer, at mange servicer til både det kommercielle marked og forbrugere påkræver, at der anvendes en cloudbaseret leverancemodel[128]. Der findes et utal af konstellationer af cloudservices, der anvendes. Bredt i samfundet af almenkendte kan nævnes Google Cloud med blandt andet Google Drive, Microsoft 365 med blandt andet Outlook, OneNote og Teams[129] og Appel med iCloud. Cloudservices kan yde mere standardiserede ydelser med snæver adgang for dataeksportøren at fastsætte supplerende foranstaltninger i form af kontraktlig eller organisatorisk art til at omhandle komplekse ydelser, hvor dataeksportøren kan have en større indflydelse på anvendelse af kontraktlig eller organisatorisk supplerende foranstaltning.[130]

Uanset omfanget af dataeksportørens adgang til nærmere regulering af en databehandlingsaftale med udbyderen af cloudservices gennem brug af kontraktlig eller organisatorisk supplerende foranstaltning, vil disse supplerende foranstaltninger have manglende effekt[131] over for et tredjeland, hvis lovgivning, der tillader, at myndigheder kan give et påbud til cloududbyderen om at udlevere krypterede data samt tilhørerede krypteringsnøgle. Derved har myndighederne adgang til personoplysninger i klartekst, som derfor er personhenførbare. Heriblandt har de amerikanske myndigheder gennem §

---

[126] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 31-32
[127] Datatilsynet, *Vejledning om cloud*, marts 2022, s. 3
[128] Datatilsynet, *Vejledning om cloud*, marts 2022, s.8
[129] https://global.techradar.com/da-dk/news/bedste-lagerplads-i-skyen , tilgået den 02.05.2022
[130] Datatilsynet, *Vejledning om cloud*, marts 2022, s,3
[131] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 23, nr. 53

1881 a i 50 USC FISA, sec. 702 adgang til at pålægge amerikanske dataimportører at udlevere personoplysninger, der er dem i hænde, samt ligeledes at udlevere krypteringsnøgler.

I forbindelse med cloudservices kan en teknisk supplerende foranstaltning som pseudonymisering ikke anvendes, grundet at cloududbyderen har behov for at kunne behandle klartekst for at kunne udføre den tildelte opgave. Herved er der ingen af de to teknisk supplerende foranstaltninger, som giver en reel effekt i forbindelse med at bringe beskyttelsesniveauet op til et niveau, som i det væsentlige svarer til det, som findes inden for de europæiske grænser. Det fremgår af henstilling nr. 01/2020 fra Det Europæiske Data Beskyttelsesråd (EDPB), at der på *"baggrund af det aktuelle tekniske niveau, ikke i stand til at forestille sig en effektiv teknisk foranstaltning, som kan forhindre denne adgang i at krænke den registreredes grundlæggende rettigheder."*[132] Denne praksis fastholdes af Datatilsynet i *Vejledning om cloud marts 2022*.

## 11.2 Del konklusion

Særlig relevant for effekten af supplerende foranstaltninger er, i hvilket omfang lovgivningen i usikkert tredjeland har adgang til at give påbud om udlevering af personoplysninger i klar tekst, som dataimportøren er i besiddelse af eller har adgang til. I det tilfælde, udgør brugen af krypterede personoplysninger hvor dataimportøren ligeledes har adgang til krypteringsnøglen, ikke en tilstrækkelig effekt. Anvendelse af kryptering, hvor krypteringsnøglen opbevares inden for de europæiske grænser og ikke kan anvendes eller tilgås af dataimportøren, vil det udgøre en effektiv beskyttelse, såfremt krypteringen under hele behandlingsperioden holdes opdateret i forhold til den tekniske udvikling samt er tilstrækkelig robust til at modstå forsøg på af kryptering foretaget af usikkert tredjelands myndigheder.

De ovenstående tekniske foranstaltninger vil ofte blive udfordret. Dette grundet et behov for at dataimportøren skal kunne tilgå personoplysninger i klartekst, for at kunne levere sine serviceydelser. Det er i denne forbindelse ikke praktisk anvendeligt at overføre personoplysninger i pseudonymiseret eller krypteret form, og beholde krypteringsnøglen inden for EU-grænser.
Det må heraf udledes, at der er en snæver adgang for dataeksportøren til at sikret et tilstrækkeligt beskyttelsesniveau gennem anvendelsen af tekniske foranstaltninger.

---

[132] EDBP, Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger, Version 2.0 Vedtaget den 18. juni 2021 s. 36

Vedrørende de kontraktslige og organisatoriske foranstaltninger, er disse relevante i forhold til at regulere behandlinger af personoplysninger hos dataeksportøren. Dels i dennes interne behandling af hvilke medarbejdere der har adgang til personoplysninger, og i hvilket format, samt at kunne regulere, hvorledes dataimportøren skal samarbejde med offentlige myndigheder. Men disse foranstaltninger kan ikke retsligt forpligte offentlige myndigheder, hvilket kan have stor negativ indflydelse på effekten af foranstaltningerne.

# 12. Samtykke

Det nærværende afsnit skal klarlægge mulighederne for at anvende samtykke som behandlingsgrund eller som supplerende foranstaltning ved overførsel til usikkert tredjeland. Indledningsvis vil definitionen af samtykke blive belyst. Herefter vil centrale elementer blive nærmere analyseret, og sag C-673/17 Planet49, sag C-61/19 Orange Romania samt Datatilsynets afgørelse med journalnummer 2021-431-0145 af 17.03.2022 vil blive analyseret. Afslutningsvis vil anvendeligheden af samtykke i praksis blive diskuteret.

Samtykke som begreb er historisk set knyttet til, at samtykkegiveren har haft kontrol med, hvilke oplysninger som, denne tillader, bliver anvendt. Denne selvbestemmelse over personoplysninger er derfor også tæt forbundet med grundrettighederne og frihedsrettighederne. Med naturligt afsæt heri er anvendelse af samtykke underlagt skærpet krav, da samtykke i nogle tilfælde kan betyde, at samtykkegiveren (i det følgende den registrerede) giver afkald på sine grund- og frihedsrettigheder. Afledt af denne selvbestemmelse følger også, at den registrerede har adgang til at tilbagekalde afgivet samtykke. Denne tilbagetrækning af samtykke kan ikke karakteriseres som at have tilbagevirkende kraft, men skal hindre, at samtykke, som nu er tilbagetrukket, kan udgøre et behandlingsgrundlag. Dette vil betyde, at dataansvarlig skal anvende et andet behandlingsgrundlag eller indstille behandling af personoplysninger.[133]

Det følger af forordningens art. 6, 1, at en behandling udelukkende er lovlig, såfremt mindst et af behandlingsgrundlagene er opfyldt. Forordningens art. 6 indeholder bestemmelser om

[133] Artikel 29-Gruppen (WP 187), Udtalelse 15/2011 om definitionen af samtykke, vedtaget den 13. juli 2011, s. 9 ff

behandlingsgrundlagene for almindelige personoplysninger. Derfor er personoplysninger om race, etnisk oprindelse, politisk, religiøs, filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data og biometriske data, som er underlagt forordningens art. 9 (i praktisk anset for at være særligt personfølsomme oplysninger), som udgangspunkt ikke inkluderet. Derfor kan forordningens art. 6 ikke anvendes som behandlingsgrundlag for personoplysninger underlagt forordningens art. 9. Udgangspunktet er blevet modificeret i 2019 af EDPB og nærmere belyst af det danske Datatilsyn. Herefter er behandling af personoplysninger, som er omfattet af forordningens art. 9, tillige underlagt behandlingsgrundlagene i forordningens art. 6.[134] Samtykke kan derfor udgøre et af behandlingsgrundlagene, som kan anvendes til personoplysninger underlagt forordningens art. 6 samt art. 9. Det følger af forordningen art. 6, 1, litra a, at: *"Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål."*

Heraf kan det konkluderes, at samtykke kan udgøre et behandlingsgrund, som har et eller flere specifikke formål. Ydermere fremgår det af forordningens præambel nr. 40, at behandling *"bør"* baseres på et samtykke eller et være lovbestemt. Det kan ikke udledes af forordningen, om eller i hvilket omfang samtykke skulle have forrang frem for andre behandlingsgrundlag. Men det er et centralt princip, at den registrerede har egen bestemmelse over sine personoplysninger og anvendelsen heraf.[135]

For at et samtykke skal være gyldigt, er der en række krav, som skal være opfyldt. I forordningens art. 4,11 er samtykke afgivet fra den registrerede defineret således: *"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"*

Denne definition kan for overblikkets skyld opdeles i individuelle betingelser, som i det følgende vil blive behandlet enkeltvis. Disse individuelle betingelser er som følger: *frivillig, specifik, informeret* samt *utvetydig*. Herudover skal forordningens art. 4, 11 læses i sammenhæng med forordningens art.

