Underimplementeres GDPR i Danmark?

- Eksemplificeret ved manglende overholdelse af dataminimeringsprincippet i MitID

Bachelorprojekt: SDU, jura

Vejleder: Fenella Billings

Udarbejdet af Mona Heide Petersen – studienummer 477810

Abstract:

The intersection of technology design and data protection law is one of the most critical issues of our age.

Under the GDPR, the data minimization requirement is central and rooted in the EU's Charter of Fundamental Rights and cannot be derogated from.

Nevertheless, it states that in the transition from GDPR to DBL to the MitID Act, the legal requirement has disappeared with the consequence that MitID makes compliance with the GDPR impossible and that you can ensure secure processes in the cloud.

The technology design of MitID makes it impossible to comply with data minimization and pseudonymous signature despite requirements for compliance with this in the GDPR.

This means that all digital processes in Denmark are identified and are therefore neither anonymous nor only identifiable but not identified.

The project examines the core of the GDPR, namely that technology-neutral rights are ensured dynamically via a principle of data minimization cf. state-of-the-art.

The sector legislation's ability to legislate on new legitimate interests does not allow the principle of data minimization to be disregarded. This conclusion is also confirmed in the project.

Tro og Love erklæring

"Det erklæres herved på tro og love, at undertegnede egenhændigt og selvstændigt har udformet denne rapport. Alle citater i teksten er markeret som sådanne, og rapporten eller væsentlige dele af den har ikke tidligere været fremlagt i anden bedømmelsessammenhæng."

Bachelorprojekt 12-05-2023

Indhold

Indledning

Danmark er det mest digitaliserede land, når det gælder offentlig digitalisering[1]. Af digitaliserings-ministerens nylige redegørelse kan man læse, at "Danmark [er desuden] i 2022 faldet ned på en andenplads i EU-kommissionens Digital Economy and Society Index (DESI), hvor Danmark i 2021 lå på førstepladsen"[2]. Danmark har altså i mange år ligget helt fremme ift. digitalisering af den offentlige sektor. Læser man videre i redegørelsen, så står der meget om den offentlige digitaliserings betydning for BNP, grøn omstilling, 5G, IoT osv. Men der står faktisk ikke noget om, hvordan vi skal beskytte borgernes persondata. Det kan der være mange grunde til, og det blotte faktum, at der intet står, er jo ikke et udsagn i sig selv.

Hvordan står det til med sikkerheden i verdens mest digitaliserede offentlige sektor[3]? Inden for nogle bestemte områder har Danmark tidligere haft udfordringer med at respektere egne borgeres persondatarettigheder. Et eksempel er Danmarks (skiftende) regeringers rolle i sagen om ulovlig telelogning. Essensen af den ulovlige telelogning kan fremstilles således: Logningsdirektivet som lå

[1] https://digst.dk/nyheder/nyhedsarkiv/2022/september/fn-kaarer-endnu-engang-den-danske-digitale-offentlige-sektor-som-verdens-bedste/

[2] https://www.folketingstidende.dk/samling/20222/redegoerelse/R12/20222_R12.pdf

[3] https://www.computerworld.dk/art/282507/danmark-er-nummer-32-i-verden-i-cybersikkerhed-det-vil-digitaliseringsministeren-goere-for-at-forbedre-den-placering

til grund for den danske lognings-bekendtgørelse, er blevet underkendt ved EU-domstolen i 2014, fordi det krænker retten til privatliv. Menneskeretten er inkorporeret i både dansk ret og EU-retten, og en minister kan derfor ikke udstede bekendtgørelser der krænker borgernes rettigheder[4].

Ikke desto mindre frikendte først Østre Landsret[5] og derefter Højesteret[6] justitsministeren.

Ulovlig telelogning har allerede været prøvet for EU-retten i en anden sag[7], hvori konklusionen er klar: hvis der fortolkes analogt med denne afgørelse, jf. især pkt. 123 i dommen, som tilsiger at "den forelæggende ret [kan derfor ikke] begrænse de tidsmæssige virkninger af en erklæring om ugyldighed, som den i henhold til national ret er forpligtet til at afgive for den nationale lovgivning, der er omhandlet i hovedsagen", så bryder Danmark med artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1 i chartret om grundlæggende rettigheder.

Og sagen om den ulovlige telelogning er ikke afsluttet endnu: "Foreningen Imod Ulovlig Logning" er lykkedes med at få rejst sagen om regerings stadige brug af telelogning for den Europæiske Menneskerettighedsdomstol[8] [9].

Så der forekommer at være en diskrepans imellem på den ene side en udbredt digitalisering af den offentlige sektor og på den anden side en mangel på beskyttelse af borgernes persondata[10].

I 2021 fik danskerne adgang til en ny digital teknologi, som benyttes til at tilgå vores offentlige sektor, herunder fx borger.dk, e-boks mm, men den fungerer også til en del private tjenester, herunder fx vores netbank, forsikring mm. Denne digitalisering er nu næsten fuldt implementeret, så hvis man ikke ønsker den – i øvrigt frivillige – tjeneste, så kan man ikke (siden november 2022) logge på sin netbank, sin forsikring mm. Og fra 30. juni 2023[11] udfases forløberen, den gamle teknologi nemID, og så bliver det ikke mere muligt at tilgå fx e-boks eller borger.dk, hvis man ikke registrerer sig med MitID.

---

[4] https://ulovliglogning.dk/#butwhy

[5] https://ulovliglogning.dk/landsretsdom

[6] https://ulovliglogning.dk/assets/docs/hrdom.pdf

[7] https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=6699129https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=325817

[8] https://www.version2.dk/artikel/justitsministeriets-brug-af-telelogning-skal-menneskerettighedsdomstolen

[9] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-222958%22]}

[10] https://www.computerworld.dk/art/282507/danmark-er-nummer-32-i-verden-i-cybersikkerhed-det-vil-digitaliseringsministeren-goere-for-at-forbedre-den-placering

[11] https://www.nemid.nu/dk-da/om-nemid/aktuelt/mitid_erstatter_nemid.html

Dette har givet mig lyst til at undersøge, hvordan det står til med borgernes persondata, når det kommer til netop denne nye digitale teknologi, MitID.

Jeg vil derfor i dette bachelorprojekt undersøge, hvordan den digitale teknologi MitID overholder gældende persondatalovgivning, repræsenteret ved hhv. GDPR[12], eIDAS-forordningen[13] og DBL[14] i Danmark.

Vi har i Danmark haft digitale teknologiske løsninger på borgerniveau siden ca. 1999[15]. Det er altså 24 år siden, at man begyndte at implementere de første digitale løsninger. Når man i dag læser præsentationsmaterialet på MitIDs hjemmeside, kan man læse, at MitID er både sikkert og "MitID giver Danmark en ny sikkerhedsinfrastruktur for digitale identiteter, hvor sikkerhedskravene lever op til de nyeste standarder for sikkerhed"[16].

Derfor skal MitID-teknologien i dette bachelor-projekt underkastes en nærmere juridisk analyse med henblik på at undersøge, om og i givet fald i hvilken grad, gældende EU-og Dansk-persondatarets-lovgivning overholdes. Fokus vil særligt være på dataminimering og "overholdelse af borgernes persondatarettigheder", koblet med Mireille Hildebrandts og Laura Tielemans artikel om teknologineutralitet og state-of-the-art.