---

[134] Pressemeddelelse fra Datatilsynet den 07.11.2019, *Behandling af følsomme oplysninger*, https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/nov/behandling-af-foelsomme-oplysninger?fbclid=IwAR0Zgt9tyjXRXwFET4aMd3Fn6Q4Tt5uk0kUOozMhmEMdBS9KF3LwnYI-aiU, tilgået den 04.04.2022

[135] Udsen*, It-Ret,* 2021, 5. udgave, s. 321

7, som fastsætter yderligere betingelser for samtykke, samt forordningens præambel nr. 32, nr. 42 og nr. 43[136].

## 12.1 Frivillighed

Det er et afgørende element, at samtykke er afgivet frivilligt og frit, samt at den registrerede har mulighed for at afvise eller på et hvilket som helst tidspunkt kan trække sit samtykke tilbage, uden dette skal påvirke den registrerede negativt.137 Artikel 29-Gruppen har i WP 131 anført angående elektroniske patientjournaler og "*frivillighed*" at ved: *"samtykke menes en viljesbeslutning, som en person, der er ved sine evners fulde brug, har truffet uden nogen form for tvang af social, økonomisk, psykologisk eller anden art. Ethvert samtykke, der er afgivet under trussel om, at den pågældende ikke vil blive behandlet eller få en dårligere behandling, kan ikke anses for at være frivillig"* [138].

Beskrivelsen ovenfor kan anses for at være særdeles omfangsrig, idet den dækker over, at et samtykke kun kan anses for at være gyldig, såfremt det er afgivet "*uden nogen form for tvang af social, økonomisk, psykologisk eller anden art"*[139].

I forhold til, om den registrerede "*bliver behandlet eller får en dårligere behandling",* fremgår det af forordningens præambel nr. 42, at et samtykke ikke kan anses for at være frivilligt i det omfang, at den registrerede *"ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende."* Herudfra fremgår det, at i det omfang, at et samtykke kan være til "*skade"* for den registrerede, anses det afgivne samtykke ikke som at have været et udtryk for frivillighed.

Frivilligheden er yderligere behandlet i forordningens art. 7, 4, hvoraf det fremgår: "Ved vurdering af, om samtykke er givet frit, tages der størst muligt hensyn til, bl.a. om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendige for opfyldelse af denne kontrakt." Heraf kan det udledes, at såfremt et samtykke er afgivet på baggrund af, at den registrerede ikke kan modtage en modydelse uden samtidig at

[136] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s. 7.
[137] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel 42
[138] Artikel 29-Gruppen (WP 187), *Udtalelse 15/2011 om definitionen af samtykke,* vedtaget den 13. juli 2011, s. 13
[139] Artikel 29-Gruppen (WP 187), *Udtalelse 15/2011 om definitionen af samtykke,* vedtaget den 13. juli 2011, s. 13

samtykke til behandling af personoplysning, som ikke er "nødvendig" for at opfylde hovedydelsen, kan det afgivne samtykke ikke anses for at være frivilligt.

Ved vurdering af frivillighed skal der tages hensyn til, om der foreligger en magtubalance mellem den registrerede og dataansvarlige. Af forordningens præambel nr. 43 fremgår det, at samtykke ikke kan udgøre et gyldigt samtykke, når der foreligger en "*klar skævhed*" mellem den registrerede og den dataansvarlige. I præamblen er offentlige myndigheder særligt fremhævet, grundet at der ofte vil foreligge få eller ingen realistiske alternativer for den registrerede i forhold til at afgive sit samtykke den til offentlige myndigheders behandlingsvilkår[140]

Artikel 29-Gruppen fremhæver ligeledes problematikken i WP 187, ved at offentlige myndigheder anvender samtykke som behandlingsgrundlag i tilfælde, når den offentlige myndighed har "*autoritative beføjelser - f.eks. retshåndhævende myndigheder*" [141]. Yderligere kan der foreligge tilfælde, hvor offentlige myndigheder har mulighed for at tilbyde den registrerede "*tillægstjenester*", der i teorien giver den registrerede mulighed for at vælge til eller fra gennem samtykke, men i realiteten vil der ofte foreligge et moment af tvang fra den offentlige myndigheds side. Det skal herudfra udledes, at offentlige myndigheder har en meget accessorisk adgang til at anvendes samtykke som behandlingsgrundlag. Hertil foreligger der gennem forordningens art. 6,1, litra c og litra e, et bedre behandlingsgrundlag for offentlige myndigheders aktiviteter[142].

Ubalance i magtforhold forefindes ikke udelukkende mellem den regerende og offentlige myndigheder, men kan også opstå i ansættelsesforhold eller andre forhold. Disse forhold vil ikke blive nærmere behandlet i denne fremstilling, og for disse forhold gælder samme udgangspunkt som for offentlige myndigheder, nemlig at enhver form for direkte eller indirekte pres eller omstændigheder, som kan have en negativ indflydelse på den registreredes frie vilje til at afgive samtykke, vil dette som udgangspunkt blive opfattet som et ugyldigt samtykke.[143]

---

[140] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s. 8
[141] Artikel 29-Gruppen (WP 187), *Udtalelse 15/2011 om definitionen af samtykke,* vedtaget den 13. juli 2011, s. 17
[142] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s. 8
[143] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s. 7

### 12.1.1 Krav om granularitet

I det tilfælde, hvor dataansvarlig ønsker at anvende den registreredes personoplysninger til flere forskellige behandlingsformål, er det en forudsætning for frivillighed, at den registrerede kan foretage særskilt samtykke for hver type behandling[144]. I forordningens præambel nr. 43 fremsættes der en formodning om, at et samtykke ikke er frivilligt i de tilfælde, hvor den registrerede, ikke har en "*mulighed for at give særskilt samtykke til forskellige behandlingsaktiviteter"*[145]. Yderligere fremgår det af forordningens art. 7, 2, at den registrerede skal kunne skelne mellem forskellige forhold i sit samtykke. Datatilsynet anfører, at et samtykke godt kan være angivet på samme formular, såfremt den registrerede har mulighed for at foretage individuelle valg i forhold til, hvilke behandlingsformål der gives samtykke til[146].

### 12.1.2 Skade

Det er yderligere en forudsætning for frivillighed, at den registrerede kan nægte eller tilbagekalde sit samtykke. Det påhviler den dataansvarlige at påvise, at en nægtelse eller tilbagekaldelse af samtykke ikke vil få en klar ulempe økonomisk. Yderligere kan skade for den registrerede ske gennem *"vildledning, intimidering, tvang eller væsentlige negative konsekvenser"*[147]. Dette underbygges yderligere i forordningens præambel 42, hvoraf det fremgår, at et samtykke bør anses for gyldigt i det omfang, at den registrerede har et *"reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende."*

Som yderligere fortolkningsbidrag til begrebet "frivilligt" vil dette blive analyseret nedenfor gennem sag C-673/17 Planet49 samt sag C-61/19 Orange România og slutningsvis Datatilsynets afgørelse med journalnummer 2021-431-0145 af 17.03.2022, som er en afgørelse i en sag om brugen af et system til ansigtsgenkendelse. Afgørelsen fra Datatilsynet og særligt EU-Domstolen samt generaladvokaten udgør, jf. nærværende fremstillings afsnit om retskildevurdering, en betydelig værdi i forbindelse med fastlæggelse af gældende ret.

---

[144] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s. 13
[145] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel nr. 43
[146] Datatilsynet, *Vejledning Samtykke*, maj 2021, s. 9
[147] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020 side 13

### 12.1.3 C-673/17 Planet49

Sagens parter er på den ene side Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, en forbundssammenslutning af forbrugerforeninger placeret i Tyskland, og på den anden side Planet49 GmbH (i det følgende Planet49), et firma, som beskæftiger sig med onlinekonkurrencer[148]. Dommen er afsagt den 1. oktober 2019. Sagens faktum er, at i 2013 har Planet49 afholdt en salgsfremmende konkurrence online. Det var en forudsætning for at deltage i konkurrencen, at den registrerede indtastede sit postnummer, hvorefter der skete en viderestillelse til en anden internetside, hvor den registrerede skulle opgive navn og adresse. På samme side var der to tekststykker, som skulle udgøre den registreredes samtykke, hvoraf den ene i afkrydsningsfeltet på forhånd var afkrydset.

Af den første tekst, som i afkrydsningsfeltet ikke forud var afkrydset (i det følgende første afkrydsningsfelt), fremgik følgende:

”Jeg er indforstået med, at sponsorer og samarbejdspartnere via post eller telefonisk eller via e-mail/sms informerer mig om tilbud inden for deres respektive forretningsområder. Disse kan jeg selv fastlægge her, ellers foretager arrangøren valget. Jeg kan til enhver tid tilbagekalde mit samtykke. Yderligere oplysninger herom kan findes her.” [149]

Af den anden tekst, som i afkrydsningsfeltet forud var afkrydset (i det følgende anden afkrydsningsfelt), fremgik følgende:

”Jeg er indforstået med, at webanalysetjenesten Remintrex anvendes hos mig. Dette har til følge, at konkurrencearrangøren [Planet49] efter registrering til konkurrencen installerer cookies, hvilket gør det muligt for Planet49 at foretage en analyse af min surf- og anvendelsesadfærd på reklamepartneres websites og dermed åbner mulighed for interessemålrettet reklame ved hjælp af Remintrex. Jeg kan til enhver tid slette disse cookies. Læs mere her.”*[150]*

[148] C-673/17, Planet49, præmis nr. 2
[149] C-673/17, Planet49, præmis nr. 25-26
[150] C-673/17, Planet49, præmis nr. 27

Brugen af cookies giver Planet49 mulighed for at analysere den registreredes adfærdsmønstre online. Disse cookies får tildelt et nummer, som kan tilbageføres til den registrerede, som har angivet sit navn og adresse. Såfremt der sker en sammenknytning af disse informationer, vil der foreligge en behandling af personhenførbare personoplysninger. Det kan udledes af det andet afkrydsningsfelt, at Planet49 foretager en sådan sammenknytning med henblik på "*interessemålrettet reklame"* over for den registrerede. Planet49 anser andet afkrydsningsfelt for at udgøre et gyldigt samtykke til at indsamle samt behandle personoplysninger samt ikke-anonyme informationer.[151]

12.1.3.1 Analysespørgsmål

Ovenstående sag vil blive analyseret for at klarlægge gældende ret for følgende:

1. Er samtykke i første afkrydsningsfelt nødvendigt i forhold til hovedydelsen, og i hvilket omfang er dette foreneligt med forordningens art. 7,4
2. Kan det andet afkrydsningsfelt, hvoraf der forud er afkrydset i et felt, anses for at være et frivilligt samtykke?
3. Er kravet til granularitet i forbindelse med samtykke iagttaget?

Indledningsvis skal henvisninger til direktiv 95/46 (databeskyttelsesdirektivet) anses for at være henvisning til forordningen, jf. forordningens art. 94,2. EU-Domstolen vil afgive sin besvarelse på den indgivne sag ved både at behandle direktiv 95/46 samt forordningen[152].

**Spørgsmål 1: Er samtykke i første afkrydsningsfelt nødvendigt i forhold til hovedydelsen, og i hvilket omfang er dette foreneligt med forordningens art. 7, 4**

Dette spørgsmål skal yderligere klarlægge anvendelse af forordningens art. 7, 4, hvoraf det blandt andet fremgår, at ved vurdering af et frit samtykke kan sådant et samtykke ikke foretages i det omfang, at der også samtykkes til unødvendige betingelser for at modtage hovedydelsen.

I det første afkrydsningsfelt, som ikke forud var afkrydset, var deltagelse i den salgsfremmende konkurrence betinget af, at der blev foretaget en afkrydsning i dette felt af den registrerede.[153].

[151] C-673/17, Planet49, præmis nr.45
[152] C-673/17, Planet49, præmis nr.43
[153] C-673/17, Planet49, præmis nr.28

Det følger af sagens faktum, at registrerede med et samtykke skulle deltage i en salgsfremmende konkurrence.[154] Dette må anses for at være hovedydelsen, hvoraf der er et underliggende "salg" af personoplysninger. Modydelsen fra den registrerede er, at sponsorer og samarbejdspartnere efterfølgende kunne kontakte den registrerede med tilbud på baggrund af de indsamlede personoplysninger. Generaladvokaten anfører, at denne situation statuerer, at der er et enligt behov for at behandle disse personoplysninger, og derfor er det nødvendigt for at kunne opfylde den kontrakt, den registrerede indgår i forbindelse med deltagelse i konkurrencen[155]. Derfor har dette forhold hjemmel i forordningens art. 7,4.

EU-Domstolen har afholdt sig fra at behandle denne problemstilling specifikt, men anfører, at i det tilfælde, hvor den registreredes deltagelse i en salgsfremmende konkurrence på betingelse af, at der kan foretages behandling af dennes personoplysninger i forbindelse med reklameformål, kan dette samtykke anses for at være foreneligt med kravet om frivilligt samtykke.[156]

Der kan ud af ovenstående besvares bekræftende på spørgsmålet om nødvendigheden af modydelser for at kunne opfylde hovedydelsen i tilfælde, hvor modydelsen omhandler "*salg*" af personoplysninger i forbindelse med salgsfremmende konkurrence.

**Spørgsmål 2: Kan det andet afkrydsningsfelt, hvoraf der forud er afkrydset i et felt, anses for at være et frivilligt samtykke?**

Til besvarelse af dette spørgsmål henvises der i Planet49 til præmis nr. 52 til generaladvokatens forslag til afgørelsen, punkt nr. 60. Heraf fremgår det, at et samtykke skal være udtryk for en "aktiv handling". Denne aktive handling tilsigter, at den registrerede har læst og forstået samt ikke har indsigelser til det samtykke, den registrerede tiltænker at afgive. I det modsatte tilfælde ved en passiv handling, som et forudafkryds i afkrydsningsfelt, som kan ses i Planet49's andet afkrydsningsfelt, ikke kan fastslå, om der foreligger et samtykke, som er afgivet frivilligt, grundet at den registrerede muligvis ikke har forholdt sig aktivt til det pågældende samtykke.[157]

---

[154] C-673/17, Planet49, præmis nr.2
[155] C-673/17, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 21. marts 2019, præmis nr.99
[156] C-673/17, Planet49, præmis nr.64
[157] C-673/17, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 21. marts 2019, præmis nr. 61-62

Dette underbygges af Planet49's præmis nr.52, hvoraf det fremgår, at det er *"praktisk umuligt objektivt at afgøre",* om den registrerede har givet sit samtykke, når sådan et samtykke er baseret på en passiv handling hos den registrerede, grundet at det ikke kan fastslås med sikkerhed, at den registrerede reelt har forholdt sig gennem læsning eller forståelse af indhold til sit samtykke. Ydermere fremgår det af forordningens art. 4,11, at et samtykke skal udgøre en: *"erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling".*

"*Klar bekræftelse"* må siges at udeblive i de situationer, hvor den registrerede bliver mødt med et samtykke, som er forudafkrydset. Dette underbygges ligeledes af forordningens præambel nr. 32, der i forbindelse med samtykke ved afkrydsning i felt på hjemmesider fastslår, at *"tavshed, forudafkrydsede felter eller inaktivitet"* ikke kan tjene som et samtykke.

**Spørgsmål 3: Er kravet til granulatet i forbindelse med samtykke iagttaget?**

Generaladvokaten anfører, at der i forbindelse med det andet afkrydsningsfelt foreligger et samtykke til to forskellige behandlingsforhold, det ene forhold er deltagelse i konkurrencen, og det andet forhold er installation af cookies[158]. Grundet at disse to behandlingsforhold er underlagt et samtykke, og at den registrerede, ikke har haft mulighed for at foretage særskilt samtykke, forligger der ikke et granuleret samtykke.

Ud fra ovenstående kan det derfor sluttes, at brugen af forudafkrydsning i afkrydsningsfeltet ikke udgør den fornødne sikkerhed for, at den registrerede har afgivet sit samtykke frivilligt. Den dataansvarlige skal i forbindelse med samtykke sikre, at der bliver afgivet samtykke af den registrerede på baggrund af en aktiv handling. Tillige at der ikke til hvert behandlingsforhold er mulighed for at samtykke eller nægte et specifikt behandlingsforhold.

### 12.1.4 C-61/19 Orange România

Sagens parter er på den ene side Orange România SA (Orange România), der er leverandør af mobilkommunikationstjenester på det rumænske marked[159], og på den anden side Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), som er den nationale

[158] C-673/17, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 21. marts 2019, præmis nr. 89
[159] C-61/19 Orange România præmis nr. 12

tilsynsmyndighed for behandling af personoplysninger i Rumænien[160]. Dommen er afsagt den 11. november 2020.