Problemformulering

- *Respekterer den digitale tjeneste MitID i sit design den juridiske implementering af EUs GDPR-krav?*
- For at besvare dette, vil jeg undersøge følgende:
- *Hvordan er MitID-designet?*
- *Hvad er EU-GDPR-kravene?*
- *Hvordan er GDPR implementeret i DBL?*
- *Hvordan overholdes GDPR-lovgivning i DK ift. fx sektorlovgivning?*

Er der diskrepans imellem de to lovgivninger og er der diskrepanser imellem implementeringen ift. MitID i DK? Systematisk gennemgang af krav iht. GDPR, DBL og MitID ift. dataminimering jf. State-of-the-art jf. eIDAS og GDPR.

---

[12] Europa-Parlamentets og Rådets forordning af 2016-04-27
om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679

[13] Forordningen om elektronisk eID og tillidstjenester (eIDAS)

[14] Lov 2018-05-23 nr. 502
om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

[15] https://digst.dk/it-loesninger/nemid/om-loesningen/historie/

[16] https://www.mitid.dk/media/hcjevl0z/om-mitid_baggrund_v1-03.pdf, besøgt 03052023

Definitioner:

I forbindelse med EU-retten er proportionalitetsprincippet jf. TEUs artikel 5(4) centralt. Det vil således løbende blive inddraget, hvor det findes relevant.

Det antages ofte i lovgivning, at proportionalitetsprincippet som udgangspunkt kan anvendes ift. at fravige GDPR og eIDAS, hvis legitime hensyn, fx økonomi eller statens sikkerhed, kræver det. Pointen med dataminimering jf. GDPRs artikel 25 er dog, at nødvendighedskriteriet har forrang, hvis muligheden foreligger for et bedre teknologidesign. Kan man dataminimere tilstrækkeligt, så bliver proportionalitetshensynet aldrig relevant, fordi der slet ikke skabes persondata, som man indsamler og behandler. Så man kan sige, at proportionalitetsprincippet først dukker op i det øjeblik, man ikke har "designet ordentligt". For hvis man har det, så behøver man slet ikke at tage stilling til proportionalitetsprincippet, dertil kommer det slet ikke.

Proportionalitetsprincippets skal endvidere her forstås som et krav om nødvendighed i forhold til den dataansvarliges behandling af personoplysninger efter persondatalovens centrale behandlingsbestemmelser. Det vil altså sige, at princippet forstås som et grundlæggende, EU-retligt princip om egnethed, nødvendighed og forholdsmæssighed ift. indsamlede og lagrede persondata. Når de behandles efter proportionalitetsprincippet, dvs. databehandler forfølger et lovligt formål, at de midler, der bringes i anvendelse, er egnede til at virkeliggøre det tilstræbte mål og at det ikke går ud over, hvad der er nødvendigt for at opnå dette.

Oprindeligt udsprang proportionalitetsprincippet som EU-retligt princip i domspraksis[17], siden blev det traktatfæstet og det gælder nu bredt, ikke blot for EUs institutioner og retsakter, men anvendes generelt af EU-retten[18].

I forhold til nødvendighedskriteriets oprindelse tales der i EU-retten om, at der skal være tale om nødvendige foranstaltninger i forhold til målet, og at der ved valgmuligheder skal vælges den mindst bebyrdende foranstaltning, jf. fx GDPRs artikel 25, stk. 1 state-of-the-art vedr. design og GDPRs artikel 35, stk. 1 om konsekvensanalyse.

Desto hårdere en retsakt rammer private interesser, desto mere må forvaltningen sikre sig, at en retsfølge ikke går videre end nødvendigt for at opfylde det lovlige formål. Hvis der er tale om et indgreb i en fundamental rettighed, eller i øvrigt om et byrdefuldt indgreb, skal det nøje overvejes, om mindre indgribende midler i tilstrækkelig grad vil kunne fremme målet[19].

"Behandlingen af personoplysninger vil i denne sammenhæng være at betragte som indgreb i en privat interesse, der karakteriseres som en fundamental rettighed. Der tales altså for en hård/indgribende nødvendighedsvurdering, hvor det nøje skal undersøges, om en mindre indgribende form for behandling vil kunne opfylde det opstillede behandlingsformål"[20].

---

[17] Neergaard, Ulla og Nielsen, Ruth, EU-ret, 8. udgave, Karnov, 2020, side 308
[18] Ibid.
[19] Christensen, Bent: Forvaltningsret, 2. udg., s. 202 og Fenger, a. st., s. 641
[20] Tranberg, Charlotte Bagger, Nødvendig behandling af personoplysninger, Forlaget Thomson, 2007, side 528

Ansvarlighedsbevis: et selvinkriminerende bevis, som kobler en person til en handling: ”jeg gjorde dette”. Det kan adskilles fra selve identiteten, fx ved at data er krypteret på en sådan måde, at det kan deanonymiseres af fx en dommer.

Metode

Jeg vil foretage en retsvidenskabelig analyse af MitID og det vil jeg gøre ved hjælp af den retsdogmatiske metode, dvs. projektet beskriver gældende ret og kommer ikke med et endegyldigt svar. Der vil derfor altid være tale om konkrete vurderinger i forhold til alle afgørelserne, da de kan påklages til domstolene for en endelig afgørelse. Den retsdogmatiske metode har til formål at beskrive, analysere og systematisere gældende ret (de lege lata).

Denne metode benyttes til at indplacere MitID i eksisterende lovgivning. Der tages afsæt i hhv. GDPR, DBL og eIDAS-forordningen med henblik på at fastsætte, hvad gældende ret er. GDPR og eIDAS er forordninger, der er almengyldige og bindende i hver medlemsstat i EU[21] og de har forrang for national ret[22]. Der er tale om retsakter med en høj retskildeværdi. Der er dog givet et frirum til national udfyldning, hvorefter der i Danmark er udarbejdet en Databehandlingslov (DBL), som supplerer GDPR-forordningen[23]. Retspolitiske overvejelser (de lege ferenda) forekommer i et vist omfang, men hovedvægten ligger på gældende ret. Der vil desuden blive inddraget andre relevante retskilder, herunder også trinlavere, for så vidt som det skønnes nødvendigt, herunder fx relevant sektorlovgivnig. Selvom der ikke er en rangorden mellem retskilderne, er der som følge af lex-principperne en

rangorden inden for normen regulering, det følger af de tre lex-principper lex superior, lex specialis og lex posterior. Lex superior medfører, at ingen lov må stride mod en højere rangeret lov, det vil sige, at ingen lov må stride mod Grundloven, og da bekendtgørelser har hjemmel i lov, må ingen bekendtgørelse stride mod en lov. Lex specialis medfører, at en speciallov har højere rang end en generel lov og lex posterior, at en ny lov har højere rang end en ældre lov[24].