Sagens faktum er som følger, at Orange România i en periode fra den 1. marts 2018 til den 28. marts 2018 har indgået skriftlig aftale om levering af mobiltelekommunikationstjenester med fysiske personer. Som tillæg til denne skriftlige aftale anvender Orange România de registrerede identitetsbeviser, såfremt den registrerede havde samtykket hertil. ANSPDCP anfægtede, at der ikke var afgivet gyldigt samtykke til at indsamle samt opbevare disse personoplysninger. I forbindelse med anvendelse af kopi af identitetsbeviser, fremgik det af de aftalevilkår, som blev oplæst af Orange Românias personale til den registrerede, at den registrerede blandt andet samtykkede til *"opbevaring af genparter af dokumenter med personoplysninger, der muliggør identifikation af kunden"*[161]. Samtykke blev afgivet på sådan en måde, at det var Orange Românias personale, som oplæste aftalevilkårene, og som på forhånd foretog afkrydsning af felter på vegne af den registrerede. Afslutningsvis underskrev den registrerede aftalen.[162]

I de tilfælde, hvor den registrerede ikke ønskede at afgive samtykke, men fortsat ønskede at indgå aftale om levering af mobiltelekommunikationstjenester, skulle den registrerede selv udfylde og underskrive en håndskrevet formular om nægtelsen [163].

12.1.4.1 Analyse spørgsmål

Ovenstående sag vil blive analyseret for at klarlægge gældende ret for følgende:

1. Kan supplerende foranstaltninger, der påkræves i tilfælde, hvor den registrerede nægter at samtykke til forhold i aftalen, påvirke frivilligheden?
2. Foreligger der frivillighed i det omfang, at den registrerede underskriver en kontrakt, hvor der på forhånd var afkrydset i felter, som bekræftede den registreredes samtykke?

[160] C-61/19 Orange România præmis nr. 13
[161] C-61/19 Orange România præmis nr. 48
[162] C-61/19 Orange România præmis nr. 43
[163] C-61/19 Orange România præmis nr. 45

Indledningsvis skal henvisninger til direktiv 95/46 (databeskyttelsesdirektivet) anses for at være henvisning til forordningen, jf. forordningens art. 94,2. EU-Domstolen vil afgive sin besvarelse på den indgivne sag ved både at behandle direktiv 95/46 samt forordningen.[164]

**Spørgsmål 1: Kan supplerende foranstaltninger, der påkræves i tilfælde, hvor den registrerede nægter at samtykke til forhold i aftalen, påvirke frivilligheden?**

I forbindelse med besvarelsen af dette spørgsmål er det relevant at anvende generaladvokatens forslag til afgørelsen af sag C-61/19, idet generaladvokaten foretager en mere dybdegående besvarelse af emnet[165]. Det fremgår af sagens faktum, at i det tilfælde, den registrerede ikke ønskede at afgive samtykke til kopiering og lagring af identitetsbeviser, skulle den registrerede selv i håndskrevet form angive, at denne ikke ønskede at give samtykke til dette formål.[166]

Generaladvokaten finder, at dette forhold ikke kan statuere, at der er afgivet gyldigt samtykke, og at frivilligheden er blevet påvirket i negativ grad gennem opsatte foranstaltninger, der gør det sværere ikke at afgive samtykke end ved at afgive samtykke. Udgangspunktet bør være, at der *"kræves derfor en positiv handling fra den registreredes side for at tilkendegive samtykke"*[167]. I nærværende sag betyder førnævnte foranstaltning, at der*" kræves en positiv handling for at nægte samtykke"*[168]. EU-Domstolen anfører yderligere, at sådan en type foranstaltning har en *"uretmæssig"*[169] indflydelse på frivilligheden.

**Spørgsmål 2: Foreligger der frivillighed i det omfang, at den registrerede underskriver en kontrakt, hvor der på forhånd var afkrydset i felter, som bekræftede den registreredes samtykke?**

Af sagens faktum fremgår det, at Orange Românias personale på forhånd havde afkrydset felter, som skulle bekræfte den registreredes samtykke. Efterfølgende blev den registrerede informeret om de faktiske forhold, som den registrerede samtykkede til[170]. Det skal herudfra udledes, at den registrerede ikke selv har foretaget en aktiv handling i forbindelse med afkrydsning af felter, som skulle

[164] C-61/19 Orange România præmis nr. 32
[165] C-61/19 Orange România præmis nr. 50
[166] C-61/19, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 4. marts 2020, præmis nr. 60
[167] C-61/19, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 4. marts 2020, præmis nr. 60
[168] C-61/19, *forslag til afgørelsen fra generaladvokaten*, M.Szpunr. 4. marts 2020, præmis nr.60
[169] C-61/19 Orange România præmis nr. 50
[170] C-61/19 Orange România præmis nr. 45

bekræfte et samtykke, men blot blev informeret om indholdet af sit samtykke. Med denne manglende aktive handling kan der ikke statueres frivillighed.[171] Dette underbygges af sag Planet49, som er analyseret i det ovenstående, hvor udeblivelse af en aktiv handling ligeledes ikke kan anses for at være et gyldigt samtykke.

Men det fremgår af Orange România, at den registrerede underskrev aftalen, hvor de afkrydsede felter fremgik af aftalernes indhold[172]. Underskriften må i sig selv være et udtryk for en aktiv handling, men med denne underskrift kan Orange România ikke med rimelig sikkerhed godtgøre, at den registrerede faktisk har læst og særlig relevant for denne sag forstået, hvilke betingelser denne samtykkede til. Dette er ikke foreneligt med frivillighedsbegrebet, jf. generaladvokatens punkt 45.[173] Dette underbygges yderligere af, at det i forordningens præambel nr. 32 fremgår, at en handling i forbindelse med samtykke skal fremgå "*tydeligt*".

### 12.1.5 Datatilsynets afgørelse i en sag om brugen af et system til ansigtsgenkendelse

Sagens parter er på den ene side Datatilsynet, den danske tilsynsmyndighed, hvis kompetencer fremgår af forordningens art. 55, og hvis opgaver fremgår af forordningens art. 57, og på den anden side FysioDanmark Hillerød ApS (FysioDanmark), som tilbyder fysioterapi, genoptræning og generelt fitnesscenter[174]. Afgørelsen er truffet den 17. marts 2022 og har journalnummer 2021-431-0145.

Sagens faktum er, at FysioDanmark påtænker at anvende et ansigtsgenkendelsessystem i deres center, og dette system skulle blandt andet anvendes til adgangskontrol for deres kunder samt medarbejdere. Anvendelse af dette system skulle baseres på et samtykke, hvor den registrerede samtykkede til behandling af følgende personoplysninger: navn, fødselsdato, adresse, e-mail samt portrætfoto. I forbindelse med tilbagekaldelse eller nægtelse af samtykke fremgår følgende: *"Hvis du ikke ønsker at give samtykke, eller hvis du tilbagekalder dit samtykke, så er det ikke muligt at benytte biometrisk scan, og vi beder dig derfor kontakte dit fitnesscenter for at høre om alternative løsninger"*[175]. I det tilfælde, at den registrerede ikke ønskede anvendelse af ansigtsgenkendelsessystem, kunne denne anvende nøglekort og kode for at dokumentere aktivt medlemskab.

---

[171] C-61/19 Orange România præmis nr. 46
[172] C-61/19 Orange România præmis nr. 46
[173] C-61/19 Orange România præmis nr. 46
[174] https://fysiodanmarkhillerod.dk/om-os, tilgået den 8. maj 2022
[175] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse,tilgået den 8. maj 2022

12.1.5.1 Analyse spørgsmål

Ovenstående sag vil blive analyseret for at klarlægge gældende ret for følgende:

1. Kan supplerende foranstaltninger, der påkræves i tilfælde, hvor den registrerede nægter at samtykke til forhold i aftalen, påvirke frivilligheden?

**Spørgsmål 1: Kan supplerende foranstaltninger, der påkræves i tilfælde, hvor den registrerede nægter at samtykke til forhold i aftalen, påvirke frivilligheden?**

Den registrerede skal i tilfælde af nægtelse til samtykke foretage en yderligere aktiv handling og skal kontakte FysioDanmark for at kunne få stillet alternative løsninger til ansigtsgenkendelsessystem til rådighed, såfremt den registrerede fortsat ønsker at anvende centerets faciliteter.

Det fremgår af afgørelsen, at Datatilsynet ikke har forholdt sig konkret til dette spørgsmål. Men i mellemtiden har Datatilsynet bekræftet, at denne type samtykke anses for gyldig, og derfor skal det udledes, at denne form for samtykkes sammensætning ikke begrænser frivillighed[176]. Det kan udledes heraf, at Datatilsynet ikke anser det førnævnte vilkår for at være *"urimeligt"*[177] og udgøre en foranstaltning, som kan være til "*skade*"[178] for den registrerede, som nægter at samtykke.

## 12.1.6 Del konklusion frivillighed

Dette afsnit har til formål at opsamle på hele afsnittet om frivillighed, der har inddraget lovgivning, vejledninger fra EDPB, Datatilsynet samt Artikel 29-Gruppen og sluttelig retspraksis. Det kan herudfra konkluderes, at frivilligheden har stor betydning for gyldigheden af et samtykke, hvilket også underbyggedes af, at frivilligheden i sit udgangspunkt giver den registrerede selvbestemmelse over, hvilke personoplysninger som, denne samtykker til, bliver behandlet.

I sagen Planet49 blev det bekræftet, at det var nødvendigt, at den registrerede samtykkede til at "sælge" sine personoplysninger for at opretholde sine forpligtelser i forhold til hovedydelsen, som

[176] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse under punkt 2.2, tilgået den 8. maj 2022
[177] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel 42
[178] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, præambel 42

var en salgsfremmende konkurrence. Dette samtykke var i overensstemmelse med forordningens art. 7, 4. Yderligere fastlægger Planet49, at anvendelse af forud afkrydsede samtykkefelter ikke bebudede den fornødne sikkerhed for den registrerede, som havde afgivet sit samtykke frivilligt, og dette var derfor ikke foreneligt med forordningens art. 4,11. Hertil var samtykkeerklæring ikke granuleret i tilstrækkeligt omfang, og derfor kunne der ikke forelægge et gyldigt samtykke.

I sagen Orange România fastslår EU-Domstolen og generaladvokaten, at der med rette kan kræves en aktiv handling fra den registrerede i forbindelse med dennes samtykke. I det modsatte tilfælde som i Orange România, hvor det krævede en aktiv handling at nægte sit samtykke, kan dette have en uretmæssig indflydelse på frivilligheden. Yderligere nuancerer Orange România anvendelse af forudafkrydsede samtykkefelter ved at fastslå, at der fortsat ikke med tydelighed kan statueres en frivillighed hos den registrerede, til trods for med dennes underskrift samtykker til forudafkrydsede samtykkefelter.

Gennem afgørelsen fra Datatilsynet ses det, at såfremt der kræves en aktiv handling fra den registrerede til at afgive sit samtykke, frem for det modsatte, må dette anses for at være et gyldigt samtykke. Yderligere kan det ikke anses for at være en begrænsning i frivilligheden, som var urimelig eller til skade, at den registrerede, såfremt denne nægter at afgive samtykke, af egen drift skulle opsøge andre muligheder gennem adgangskort og kode for fortsat at kunne anvende centerets faciliteter. Dette forhold var derfor foreneligt med forordningens præambel nr. 42.

I det følgende afsnit vil næste forudsætning for et gyldigt samtykke blive behandlet, nemlig kravet om et specifikt samtykke.

### 12.2 Specifikt

Det er en forudsætning for gyldigheden af et samtykke, at det er specifikt. Et specifikt samtykke skal være, at det er forståeligt og klart og præcis fastslår omfanget og konsekvenserne af samtykke af et behandlingsforhold.[179] Kravet om et specifikt samtykke hænger uløseligt sammen med kravet om et informeret samtykke,[180] som vil blive behandlet nedenfor.

[179] Datatilsynet, *Vejledning Samtykke*, maj 2021, s. 10
[180] Artikel 29-Gruppen (WP 187), *Udtalelse 15/2011 om definitionen af samtykke,* vedtaget den 13. juli 2011, s. 18 ff.

Af forordningens art. 6,1, litra a fremgår det, at den registrerede skal give sit samtykke til et eller flere *"specifikke"* formål. Afledt heraf hænger et specifikt samtykke sammen med et granuleret samtykke, grundet at forordningen tillader *"et eller flere"*[181] behandlingsformål, og derfor skal både specifikt og granuleret iagttaget for at opnå et gyldigt samtykke. Kravet om et specifikt behandlingsformål kan også udledes af forordningen art. 5,1, litra b[182], hvoraf det fremgår, at der skal indsamles til *" udtrykkeligt angivne*" formål. Yderligere må de indsamlede personoplysninger ikke viderebehandles uden for dette formål. For at kunne overholde dette princip er det nødvendigt, at formålet er specifikt.

I tilfælde, hvor dataansvarlige ønsker at behandle personoplysninger til flere formål, skal den dataansvarlige foretage foranstaltninger, der sikrer, at den registrerede klart kan skelne mellem de forskellige forhold og foretage en specifik vurdering. En samtykkeerklæring skal være udformet således, at den for en registreret er "*letforståelig"* og i en *"lettilgængelig form og i et klart og enkelt sprog"*[183].

Som yderligere fortolkningsbidrag til begrebet "specifikt" vil dette blive analyseret nedenfor gennem sag C-673/17 Planet49 samt sag C-61/19 Orange România og slutningsvis Datatilsynets afgørelse med journalnummer 2021-431-0145 af 17.03.2022. Dommerne og afgørelsens faktum er fremlagt i afsnittet om frivillighed og vil derfor ikke blive gentaget i dette afsnit. Men centrale præmisser og fakta vil blive tydeliggjort.

I C-673/17 Planet49 fremgår det i forbindelse med den dataansvarliges brug af cookies, at det (i modsætning til i nærværende sag) specifikt fremgår, hvor lang tid cookies er i funktion, efter samtykket er givet. Yderligere skal det fremgå, i hvilket omfang tredjemand har adgang til oplysninger, som er opnået gennem brugen af cookies.[184] Yderligere fremgår det af dommen, at samtykke skal være så specifikt, at det *"vedrører præcist"*[185] det pågældende behandlingsformål, og det kan derfor ikke udledes, at samtykke er afgivet til andet formål.

[181] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 6, 1, litra a
[182] Nielsen og Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, 1. oplag 2020, s. 295.
[183] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 7, 2
[184] C-673/17, Planet49, præmis nr. 81
[185] C-673/17, Planet49, præmis nr. 58

I C-61/19 Orange România er de afkrydsede felter visuelt mere opdelt end i C-673/17 Planet49, men EU-Domstolen finder, at der ikke er opnået tilstrækkelig opdeling af de forskellige aftalevilkår[186].

I Datatilsynets afgørelse med journalnummer 17-03-2022 finder Datatilsynet, at FysioDanmark har opfyldt betingelserne for gyldigt samtykke gennem at oplyse den registrerede entydigt om formålet for behandlingen: *"Dine personoplysninger behandles til det formål at føre kontrol med gyldigheden af dit medlemskab ved adgang til fitnesscentret."*[187] Yderligere har den registrerede haft mulighed for at foretage separate afkrydsninger i forhold til hvert behandlingsformål. I forhold til sproget er der i den pågældende samtykkeerklæring anvendt letforståeligt sprog. Dette ses blandt andet ved, at ordet "biometrisk scan" er uddybet og simplificeret. Hertil er yderligere henvisninger gjort lettilgængelige ved, at der er indsat link med supplerende informationer. Disse foranstaltninger bør anses for at være forenelige med forordningens art. 7, 2.

Som afsnittet blev indledt med, er kravet om specifikt samtykke tæt forbundet med kravet om et informeret samtykke, som vil blive behandlet i følgende afsnit.

### 12.3 Informeret

Kravet om et informeret samtykke følger af behovet for, at den registrerede skal kunne afgive sit samtykke på et informeret grundlagt.[188] Dette er med til at sikre en gennemsigtighed, som er forankret i forordningens art. 5[189]. Dette underbygges af, at der i forordningens præambel 43 fremgår, at den registrerede skal være *"bekendt"* med omfanget af samtykket. Yderligere fremgår det af forordningens præambel 43, at for, at der foreligger et frivilligt samtykke, skal den registrerede som minimum informeres om identitet på den dataansvarlige samt formålet for behandlingen. Dette minimumskrav er blevet udvidet gennem retspraksis, og det følger af C-61/19 Orange România, præmis nr. 40, hvor minimumskravet udvides med, at den registrerede skal informeres om "*type personoplysninger"*, *"varigheden af behandlingen",* samt hvorledes behandlingen foretages.[190] I tilfælde, hvor

[186] C-61/19 Orange România, præmis nr. 47
[187] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse under punkt. 2.1, tilgået den 8. maj 2022
[188] Datatilsynet, *Vejledning Samtykke*, maj 2021, s. 11
[189] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s.16
[190] C-61/19 Orange România, præmis nr. 40

behandlingen af personoplysninger vil blive anvendt til at foretage automatiske afgørelser om den registrerede, skal der i samtykkeerklæringen fremgår informationer herom.[191]

Yderligere følger det af forordningens art. 7,3, at den registrerede skal have oplysning om, at denne til enhver tid kan tilbagetrække sit samtykke. Yderligere er det en forudsætning, at adgangen til at tilbagekalde et samtykke er *"lige så let"* som at afgive det. I modsætning hertil kan nævens C-61/19 Orange România, præmis nr. 45.