Den retlige ramme

Samspillet mellem den EU-retlige og den danske regulering på persondatarettens område skal kort belyses i dette afsnit:

Det danske reguleringssystem finder anvendelse, da den dataansvarlige er etableret i Danmark og dermed er underlagt dansk ret. Med Danmarks tiltrædelseslov med senere ændringer har Danmark ratificeret EUs traktatgrundlag, herunder bl.a. TEU og TEUF. Disse traktater er en del af den

[21] Sørensen m.fl.: EU-retten (2014), s. 96
[22] Ibid. s. 174
[23] Blume, Peter: Den nye persondataret (2018), s. 29f
[24] Tvarnø, Christina og Nielsen, Ruth, Retskilder og retsteorier. Jurist- og Økonomforbundets Forlag, 5. reviderede udgave, 1. oplag, 2017, s. 235-240

primære EU-ret og indeholder bl.a. hjemmelsbestemmelser, der giver EU-institutionerne mulighed for at vedtage sekundær EU-lovgivning i form af fx forordninger og direktiver[25].

I dette projekt vil GDPR med tilhørende præambelbetragtninger blive inddraget, desuden supplerende lovgivning, hvis det skønnes relevant.

GDPR er en forordning og, som jeg uddyber i senere afsnit, det er dermed bindende EU-retlig sekundærregulering, der har fuld direkte virkning i EU-medlemsstaterne, herunder i Danmark, jf. TEUF art. 288, 2. pkt.

Dette indebærer, at GDPR både har horisontal og direkte virkning i Danmark, og derfor kan borgere i Danmark påberåbe sig GDPR overfor staten og en anden borger[26]. GDPR har til formål at regulere alle væsentlige spørgsmål om databeskyttelse og gøre dette på en måde, der medfører ensartethed i EU-medlemsstaternes persondataretlige regulering. Derfor kan GDPR karakteriseres som den centrale retskilde i dansk persondataret. Som led i fortolkningen af bestemmelserne i GDPR vil, som nævnt, de tilhørende præambelbetragtninger, hvor det skønnes relevant, blive inddraget. Betragtningerne er vedtaget sammen med GDPR, og derfor skal de læses som en helhed[27].

Også EUs charter for grundlæggende rettigheder, "Chartret", indgår i projektet. I medfør af TEU art. 6, stk. 1, gælder Chartret på traktatniveau, og er ligesom TEU og TEUF derfor en del af den primære EU-ret[28]. Chartret kodificerer en række grundlæggende rettigheder og almindelige retsprincipper, der oprindeligt er blevet udviklet af EU-Domstolen[29]. Chartrets nærmere betydning for dansk persondataret fastslås i præambelbetragtning 4 i GDPR, efter hvilken GDPR overholder Chartret. Chartret skal og bliver inddraget ved fortolkningen af GDPR. Når chartret anvendes, skal altid læses på baggrund af chartrets artikel 52, som fastsætte rækkevidden af chartrets rettigheder og principper og fortolkningen af dem.

EU-Domstolen tillægger Chartret en vægtig betydning, når den træffer afgørelse om persondataretlige spørgsmål[30]. Dette illustreres af EU-Domstolens domme i henholdsvis Schrems I og Schrems II, hvoraf kun sidstnævnte vil blive inddraget i projektet. Begge domme er præjudicielle afgørelser, og jf. TEUF art. 267, 1. pkt., fremgår det, at EU-Domstolen i sådanne afgørelser har kompetence til at afgøre præjudicielle spørgsmål om fortolkningen af EUs traktater samt om gyldigheden og fortolkningen af retsakter udstedt af EUs institutioner. Afgørelserne kan ikke appelleres. Derfor er det EU-Domstolen, der med bindende virkning endeligt fastlægger EU-rettens indhold, herunder ikke mindst reglerne og rettighederne som fastsat i GDPR og Chartret. EU-Domstolens afgørelser kan derfor tillægges øverste retskilderang i en EU-retlig sammenhæng[31]. Om

[25] Christoffersen, Jonas m.fl., EUs Charter om Grundlæggende Rettigheder med kommentarer, 2. udgave, 1. oplag, 2018, s. 40
[26] EUR-Lex, EU-rettens direkte virkning, https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=uriserv%3Al14547 (sidst besøgt: 8/5 2023).
[27] Blume, Peter, Databeskyttelsesret, 5. udgave, 1. oplag, 2018, s. 60 f.
[28] Christoffersen, Jonas m.fl., EUs Charter om Grundlæggende Rettigheder med kommentarer, 2. udgave, 1. oplag, 2018, s. 40
[29] Tvarnø, Christina og Nielsen, Ruth, Retskilder og retsteorier, Jurist- og Økonomforbundets Forlag, s. 5. reviderede udgave, 1. oplag, 2017, s. 102
[30] Blume, Peter, Databeskyttelsesret, 5. udgave, 1. oplag, 2018, s. 60
[31] Blume, Peter, Databeskyttelsesret, 5. udgave, 1. oplag, 2018, s. 63

EU-dommes præjudikatvirkning i forhold til nationale domstole, så fremgår det ifølge EU-Domstolen af loyalitetsforpligtelsen efter TEU art. 4, stk. 3, samt EU-Domstolens praksis, at nationale domstole har pligt til at rette sig efter EU-Domstolens fortolkninger[32].

Vedr. forholdet mellem Chartret og EMRK, så har EU ikke ratificeret EMRK, men det ændrer ikke ved det forhold, at EU-retten i stigende grad, gennem de seneste 10-15 år, henviser til EMRK[33].

I Danmark er DBL generelt set en central retskilde i dansk persondataret. DBL udfylder og supplerer GDPR, hvilket i et vist omfang åbner op for et nationalt råderum[34].

Begreber og principper, en kort gennemgang:

Behandling af personoplysninger:
I medfør af legaldefinitionen i GDPR art. 4, nr. 1, skal personoplysninger forstås som enhver form for information om en identificeret eller identificerbar fysisk person, der kan karakteriseres som "den registrerede". Ifølge GDPR art. 4, nr. 2, vil en behandling bestå i enhver aktivitet eller række aktiviteter, som de nævnte personoplysninger gøres til genstand for.

Dataansvarlig og databehandler
Den dataansvarlige er persondatarettens primære pligtsubjekt. I medfør af GDPR art. 4, nr. 7, er den dataansvarlige den, som udøver bestemmelsen over persondatabehandlingens formål, og på hvilken måde behandlingen foregår. Omvendt er databehandleren ifølge GDPR art. 4, nr. 8, enhver, som på vegne af den dataansvarlige varetager den faktiske persondatabehandling[35].

Teknologineutralitet

Det fremgår af eIDAS' præambel 27, at der stilles krav om teknologineutralitet. Det betyder i klartekst, at de specifikke teknologiske løsninger kan vedtages på nationalt niveau. Denne præambel er formentlig tydeligt inspireret af Mireille Hildebrandt og Laura Tielemans artikel om samme emne. I artiklen" *Data protection by design and technology neutral law*[36] behandler de begrebet "Privacy by design". Pointen i artiklen er, at for at opnå en teknologineutral lov, er man nogle gange nødt til at vedtage teknologispecifik lovgivning. Forfatterne opererer med tre formål ift. som ofte underforstås som teknologisk neutralitet: de tre formål er kompensationsmålsætningen, innovationsmålsætningen og bæredygtighedsmålsætningen.