I tilfælde, hvor den dataansvarlige vil foretage overførsel af personoplysninger i forbindelse med forordningens art. 46, skal den registrerede informeres om eventuelle risici[192]. Denne adgang til overførsel er særlig relevant for denne fremstilling og vil derfor blive behandlet i et selvstændigt afsnit, under "Undtagelser i særlige situationer, art. 49".

### 12.4 Utvetydigt

I nærværende afsnit vil kravet om utvetydigt samtykke blive behandlet perifert. Samtykke skal have karakter af at være en viljeserklæring, og det skal derfor være afgivet på baggrund af en aktiv handling[193]. Denne aktive handling kan komme til udtryk gennem skriftlig erklæring eller mundtlig erklæring. Samtykket kan yderligere afgives på baggrund af afkrydsning i afkrydsningsboks. Et swipe, et vink foran et smartkamera, at bevæge sin smartphone rundt med uret eller i en ottetalsbevægelse[194] kan være udtryk for et utvetydigt samtykke, hvorimod travlhed eller forudafkrydsede felter eller passivitet ikke kan anses for at være grundlag for gyldigt samtykke, jf. forordningens præambel 32[195]. Under alle omstændigheder skal kravet om utvetydig tolkes restriktivt, således der ikke må foreligge nogen former for tvivl, om der er afgivet samtykke til den påtænke behandling[196].

---

[191] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020, s.16
[192] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020 s. 16
[193] Yderligere behandlet i afsnittet om frivillighed
[194] Datatilsynet, *Vejledning Samtykke*, maj 2021, side 12
[195] Udsen, *It-Ret*, 2021, 5. udgave, s 327
[196] Artikel 29-Gruppen (WP 187), *Udtalelse 15/2011 om definitionen af samtykke,* vedtaget den 13. juli 2011, s. 38

## 12.5 Tilbagekaldelse af samtykke

En af grundbetingelserne for anvendelse af samtykke som behandlingsgrundlag er, at den registrerede til hver en tid kan tilbagekalde et afgivet samtykke. Adgang til tilbagekaldelse skal være lige så let som adgang til at afgive et samtykke. I tilfælde, hvor den registrerede anvender retten til at tilbagekalde et afgivet samtykke, må dette ikke have en negativ indflydelse for den registrerede. Derfor er det blandt andet ikke tilladt at opkræve en afgift i forbindelse med tilbagekaldelse[197]. Dette underbygges af forordningens art. 7, 4.

Anvender den registrerede retten til tilbagekaldelse, skal den dataansvarlige ophøre med at behandle den registreredes personoplysninger uden ugrundet ophold. Dette omfatter ligeledes opbevaring af personoplysninger, da dette ifølge forordningens definition også er behandling. Derfor bør den dataansvarlige foretage en sletning af de pågældende personoplysninger. Ligeledes har den registrerede ret til at kræve personoplysninger slettet[198].

## 12.6 Undtagelser i særlige situationer

Særlig relevant for denne fremstilling er tilfælde, hvor dataansvarlig anvender samtykke som overførselsgrundlag i forbindelse med overførsel til usikkert tredjeland, hvor forordningens art. 45 samt art. 46 ikke tilsikrer et tilstrækkeligt beskyttelsesniveau[199].

Anvendelse af forordningens art. 49, 1, litra a er særdeles restriktiv, anvendelse er betinget af, at den registrerede har givet *"udtrykkelig"* samtykke til overførslen. Desuden skal den registrerede *"informeret om de mulige risici",* der kan foreligge ved den konkrete overførsel.

Yderligere skal overførslen være forenelig med forordningens art. 5 (principper for behandling)[200], art. 4, 11 (definition på samtykke), art. 7 (betingelser for samtykke) samt art. 44 (som fastsætter, at alle bestemmelser i forordningens kapitel V skal anvendes). Anvendelse af forordningens art. 49 må overordnet ikke føre til en underminering af den registreredes grundlæggende rettigheder og

[197] Datatilsynet, *Vejledning Samtykke*, maj 2021, s. 15
[198] Datatilsynet, *Vejledning Samtykke*, maj 2021, s. 15-16
[199] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 46
[200] Nielsen og Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, 1. oplag 2020, s. 809

frihedsrettigheder.[201] Det følger endvidere af EU-retten, at i forbindelse med anvendelse af undtagelser må disse undtagelser ikke over tid blive til reglen. Dette støtter den strenge adgang, der er til at anvende denne bestemmelse.[202]

Nedenfor vil de to bærende principper for anvendelse af forordningens art. 49 blive nærmere behandlet.

### 12.6.1 Udtrykkeligt

Ved anvendelse af det "normale" samtykke, som er blevet behandlet ovenfor, er en af betingelserne, at samtykke skal være *"utvetydigt"*[203]. Der foreligger en strengere betingelse for anvendelse af forordningens art. 49, idet der skal foreligge et *"udtrykkeligt"* samtykke ligesom i forbindelse med behandling af følsomme personoplysninger[204] samt automatiske afgørelser.[205] [206]

Det er en forudsætning, at samtykket bliver givet på sådan en vis, at den registrerede afgiver en udtrykkelig samtykkeerklæring. Til dette formål kan totrinsverifikation anvendes til at sikre gyldigheden. Denne totrinsverifikation kan i praksis anvendes ved først at sende en "almindelig" samtykkeerklæring, som opfylder forordningens art. 4 samt art. 7. Når der samtykkes hertil, sendes et yderligere kontrollink, hvor den registrerede igen, bekræfter sit samtykke.[207]

### 12.6.2 Mulige risici

Den anden yderligere betingelse for anvendelse af forordningens art. 49 er kravet om, at den registrerede skal informeres om mulige risici, der er forbundet i forbindelse med overførsel til usikkert tredjeland, hvor dataansvarlig har vurderet, at der ikke kan stilles fornødne garantier eller supplerende foranstaltninger. De "fund", som dataansvarlig har fundet i forbindelse med vurdering af det pågældende usikkert tredjeland, skal videreformidles til den registrerede. Yderligere skal der informeres

---

[201] EDPB, Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679, Vedtaget den 25. maj 2018 s. 3 ff.
[202] EDPB, Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679, Vedtaget den 25. maj 2018 s. 4
[203] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 4, 11
[204] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 9, 1
[205] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016, art. 22, 2, litra c
[206] EDPB, Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679, Vedtaget den 25. maj 2018 s. 6
[207] EDPB, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020 s. 23

om, hvilken type personoplysninger der overføres og til hvilke tredjelande, og hvem i det usikkert tredjeland som har adgang eller kan få adgang til disse personoplysninger[208].

## 12.7 Del konklusion

Baseret på denne fremstillings analyse, vil følgende konklusion sammenfatte krav til specifikt, informeret og utvetydigt samtykke, samt tilbagekaldelse af samtykke og undtagelser i særlige situationer reguleret i forordning art. 49. Samtykke er nærmere defineret i forordningens art 4, ll. Yderligere skal forordningens art. 7, samt forordningens præambel nr. 32, nr. 42 og nr. 43 iagttages, når den dataansvarlige ønsker at anvende samtykke som overførelsesgrundlag.

Det kan konkluderes, at et samtykke skal gives på specifikt og informeret grundlag. Der kan altså ikke gives samtykke til et bredt anvendelsesområde, da den registrerede, ikke i samme grad har mulighed for at overskue konsekvenserne af sit samtykke. Dette vil også have en negativ indflydelse på det frivillige aspekt af samtykket.

Samtykket skal være opdelt (granulariet) som følge af C-61/19 Orange România samt afgørelsen fra datatilsynet omkring FysioDanmark. Derfor skal den dataansvarlige være opmærksom på, hvordan samtykkeerklæringer er opbygget, således at opdelingen er granuleret. Det skal være muligt for den registrerede at skelne mellem de forskellige forhold, som den dataansvarlige ønsker at behandle personoplysninger på baggrund af.

Hertil skal den dataansvarlige forholde sig til hvem modtageren af en samtykkeerklæring er, da den information, som gøres tilgængelig, skal være letforståelig og lettilgængelig for modtageren. Dette er særligt relevant, når der indgår tekniske løsninger, som for eksempel cookies eller kryptering. Her skal den dataansvarlige tydeliggøre, hvad dette har af indflydelse for den registrerede. Derfor skal den dataansvarlige være påpasselig med at være forudindtaget. Dette kan udledes af C-673/17 Planet49. Den dataansvarlige bør dog også være påpasselig med at ”overfylde” samtykkeerklæringen, da dette kan have negativ indflydelse på samtykkets læselighed. Den dataansvarlige skal inkludere følgende i samtykkeerklæringen:

[208] Nielsen og Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, 1. oplag 2020, s. 810

- Den dataansvarliges identitet
- Formålet med hver enkel behandlingsoperation, der indhentes samtykke til. Hvilken type data, der vil blive indsamlet og anvendt
- Retten til at trække samtykke tilbage
- Oplysninger om dataenes anvendelse til automatiske afgørelser, jf. artikel 22, stk. 2, litra c
- Eventuelle risici ved dataoverførsler som følge af manglende afgørelse om beskyttelsesniveauets tilstrækkelighed eller fornødne garantier, jf. artikel 46

Den dataansvarlige skal sikre, at der kan fremvises fornøden dokumentation for, at kravene til frivilligt, specifikt, informeret og utvetydigt samtykke reelt foreligger, jf. C-673/17 Planet49, samt C-61/19 Orange România.

Anvendelsen af en samtykkeerklæring, som er oplistet under "undtagelser i særlige situationer", er reguleret i forordning art. 49. På basis af denne fremstilling, anses anvendelsen for i praksis at være særdeles begrænset. EU-retten anser ikke, at "undtagelser" over tid skal blive en fortrukken anvendt retsregel. Yderligere vil en generel anvendelse af denne undtagelse, fremfor anvendelse begrænset til særlige tilfælde, resultere i en underminering af artiklens formål. Dette ville også gøre sig gældende i forbindelse med brug som overførselsværktøjet til usikkert tredjeland.

Hvis den dataansvarlige finder, at det pågældende tredjelands lovgivning giver offentlige myndigheder adgang til personoplysninger på en uforenlig måde i henhold til forordning, vil samtykke ikke kunne være tilstrækkeligt som overførselsgrundlag. Dette grundet at det med stor sandsynlighed ikke kan tilbagekaldes, samt at samtykkeerklæring ikke kan udformes tilstrækkeligt specifikt og informeret, for at den registrerede kan gennemskue omfanget og konsekvenserne af at samtykke til overførelse til usikkert tredjeland.

# 13. Konklusion

Det nærværende speciales hovedformål var at klarlægge, hvilke væsentlige hensyn en dataansvarlig skal iagttage, i forbindelse med at overføre personoplysninger til usikkert tredjeland. Baseret på specialets fund, er konklusionen trefoldig: kendskab til lovgivning; forholdet mellem analyseret retspraksis; samt anvendelsen af samtykke vil sammenfattes. Indledningsvis bør det fastslås, at et væsentligt hensyn er, at dataansvarlig i sit hverv iagttager Charterets art. 7 og art. 8, samt gennem Charterets art. 52, 1 balancerer beskyttelse af personoplysninger, jf. forordningens art. 1, 2, overfor behovet for fri udveksling af personoplysninger, jf. forordningens art. 1, 3.

## 13.1 Kendskab til usikkert tredjelands lovgivning

Et dybdegående kendskab til usikkert tredjelands lovgivning og retspraksis er central for, at dataansvarlig kan vurdere, hvilke hensyn der skal iagttages for at sikre, at overførelser af personoplysninger sker med et tilstrækkeligt beskyttelsesniveau. Et eksempel er kryptering, hvor, hvis sådanne anvendes overfor et usikkert tredjeland der enten har forbud mod kryptering, eller kan pålægge en dataimportør at udlevere krypteringsnøglen, så vil foranstaltningen miste sin effekt. Altså, såfremt en foranstaltning anvendes overfor usikkert tredjelands lovgivning der strider imod denne, vil foranstaltningen ikke have effekt og kan derved ikke danne grundlag for overførslen. Ligeledes ses det i Schrems II at anvendelsen af Privacy Shield ordningen ikke havde den fornødne effekt, blandt andet fordi den registrerede ikke havde adgang til at håndhæve retskrav over for den amerikanske stat. Det er altså et væsentligt hensyn, at den dataansvarlige sikrer at et ethvert overførelsesværktøj, samt foranstaltninger, har en real effekt i forhold til at sikre et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er garanteret i Charterets ar. 47 og forordningen.

## 13.2 Forholdet mellem Schrems ll og c-511/18 La quadrature du net

Af Schrems II præmis nr. 95 fremgår det at tredjelands lovgivning i væsentlighed skal svare til det niveau, som er sikret i Unionen. Heraf bør det udledes, at lovgivning i usikkert tredjeland ikke skal være identisk med Unionens lovgivning. Det samme princip vil være gældende i forbindelse med lignende overførelser til andre usikkert tredjeland. Det giver naturligt et vist råderum for dataansvarlig, som fortsat er udefineret af EU-domstolen. I Schrems II har EU-domstolen anlagt en meget restriktiv tilgang til vurdering af tredjelands lovgivning, hvorimod proportionalitetsprincippet i c-511/18 La quadrature du net (Charterets art. 52, 1) er fortolket mindre restriktivt. Det bør antages, at råderummet ligger mellem disse to sager. Dataansvarlig bør i forbindelse med en ny retssag hos EU-

domstolen lægge vægt på de forhold, som er ens med c-511/18 La quadrature du net og de konkrete bestemmelser i det usikkert tredjeland. Desuden bør dataansvarlig anvende Schrems II til at illustrere, at lovgivning i det usikkert tredjeland ikke skal være identisk med Unionens.

### 13.3 Anvendelsen af samtykke

En del af de grundlæggende rettigheder og frihedsrettigheder er, at den registrerede skal have selvbestemmelse over de personoplysninger, som henhører denne. Derfor er samtykke en integreret og vigtig del af forordningen og reguleret i forordningens art. 6, 1, litra a, art. 4, 11, art. 7 og forordningens præambel nr. 32, nr. 42 og nr. 43. I denne fremstilling er samtykkeerklæringer blevet analyseret for at klarligge anvendeligheden som xx overførelse grundlag. Heraf bør det konkluderes, at brugen af samtykkeerklæringer, hvor offentlige myndigheder har eller kan få adgang til personoplysninger i klar tekst, og hvor der ikke foreligger effektive retsmidler, som er lettilgængelig for den registrerede, i overvejende grad ikke er anvendelig som overførelsesgrundlag til usikkert tredjeland. Navnligt grundet, at et samtykke næppe vil kunne formuleres tilstrækkeligt specifikt og informeret i forbindelse med, hvorledes offentlige myndigheder, og særligt efterretningstjenester, anvender disse personoplysninger. Yderligere, vil førnævnte scenarie også være problematisk i forhold til tilbagekaldelse af afgivet samtykke.

Afslutningsvis og overordnet set har nærværende fremstilling tydeliggjort, at overførsel af personoplysninger til usikkert tredjeland ikke er muligt baseret på nuværende forordning, og særligt retspraksis. Derfor er førnævnte balanceøvelse karakteriseret af, at beskyttelsen af personoplysninger vægter tungere end fri udveksling af personoplysninger. Dette værende naturligt udfordrende i en globaliseret verden, hvor samhandel er af afgørende betydning, og den digitale verden samt borgere ikke lader sig begrænse af grænser.

# Litteraturliste


**Love og bekendtgørelser**

- Den Europæiske Union (26.oktober 2012) Europæiske Unions charter om grundlæggende rettigheder. 2012/C 326/02
- Den Europæiske Union (1991) *Traktaten om Den Europæiske Union* (TEU)
- Den Europæiske Union (13.december. 2007) *Traktaten om Den Europæiske Unions Funktionsmåde* (TEUF)
- Den Europæiske Union. (2016). EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF
- Europa Kommissionen (4. juni 2021) KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2021/914 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679
- Federal Bureau of Investigation. (2015). *Presidential Policy Directive 28.*
- Justitsministeriet. (2016). Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning. Betænkning nr. 1565.
- Justitsministeriet. (2018). Databeskyttelsesloven (lovnr. 502).
- Executive Order 12333 (4. december 1981)
  hentet fra: https://www.archives.gov/federal-register/codification/executive-order/12333.html
- Office of the Director of National Intelligence. (u.d.). Section 702 overview.
  Hentet fra: https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf
- U.S. Senate Select Committee of Intelligence. (u.d.). *Legal Resources*.
  Hentet fra: https://www.intelligence.senate.gov/laws/united-states-intelligence-activities

**Retspraksis**

- EU-domstolen. (1. Oktober 2019). *C-673/17 – (Planet49)*.
- EU-domstolen. (11. November 2020). C-61/19 (Orange România).
- EU-domstolen. (2020). *C-311/18 (Schrems II).*
- EU-domstolen. (2020). C-511/18 (La quadrature du net).
- EU-domstolen. (1964). C-6/64 (Flaminio Costa mod ENEL).