Hildebrandt et al opererer med tre parametre i forhold til Dataprotection Privacy by design (DPbD), nemlig *kompensation, innovation* og *bæredygtighedsmålsætningen.* Hildebrandt og Tielemans operer med tre fokuspunkter i deres undersøgelse: 1) for at være neutral, er loven nødt til at være

[32] Tvarnø, Christina D. og Nielsen, Ruth, Retskilder og retsteorier, 5. reviderede udgave, 1. oplag, 2017, s. 156
[33] Neergaard, Ulla og Nielsen, Ruth, EU-ret, 8. udgave, Karnov, 2020, side 173
[34] Blume, Peter, Databeskyttelsesret, 5. udgave, 1. oplag, 2018, s. 53
[35] Blume, Peter, Den nye persondataret, 2. udgave, 1. oplag, 2018, s. 73 ff.
[36] Fra Computer Law & Security Review, volume 29, issue 5, October 2013

teknologisk specifik (Jf. GDPRs artikler 25 og 32). 2) Desuden nævnes begreberne" technology neutral law" og 'technologically neutral law'. Der vil I dette projekt ikke blive sondret mellem disse to, men begreberne vil opfattes som ét, som handler om teknologisk neutral lov og endelig 3) skal lovgivningen være dynamisk for ikke at blive teknologisk uaktuel for hurtigt. Andreas Politis reflekterer i sin artikel "Is the GDPR a technology neutral legislation" over forskellene på hhv. teknologi-specifik og teknologi-neutral lovgivning:

"A technology specific law will most likely not be able to cover future developments of technology, and thus become obsolete quicker. A technology-neutral law, on the other hand, will possibly cope better with technological advancement, but depending on its interpretation, it might become in the end technology specific. In this case, a dynamic interpretation, parallel to the technological advancement, could remedy this oxymoron".

Dataminimering i henhold til state-of-the-art

GDPR-artikel 25, stk. 1 fastlægger begreberne pseudonymisering og dataminimering, særligt ift. design og standardoplysninger[37]. Når begreberne anonymitet og pseudonymitet benyttes, så menes der her den "ægte" pseudonymitet og anonymitet, altså den i sikkerhedsmæssig forstand vedr. databeskyttelsesprincipper jf. de grundlæggende principper i eIDAS-artikel 5, stk. 1, og altså ikke den som foreligger som en proces, efter at der *er* opsamlet persondata. Begrebet pseudonymisering er i databeskyttelsesforordningen defineret som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person[38].

Bestemmelsens centrale del er at sikre tilstrækkelig og effektiv databeskyttelse både gennem design og gennem standardindstillinger. Det vil sige, at dataansvarlige bør kunne påvise, at de i behandlingen anvender tilstrækkelige foranstaltninger og garantier, der sikrer, at databeskyttelsesprincipperne og de registreredes rettigheder og frihedsrettigheder rent faktisk gennemføres[39]. Det handler således om databeskyttelse gennem design i artikel 25, stk.1. I forbindelse med artikel 25 forpligter tilsvarende omtalen af "det aktuelle tekniske niveau" dataansvarlige til at tage hensyn til eksisterende teknologiske fremskridt, der er på markedet[40], dvs. state-of-the-art.

Dataminimeringsbegrebet tilsiger at behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet[41]. Ultimativt er det et krav om at designe persondata ud af it-

[37] https://pro.karnovgroup.dk/b/documents/7000751611?tab=karnov#EUFOR2016679_A5
[38] https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvad-er-personoplysninger

[39] https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf, side 5

[40] Ibid., side 9
[41] https://www.datatilsynet.dk/media/6559/generel-informationspjece-om-databeskyttelsesforordningen.pdf, side 10

løsninger i videst muligt omfang. Dataminimeringen ophører således først, når loven ikke gælder længere. Altså når man først ikke mere "skaber" persondata. GDPR gælder på identificerede eller identificerbare data. Den ultimative form for dataminimering er, når data ikke er til fare for nogen, altså hverken er identificerbare eller identificerede eller dermed ikke kan samkøres.

GDPRs artikel 25, stk. 2 handler om databeskyttelse gennem standardindstillinger. Den dataansvarlige bør vælge og stå til ansvar for at gennemføre forudindstillinger og valgmuligheder på an sådan måde at, der som standard kun foretages behandling, der er strengt nødvendig for at opfylde det fastlagte lovlige formål. Her bør dataansvarlige støtte sig til deres vurdering af behandlingens nødvendighed med hensyn til retsgrundlaget i artikel 6, stk. 1[42].

GDPR-artikel 32, stk. 1.a. handler om pseudonymisering og kryptering iht. at dataminimere jf. state-of the-art,

Kvalificerede Pseudonyme Signaturer i eIDAS artikel 5.1 -forstand er identifikation jf. eIDAS, men per definition "identificerbare, men ikke idenficerede" jf. GDPR Artikel 25, stk. 1, fordi personhenførbarhed kræver, at den trustede part frigiver koblingen og det er, indtil dette er sket, den eneste part udover borgeren selv, som kan gøre dette, dvs. det er pr. definition persondata.

Kvalificerede Anonyme Signaturer i eIDAS- forstand er i GDPR- forstand hverken identificerede eller identificerbare. Det er identiteter, som indebærer, at man kan "stole på" data og nøglen er låst til én og kun én borger, men ingen véd hvilken borger. Et andet eksempel er et fysisk folketingsvalg, eller i forskningsøjemed, adgang til politiske medier mm. For at opnå en ækvivalent digital signatur overfor domstolene, kan en trustworthy anonym signatur, kombineret med ansvarlighedsbeviser[43], som etablerer mulighed for at en dommer – under visse betingelser[44] – kan åbne for en beviselig kobling mellem borgeren og den anonyme signatur.

State-of-the-art jf. GDPR:

I GDPR-forordningen stilles der krav om at der skal dataminimeres jf. State-of-the-art-princippet.

Af eIDAS´ artikel 5.1 fremgår det, at "Behandling af personoplysninger skal udføres i overensstemmelse med direktiv 95/46/EF"[45]. Denne artikel henviser således til koblingen ml eIDAS og GDPR. Af eIDAS artikel 5.2 fremgår det, at hvis der kan skabes pseudonyme data, så må brugen af disse ikke forhindres. I klartekst betyder det, at hvis GDPR kræver, at man skal lave State-of-the art, så gælder dette også i eIDAS. Dvs. modparten skal acceptere en pseudonym signatur og må ikke uden eksplicit hjemmel kræve identifikation udover pseudonymiteten.

Delkonklusion

[42] Ibid., side 12

[44] Fx hvis en borger er mistænkt i en sag

[45] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32014R0910&from=NL

Artiklen lægger op til, at teknologineutralitet skal implementeres, men det skal være på en dynamisk måde og det overlades til nationalstaterne, hvordan de præcis vil gøre det. Grundkravet er, at man altid skal bruge de teknologier, der bedst varetager borgernes interesser. Dataminimering i henhold til state-of-the-art i forhold de lovgivne hensyn er det primære værktøj i forhold til at sikre, at den teknologineutrale GDPR sikrer en teknologiske udvikling som løbende varetager borgernes rettigheder.