- Datatilsynet. (17. Marts 2022). *Datatilsynet har truffet afgørelse i en sag om brugen af et system til ansigtsgenkendelse*.
  Hentet fra: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse

**Tilladelser**

- Datatilsynet (17. januar 2021) Videregivelse fra Region Nordjylland til The Brigham and Women's Hospital (§ 10, stk. 3, nr. 1 og 2)
- Datatilsynet (27. januar 2021) Videregivelse fra Region Syddanmark til The EMBO Journal (§ 10, stk. 3, nr. 3)
- Datatilsynet (27. januar 2021) Videregivelse fra Region Syddanmark til Nature Communications (§ 10, stk. 3, nr. 1 og 3)
- Datatilsynet (11. juli 2021) Videregivelse fra Region Midtjylland til Nature Communications (§ 10, stk. 3, nr. 1 og 3)
- Datatilsynet (11. juli 2021) Videregivelse fra Region Hovedstaden til Stanford Center for Sleep Sciences and Medicine (§ 10, stk. 3, nr. 1 og 2)
- Datatilsynet (07. september 2021) Videregivelse fra Region Syddanmark til Kite Pharma, Inc. Gregory A. Maglinte (§ 10, stk. 3, nr. 1)
- Datatilsynet (03. november 2021) Videregivelse fra Københavns Universitet til MetaboLights, MassIVE og European Nucleotide Archive
- Datatilsynet (17. december 2021) Videregivelse fra Region Hovedstaden til Istituto Cardiocentro Ticino (§ 10, stk. 3, nr. 1)
- Datatilsynet (07. januar 2022) Videregivelse fra Region Hovedstaden til Insel Gruppe AG (§ 10, stk. 3, nr. 1)
- Datatilsynet (12. januar 2022) Videregivelse fra Syddansk Universitet til Victoria University of Wellington (§ 10, stk. 3, nr. 1)

**Forslag til afgørelse fra generaladvokat**

- Forslag til afgørelse fra generaladvokat, M. Szpunar. (21. marts 2019). *C-673/17 – (Planet49)*.
- Forslag til afgørelse fra generaladvokat, M. Szpunar. (4. marts 2020). C-61/19 (Orange România).

**Faglitteratur**


- Blume, P. (2018). *Den nye persondataret.* 2. udgave. Djøf Forlag.
- Nielsen, K. K., & Lotterup, A. (2020). *Databeskytttelsesforordningen og databeskyttelsesloven.* 1. udgave. Jurist- og økonomiforbundets Forlag.
- Munk-Hansen, C. (2021). *Den juridiske løsning*. 2 udgave. Djøf Forlag..
- Tvarnø, C. D., & Nielsen, R. (2021). *Retskilder og retsteorier*. 6. udagve. Jurist og økonomforbundents forlag.
- Udsen, H. (2021). It-Ret. I H. Udsen, *It-Ret,* 5. udgave. Danmark: Ex Tuto Publishing.
- Sørensen, K. E., & Nielsen, P. R. (2022). *EU-retten.* 8 udgave. Jurist- og økonomiforbundents forlag.
- Hamer Risvig, C & Schaumburg-Müller, S. (2020) *Juraens verden*. 1 udgave, 1 oplag. Djøf Forlag.


**Vejledninger og retningslinjer**


- Artikel 29-gruppen vedrørende databeskyttelse. (13. Juli 2011). *Udtalelse 15/2011 om definitionen af samtykke*
  Hentet fra: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_da.pdf
- Artikel 29-Gruppen (28 november 2017) *Retningslinjer vedrørende samtykke i henhold til forordning 2016/679.*
  Hentet fra: https://www.datatilsynet.dk/media/7871/wp259-rev-01_da.pdf
- Datatilsynet. (2017). *Vejledning om dataansvarlige og databehandlere.*
  Hentet fra:
  https://www.datatilsynet.dk/Media/7/6/Dataansvarlige%20og%20databehandlere.pdf
- Datatilsynet. (7. November 2019). *Behandling af følsomme oplysninger*.
  Hentet fra https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/nov/behandling-af-foelsommeoplysninger?fbclid=IwAR0Zgt9tyjXRXwFET4aMd3Fn6Q4Tt5uk0kUOozMhmEMdBS9KF3LwnYI-aiU
- Datatilsynet. (Juli 2021). *Vejledning Overførsel af personoplysninger til tredjelande*.
  Hentet fra:

https://www.datatilsynet.dk/Media/637626336767031457/Datatilsynet_Overf%C3%B8rsel_til_tredjelande_V3_1.0_juli2021.pdf

- Datatilsynet. (Maj 2021). *Vejledning Samtykke.*
  Hentet fra: https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf
- Datatilsynet. (2022). *Vejledning om cloud.*
  hentet fra:
  https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf
- European Data Protection Board, (25. Maj 2018). *Retningslinjer 2/2018 vedrørende undtagelser i artikel 49 i forordning 2016/679*.
  Hentet fra:
  https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_da.pdf
- European Data Protection Board ,(10. November 2020). Henstilling nr. 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger.
  Hentet fra:
  https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_da.pdf
- European Data Protection Board. (10. November 2020). Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.
  Hentet fra:
  https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_da.pdf
- European Data Protection Board. (4. Maj 2020). *Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679*.
  Hentet fra:
  https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_da.pdf
- Medarbejder og Kompetence Styrelsen. (27. September 2019). *9.3.4. "Skøn under regel"*.
  Hentet fra: https://pav.medst.dk/forvaltningsret-persondataloven-mv/andre-forvaltningsretlige-grundsaetninger/skon-under-regel/

**Hjemmesider**


- Borten, K. (2022). *Bedste cloud storage 2022*,
  Hentet fra: https://global.techradar.com/da-dk/news/bedste-lagerplads-i-skyen
- Danmarks Statistik. (Marts 2022). *It-anvendelse i befolkningen 2021*.
  Hentet fra:
  https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=39431&sid=itbef2021
- FysioDanmark Hillerød. (u.d.). *FysioDanmark Hillerød: Om os*.
  Hentet fra: https://fysiodanmarkhillerod.dk/om-os
- Herlufsen, K. (28. April 2011). *Dankortets historie.*
  Hentet fra: https://samvirke.dk/artikler/dankortets-historie
- MOCH. (1. April 2022). *Schrems II-sagen*.
  Hentet fra: https://www.moch360.com/da/schrems-ii/
- Poulsen, J. (u.d.). *Så hurtigt vokser Internettet (antal sites, brugere, social media etc.)*.
  Hentet fra: https://www.skjoldby.com/www-historie/
- Region Hovedstaten. (21. Maj 2016). *Sundhedsplatformen i luften*
  hentet fra: https://www.regionh.dk/presse-og-nyt/pressemeddelelser-og-nyheder/Sider/Sundhedsplatformen-i-luften.aspx
- Skoldby & Co. (u.d.). *42 milepæle i World Wide Webs historie og udviklilng* .
  Hentet fra: https://www.skjoldby.com/www-historie/
- Datatilsynet (den 07. november 2019) *Behandling af følsomme oplysninger*
  Hentet af: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/nov/behandling-af-foelsomme-oplysninger?fbclid=IwAR0Zgt9tyjXRXwFET4aMd3Fn6Q4Tt5uk0kUO-ozMhmEMdBS9KF3LwnYI-aiU


**Andet**


- Madsen, L. H. (2022). *Retsdogmatisk forskning.*
  Hentet fra: https://www.lhgm.dk/Praktisk-Forskning.pdf.
- Secretary, The White House - Office of the Press. (17. Januar 2014). Presidential Policy Directive - Signals Intelligence Activities.
  Hentet fra: *https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities*.

- U.S. Senate Select Committee of Intelligence. (u.d.). *Legal Resources*. Hentet fra: https://www.intelligence.senate.gov/laws/united-states-intelligence-activities