Fra Digital Signatur til MitID: den teknologiske udvikling i Danmark fra 1999 – 2023, et kort overblik:

I Danmark blev der i 2021 indført en ny digital sikkerhedsløsning. Navnet på denne nye it-teknologi er MitID. MitID er et samarbejde mellem det offentlige og pengeinstitutterne. På MitIDs hjemmeside angives det, at MitID blev lanceret i 2021 og gradvist vil erstatte NemID, i takt med, at alle NemID-brugere får MitID. MitID er således en direkte forlængelse af den tidligere digitale løsning NemID. Og som det også fremgår af siden, er det hensigten, at alle danskere migrerer – flytter over på – denne nye teknologi i løbet af 2023.

MitID var altså en efterfølger til det tidligere NemID. MitID afløste NemID af sikkerhedsårsager og MitID lever, i henhold til MitIDs egen hjemmeside, op til "de nyeste standarder for sikkerhed. MitID er designet, så det er nemt at tilpasse til fremtidige behov. Med MitID styrker vi sikkerheden", fremgår det af MitIDs egen whitepaper[46].

MitID-partnerskabet består af Digitaliseringsstyrelsen, der repræsenterer staten, de danske regioner, kommunerne og landets pengeinstitutter, repræsenteret ved deres interesseorganisation, Finans Danmark. Det er MitID-partnerskabet alene, der ejer MitID[47].

Hvordan er MitID teknisk designet?

MitID er designet som en "SSO-løsning", dvs. en Single Sign On-løsning. Dette betyder, at man skal logge ind på en central server, hver gang man skal bruge MitID. Denne løsning adskiller sig fx fra en certifikatstyret signatur, som man som bruger kan kontrollere. Hvis man skal kunne kontrollere denne løsning, ville det indebære, at der skabes et Offentligt/hemmeligt nøglepar, hvor den offentlige nøgle "certificeres", dvs. der skabes en datastruktur, underskrevet af CA[48], som låser den offentlige nøgle til borgeren. Den hemmelige/private nøgle bruges til at bevise at man er den som kontrollerer den offentlige nøgle, hvilket man fx kunne med NemID. I NemID lå borgerens private nøgle i et central HSM[49], som kun kunne aktiveres, hvis man kendte det tilhørende password, som NemID angiveligt ikke gemte. (men som let kunne opsamles i en transaktion og

[46] https://www.mitid.dk/media/ybkbbpgy/om-mitid_baggrund_whitepaper-v1-02.pdf
[47] (hentet fra https://www.mitid.dk/om-mitid/ 11012023).
[48] CA= Certificate Authority: en eIDAS-autoriseret nøgleudsteder, fx Digitaliseringsstyrelsen.
[4949] HSM: Hardware Secure Module, en såkaldt "secure enclave" som skal sikre, at de private nøgler aldrig forlader et kontrolleret rum.

genbruges i den næste). Nøglekortet indeholdt engangskoder, som var låst til denne certifikatnøgle, som var en adgangskontrol til den centrale nøgleserver, dvs. fungerede som password til den private nøgle kontrolleret centralt. I MitID-konstruktionen er papkorts-løsningen udgået (den kunne kopieres), men man har også fjernet den eneste nøgle, som borgeren "kontrollerer[50]"

"Med MitID styrker vi sikkerheden, så du blandt andet bliver bedre beskyttet mod identitetstyveri"[51].

Når man skal logge på MitID første gang, sker dette ved hjælp af biometri som ID-autentificering: man skal scanne chippen i sit pas og dernæst scanne sit ansigt ved hjælp at sin telefons kamera. Scanningen danner derefter et 3D-billede af ansigtet, der sammenlignes med det indscannede 2D pasfoto fra passets chip (On-phone biometrics). Dette sker via upload til server, dvs. biometrien opsamles, selvom MitID hævder, at de sletter dem igen. Derudover verificerer ansigtsscanningen, at det er en levende persons ansigt (modsat fx. en dukkes). Videoen fra "likenesstjek"' og attributterne fra ansigtsscanningen gemmes i krypteret form og oplysningerne fra passet gemmes. Tilsvarende opbevares billederne på en server, der tilhører leverandøren af MitID – og altså ikke lokalt hos borgeren – og således kunne man risikere, at de biometriske data lægges på en 3. partsserver. Som borger har man ikke nogen dokumentation for, at dette ikke sker.

Historisk rids over databeskyttelseshistorikken i Danmark

For at kunne leve op til EU-lovgivers mål om et fælles marked og en lige konkurrence, var det nødvendigt at lave lovgivning med fælles regler på europæisk plan. Baggrunden skal findes i, at evt. forskellige nationale regler ofte kan være til hinder for, at EU-reglerne bliver anvendt tilstrækkelig ensartet, dels kan de nationale regler fremkalde konkurrenceforvridende situationer og/eller skade det fælles markeds funktion. Det var derfor nødvendigt at harmonisere behandling og udveksling af personoplysninger[52]. Dette skete først i form af Direktivet om persondatabeskyttelse, som kom i 1995 (Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995) og siden med Rådets forordning nr. 2016/679 af 27. april 2016 (GDPR) som er implementeret i Danmark som Databeskyttelsesforordningen/Persondataforordningen (DBF).

I Danmark havde vi haft Registerloven (indført 1987), derefter Persondataloven i 2000, (lov nr. 429 af 31. maj 2000 med senere ændringer), så fulgte Retshåndhævelsesdirektivet, Lov 2017-04-27 nr. 410 og endelig den supplerende Databeskyttelseslov (DBL), lov nr. 502 af 23. maj 2018. Der findes også TV-overvågningsloven og logningsloven, men her skal fokus primært være på GDPR-forordningen, eIDAS-forordningen og DBL.

Databeskyttelsesforordningen (DBF) tjener to overordnede formål:

- Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og
- Fri udveksling af personoplysninger, herunder harmonisering af reglerne inden for EU

[50] "kontrollerer" fordi engangskoderne er skabt og udsendt af NemID/NETS
[51] https://www.mitid.dk/sikkerhed/ Besøgt 12042023
[52] EU-rettens påvirkning af dansk forvaltningsret, Fenger, Niels, 3. udgave, Jurist- og Økonomforb. Forl., 2018, side 14

Skal man kategorisere Databeskyttelsesforordningens indhold generelt, kan man sige, at det er en af de væsentligste nyskabelser ved databeskyttelseslovgivningen, at EU-lovgiver valgte at udstede en forordning. Det følger af TEUF art. 288, 1. og 2. pkt., at en forordning er almengyldig og bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

En forordning virker således som en lov i medlemsstaterne, og den gælder i den form, som den er vedtaget i[53], og den må som udgangspunkt ikke gennemføres i nationalret. Det vigtige at iagttage i denne forbindelse er således, at der ikke kan laves nationale regler – love – der tilsidesætter reglerne i en forordning.

Der er imidlertid en lang række modifikationer i databeskyttelsesforordningen til dette udgangspunkt, idet visse regler i forordningen bestemmer, at medlemsstaterne inden for nærmere bestemte områder enten skal eller kan fastsætte nationale regler.

Selv om der er hjemmel til at lave en forordning, følger det af subsidiaritetsprincippet, at EUs involvering skal være så enkel som mulig, og derfor skal direktiver, alt andet lige, prioriteres. Når man derfor i dette tilfælde laver en forordning, skyldes det, at der er behov for ensartet anvendelse og retssikkerhed i hele EU[54].

Overholder MitID gældende GDPR-lovgivning?

Af artikel 23 i GDPR-forordningen fremgår det, at artiklerne 12-22, og 34, under visse forudsætninger, kan fraviges. Fortolker man således artikel 23 modsætningsvist, fremgår det også, hvad der ikke kan fraviges, herunder fx artiklerne 25, 32 og 35. Og da GDPR jo er en forordning, kan disse artikler ikke fraviges, da den er en bindende retsakt[55].

Som tidligere nævnt følger det af proportionalitetsprincippet, at behandling af personoplysninger aldrig må omfatte mere, end hvad der kræves til opfyldelse af de formål, som den dataansvarlige er berettiget til at forfølge. Artikel 5.1. i eIDAS statuerer, at GDPR skal respekteres, dvs. at hvis man – i dette tilfælde staten – kan designe tilstrækkeligt sikre løsninger, så er staten også forpligtet til at gøre det. I dag kan man fx lavekvalificerede pseudonyme løsninger som fx NemID-medarbejdersignatur. Og når staten kan det, så skal den lave trustworthy ("when you do not need to trust") anonyme signaturer[56], optionalt set kombineret med en betinget ansvarlighed, som fx kun en dommer har adgang til under visse betingelser. Den danske stat skal således, jf. artikel 5.1 i eIDAS, som en del af MitID, tilbyde en kvalificeret pseudonym løsning, så borgerne kan sikre sig i henhold til eIDAS artikel 5.2 i fx applikationer.

[53] Neergaard, Ulla og Nielsen, Ruth, EU-ret, 8. udgave, Karnov, 2020, side 216
[54] Neergaard, Ulla og Nielsen, Ruth, EU-ret, 8. udgave, Karnov, 2020, side 143
[55] På engelsk er det en forpligtelse til at lave værktøjer som sikrer borgerne med dataminimering. På dansk kan det klares med en bekendtgørelse (som ikke har samme retskildemæssige tyngde som fx en lov).
[56] Se senere uddybning vedr. nemID-erhvervs-signatur

Hvad er EU-GDPR-og eIDAS-kravene ift. MitID?

Som ovenfor angivet, kan artiklerne 25, 32 og 35 i GDPR-forordningen ikke fraviges. Da disse artikler er relevante ift. MitID og borgernes databeskyttelse, skal de undersøges nærmere. Desuden inddrages eIDAS-forordningen hvor den skønnes relevant, fx her ved betragtning 11 i præamblen: ” […] autentifikation i forbindelse med en onlinetjeneste [bør] derfor kun omfatte behandling af de identifikationsdata, [der er] tilstrækkelige, relevante og ikke omfatter mere, end hvad der kræves for at give adgang til den pågældende onlinetjeneste. Desuden bør tillidstjenesteudbydere og tilsynsorganer opfylde kravene i direktiv 95/46/EF om fortrolighed og behandlingssikkerhed".

Endvidere fremgår det også af GDPRs artikel 25 stk. 1, at hvis den dataansvarlige kan gennemføre passende tekniske foranstaltninger i forhold til at pseudonymisere og dataminimere, så skal man gøre det. Herunder menes især ift. design og standardoplysninger.

Af GDPR-artikel 32[57], stk. 1.a. fremgår det, at den dataansvarlige skal gennemføre pseudonymisering og kryptering iht. at dataminimere jf. state-of the-art jf. eIDAS artikel 5.2, som statuerer et krav om pseudonyme data, hvis det teknologisk er muligt.

Formålet med eIDAS og MitID er, at man kan stilles til ansvar, hvis man fx ikke overholder loven eller bryder en aftale. Hvis man identificerer/koblet til CPR på handletidspunktet, fører det til, at man altid skaber identificeret persondata. Ved at bruge pseudonyme signaturer, kan man undgå, at data er identificerede, så de kun er identificerbare. Heraf retskravet iht. eIDAS artikel 5.2 pseudonyme signaturer.

Ved at bruge ansvarlighedsbeviser, kan man låse identifikationen til en dommer, som kan koble rettighedsbruddet med identifikationen, i praksis ved domfældelse. Dette eliminerer muligheden for identifikation uden domfældelse, hvilket er en direkte kobling mellem GDPR, eIDAS og domstolene. Et sådan bevis udsætter GDPR-persondataproblemet og selv-inkrimineringen (”jeg gjorde dette”) i digital signatur, indtil et rettighedsbrud er verificeret.

Delkonklusion, GDPR- og eIDAS-krav

Anvender man disse tre parametre på MitID, er resultatet følgende: 1) for at være neutral, er loven nødt til at være teknologisk specifik (Jf. GDPRs artikler 25 og 32). Da det det løbende er dokumenteret i nærværende projekt, at MitID i sit teknologi-design forstøder mod hhv. artiklerne 25, stk. 1 og 2, og 32, stk. 1a., kan denne specifikke, mest betydningsfulde lovgivning, ikke respekteres. 2) Om teknologi-neutral-lovgivning: i sin grundsubstans handler kravet om teknologineutral lovgivning om, at man, nationalstaterne, skal kunne vælge, de skal selv kunne bestemme.

Af ovenstående afsnit fremgår det, at den dataansvarlige skal dataminimere iht. state-of-the-art, hvis det, rent teknisk, er en mulighed.

[57] art. 5, stk. 1, litra f, jf. art. 5, stk. 2, og til art. 30, stk. 1, litra g

Analyse af MitID ift. overholdelse af GDPR

Som ovenfor nævnt kan man med MitID kun logge på en central server. I et databeskyttelsesperspektiv forhindrer denne proces dataminimering jf. GDPRs artikel 25, stk. 2 og GDPRs artikel 32, stk. 1.a, fordi oplysningerne fra passet gemmes, og billederne opbevares på en server, der tilhører leverandøren af MitID, og de biometriske data gemmes på en 3. partsserver og fordi transaktionen dermed pr definition altid er identificeret[58]. Denne leverandør har derefter fri adgang til brugerens biometriske data, dvs. følsomme, personhenførbare data, om borgeren, koblet til hans CPR, som opbevares hos 3.-partsleverandøren[59]. Da databeskyttelsesretten hviler på en risikobaseret tilgang, betyder det, at jo større risiko for den registrerede, desto strengere krav til den dataansvarlige. Det er ganske vist ikke dokumenteret, at tredjeparts-leverandører gemmer billedet, men det er sikkert, at de gemmer referencen til CPR/navn, da det er dét, MitID verificerer hver gang. Og således er transaktionen per definition identificeret.

Det har derfor betydning, hvilke personoplysninger der behandles. Her er artikel 9 i GDPR udtømmende og omfatter bl.a. biometriske data.

Det forhold, at biometriske data ligger på en 3. parts server (Server-side biometrics), forstøder imod artikel 25, stk. 1 i GDPR om pseudonymisering, fordi det deraf fremgår, at myndigheden har pligt til at dataminimere, hvis teknologien findes, altså under hensyntagen til det aktuelle tekniske niveau. Om det aktuelle tekniske niveau kan tilføjes, at teknologien allerede findes, se fx NemID-medarbejdersignatur[60].

Og jf. GDPR art. 25, stk. 2, så skal den dataansvarlige gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på, gennem standardindstillinger, at sikre at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Og eftersom det er unødvendigt jf. nødvendighedskriteriet, at biometriske data opbevares på 3.-parts server, forstøder denne opbevaring af data mod GDPRs artikel 25, stk. 2.

Tilsvarende forstøder opbevaringen af biometriske data imod GDPRs artikel 32, stk. 1.a. om at dataminimere i henhold til state-of-the-art-princippet, fordi der findes andre løsninger end at lægge biometriske data i 3.-parts server. Denne løsning kendte man tidligere fra fx en rollebaseret signatur i nemID-erhvervssignatur: firmaet vidste, at det var en medarbejder i virksomheden der loggede på, men man vidste ikke, præcis hvem det var.

Hvis dataminimering efter "State-of-the-art"-princippet jf. GDPRs art. 32, stk. 1.a og eIDAS art. 5,1. skulle gennemføres her, måtte der hverken blive opsamlet eller gemt biometriske data.

---

[58] Som tidligere nævnt kan man ikke de facto vide, om de biometriske data gemmes på 3.-partsserveren, men der findes ikke dokumentation for, at de ikke gør, og derfor antages det her, da det er evident, at MitID kan gøre det.
[59] Iht. Lov om MitID, § 14, kan "Digitaliseringsstyrelsen kortvarigt og i et sikret teknisk miljø behandle følsomme personoplysninger i forbindelse med validering af digitale signaturer i valideringstjenesten i serviceområdet Digital signering"
[60] Beskriv NemID-erhvervssignatur:

Staten har, jf. eIDAS præambel 16, brug for at kunne verificere, at "du er dig"[61] for at kunne lave en digital signatur. Det er som udgangspunkt også acceptabelt[62], at der benyttes biometri som ID. Problemet ved denne sign-on-metode er, at "den som har telefonen, er dig", dvs. det er ikke sikkert alligevel. Og et eksempel på sårbarheden er, at den der har nøglen, i dette tilfælde telefonen, helt konkret er ejeren, uanset om det, som nævnt, er en stjålet telefon. Det betyder de facto, at man ikke kan kontrollere sine nøgler, og dermed kan man heller ikke bevise noget (data er hermed untrustworthy) og ad absurdum betyder det, at hvis jeg får stjålet min telefon, så kan tyven sælge mit hus, uden at jeg kan bevise, at det ikke var mig der gjorde det[63].

Det observeres, at dataminimeringskravet som fremsat i eIDAS artikel 25, stk. 1, som kunne udtrykkes fx via en pseudonym signatur, ikke ses hverken Lov om MitID eller i den tekniske implementering af MitID. Det må konkluderes, at dataminimeringskravet, som er det helt centrale begreb i GDPR, er bortfaldet i lovprocessen undervejs fra GDPR->DBL-> Lov om MitID.

Delkonklusion, MitIDs overholdelse af GDPR og eIDAS

Det må konkluderes, at ovenstående måde at logge på på medfører, at man ikke kan undgå at skabe persondata og der er ingen mulighed for at skabe pseudonyme eller trustworthy signaturer. Desuden fører SSO-teknologien til ulovlig logning (man-in-the-middle data-retention[64]), hvilket forstøder mod GDPRs artikel 25, stk. 2 om at data ikke må hverken opsamles eller opbevares på 3.-parts-servere. Desuden forstøder det imod GDPR-artikel 32, stk. 1.a. handler om pseudonymisering og kryptering iht. at dataminimere jf. state-of the-art jf. eIDAS artikel 5.2.

Forholdet mellem GDPR og DBL i Danmark

DBF er en såkaldt uegentlig forordning. Der er således bestemmelser i forordningen, som skal gennemføres i dansk ret, og bestemmelser, som giver mulighed for at fastsætte særlige danske regler af mere generel og tværgående karakter.

Der er på den baggrund behov for en generel lov om behandling af personoplysninger som supplement til forordningen, og Databeskyttelsesloven (DBL) blev derfor vedtaget i maj 2018.

---

[61] "Sikringsniveauer bør afspejle graden af tillid til, at et elektronisk identifikationsmiddel kan fastslå identiteten på en person og således give sikkerhed for, at den person, der gør krav på en specifik identitet, faktisk er den person, hvortil identiteten er blevet knyttet".

[62] I en persondatarets-kontekst

[63] https://www.sn.dk/ringsted-kommune/aegtepar-udsat-for-svindel-vi-er-helt-afkoblet/?fbclid=IwAR1LuNWlJyMJNSFIj-wcimLg9K7At97Nj1p_U2EzMqIMgp_r5e4bR3vZvMg#

[64] MITM: A man-in-the-middle attack (MITM) is defined as an attack that intercepts communication between two parties with the aim of gathering or altering data for disruption or financial gain. This article explains a man-in-the-middle attack in detail and the best practices for detection and prevention in 2022. https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

Opsamlende kan det konkluderes, at GDPR og DBL supplerer hinanden[65].

Det skal herefter undersøges, hvorledes GDPR forholder sig til MitID, ligesom det først skal undersøges, hvilke muligheder for rum for national lovgivning, GDPR efterlader plads til.

Af præambelbetragtning 8 i GDPR-forordningen fremgår det, at medlemsstaterne, i det omfang de finder det nødvendigt, kan indarbejde elementer i denne forordning i deres nationale ret. Dette forhold ses fx realiseret i DBLs §§ 5-7, der delvis gengiver forordningens tekst.

Af præambelbetragtning 10 i GDPR efterlades et stort rum for nationale regler om behandling af personoplysninger. Dette gælder fx art. 6, stk. 2-3, og art. 9, stk. 4 samt betragtning 45.

Det nævnes specifikt, at det er muligt at "medlemsstaterne har flere sektorspecifikke love på områder, hvor der er behov for mere specifikke bestemmelser. Denne forordning indeholder også en manøvremargen, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger (»følsomme oplysninger«).

Men henset til Hildebrandt/Tielemans-artiklen og dataminimeringskravet jf. GDPR art. 25, stk.1 indebærer det, at tillægslovgivningen kan tilføre nye legitime interesser og hensyn, fx forskning og anticrime iht. GDPRs artikel 23. Måden, man implementerer på, skal stadig overholde dataminimeringskravet jf. artikel 25 i GDPR.

Delkonklusion om samspillet mellem GDPR og DBL

Med pseudonyme signaturer indebærer dataminimeringskravet, at man skal kunne dokumentere nødvendigheden af at lave tranaktionen identificeret i stedet kun identificerbar, herunder hvorvidt man helt kan undlade ansvarlighedsbevis eller sikre, at det kun er en dommer der kan dekryptere.

Delkonklusion, MitID og proportional persondataindsamling- og behandling

Som nævnt kan man med MitID kun logge på en central server, hvilket forhindrer dataminimering jf. GDPRs artikel 25, stk. 2 og GDPRs artikel 32, stk. 1.a, da sessionen per definition bliver identificeret.

Samlet set kan det altså konkluderes, at denne måde at logge på på medfører, at man ikke kan undgå at skabe persondata (ingen mulighed for pseudonyme/trustworthy signaturer). Desuden fører SSO-teknologien til ulovlig logning (man-in-the-middle data-retention[66]) uden grund. Hvis man ikke kan dataminimere, fordi Mitid som teknologi som udgangspunkt altid er programmeret til at "datamaksimere", så forstøder hele konstruktionen af MitID grundlæggende mod GDPR-artiklerne

[65] Disse afgørelser er et eksempel på, hvordan de to retskilder supplerer hinanden: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/mar/risikovurdering-ved-videregivelse-af-personoplysninger?fbclid=IwAR2__lw7HyfXMorZL6W-c1oCDcBv3bayNrCLcGU2F0ScuHpq8dljCKTEScU

[66] MITM: A man-in-the-middle attack (MITM) is defined as an attack that intercepts communication between two parties with the aim of gathering or altering data for disruption or financial gain. This article explains a man-in-the-middle attack in detail and the best practices for detection and prevention in 2022. https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

25, stk. 1 og 2, og 32, stk. 1a. Desuden bør betragtning 11 til eIDAS-forordningen iagttages: ” […] autentifikation i forbindelse med en onlinetjeneste [bør] derfor kun omfatte behandling af de identifikationsdata, [der er] tilstrækkelige, relevante og ikke omfatter mere, end hvad der kræves for at give adgang til den pågældende onlinetjeneste”. Det understreges således, at hensigten med lovgivningen netop er at sikre en proportional behandling af persondata. Dette kan dog ikke opfyldes, når MitID i sit design modarbejder dette proportionalitetskrav.

Forhindrer MitIDs måde at indsamle persondata på, at data behandles trustworthy?

Teknisk definition ift. at konstruere trustworthy anonyme signaturer på:

1) en juridisk bindende signatur – fx afledt fra cpr – anonymt i det anonyme rum (trustworthy pki): man slipper af med den trustede part (fra pseudonym -> anonym) og den eksisterer allerede i henhold til eidas (den gamle, ikke 2.0).

2) løsningen fra 2012 – anonyme akkreditiver –> selected disclosure, en måde hvorpå man kan bevise, at man tilhører en bestemt gruppe, men andre kan ikke identificere, hvem man er (en speciel slags matematik!) Denne metode er først netop blevet standardiseret nu (2023) med verified credentials (bliver introduceret med eIDAS 2.0)

En pseudonym signatur på en kontrakt vil skabe ikke-direkte henførbare persondata: sporbarhed, ansvarlighed, men man har ikke lagt persondata i cloud pga. schrems II-problemet (persondata i cloud).

Delkonklusion, trustworthy persondatabehandling og MitID

MitIDs måde at opsamle persondata på gør, at det forhindres, at data kan behandles trustworthy anonymt i fx forskning og identificerbart men ikke identificeret i andre sammenhæng.

Schrems II-dommen

Privataktivisten Max Schrems har anlagt flere sager ved EUD vedr. den såkaldte ”Privacy Shield”-

aftale mellem US og EU, som handler om overførsel af persondata til US-Cloud. Sagen ved EU-Domstolen udspringer af en retssag, som det irske datatilsyn (DPC) har anlagt på baggrund af en klage fra den østrigske statsborger, Maximillian Schrems. Klagen vedrørte overførsel af hans personoplysninger fra Facebook Ireland til virksomhedens moderselskab Facebook Inc., der er etableret i USA. Facebook Ireland kunne tidligere henholde sig til den såkaldte Safe Harbour-aftale som overførselsgrundlag. Denne aftale betød, at amerikanske virksomheder omfattet af ordningen blev anset for at være beliggende i et 'sikkert tredjeland’. Men efter EU-domstolens underkendelse af Safe Harbour-aftalen mellem EU og USA i Schrems I-dommen, overgik Facebook Ireland til at bruge EU-Kommissionens standardkontrakt som overførselsgrundlag. Omdrejningspunktet er og har været, at amerikanske sikkerhedstjenester, ved fx mistanke om terror, til enhver tid kan forlange indsigt i de amerikanske virksomheders oplysninger, herunder personoplysninger, som er overført af EU-baserede virksomheder til virksomheder i US. Dette krav strider umiddelbart imod EUs GDPR-regler. Når det nævnes i dette projekt, skyldes det, at Schrems II-sagen har påkaldt sig stor opmærksomhed, ikke mindst fordi EU-domstolen har afgjort til fordel for Schrems og imod US.

Når man læser Schrems II-dommen igennem, fylder chartret en del, jf. fx af forordningens (GDPR) indledning fremgår det, af pkt. 1, at beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, er en grundlæggende rettighed. I artikel 8, stk. 1 er også fra chartret og i artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF) fastsættes det, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. Af pkt. 2 fremgår det at "Principperne og reglerne for beskyttelse af fysiske personer i forbindelse med behandling af deres personoplysninger bør, uanset deres nationalitet eller bopæl, respektere deres grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.

Af pkt. 4 fremgår det desuden, at "Behandling af personoplysninger bør have til formål at tjene menneskeheden". Samtidig er retten til beskyttelse af personoplysninger ikke er en absolut ret, men (den) skal ses i sammenhæng med sin funktion i samfundet og afvejes i forhold til andre grundlæggende rettigheder i overensstemmelse med proportionalitetsprincippet. Denne afvejning kommer jeg tilbage til i min perspektivering, da den en grundsten ift. danskernes og EU-borgernes rettigheder på området.

Da dommen behandler hhv. FISAs section 702, E.O. 12333 og PPD-28, skal disse myndigheder kort defineres:

FISA Section 702, E.O. 12333 samt PPD-28 er føderal lovgivning, institutioner i den amerikanske sikkerhedslovgivning, som gælder på tværs af de enkelte amerikanske delstater. E.O. 12333 samt PPD-28 kan karakteriseres som henholdsvis et præsidentielt dekret og et præsidentielt direktiv udstedt af den amerikanske præsident. Disse retlige instrumenter kan, som oven for nævnt, sidestilles med føderal lovgivning[67].

Og som eksempel på, hvilke typer af lovgivning, der således ikke overholder ovennævnte rettigheder (FISAs[68] section 702 eller E.O. 12333, sammenholdt med PPD-28) opfylder de således ikke de mindstekrav, som i henhold til EU-retten er knyttet til proportionalitetsprincippet, således at det ikke kan fastslås, at de overvågningsprogrammer, som er baseret på disse bestemmelser, er begrænset til det strengt nødvendige.

Under disse omstændigheder er de begrænsninger af beskyttelsen af personoplysninger, som følger af USAs nationale lovgivning om de amerikanske offentlige myndigheders adgang til og brug af sådanne oplysninger, der overføres fra Unionen til USA, og som Kommissionen har vurderet i afgørelsen om værnet om privatlivets fred, ikke afgrænset på en sådan måde, at de lever op til krav, som i det væsentlige svarer til dem, der er foreskrevet i EU-retten ved chartrets artikel 52, stk. 1, andet punktum"[69].

---

[67] 8 Patel, Oliver og Lea, Nathan, EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, 2020, s. 23 USA.gov, How Laws Are Made and How to Research Them, https://www.usa.gov/how-laws-are-made (Sidst besøgt 8/5 2023) CRS, Presidential Directives: An Introduction, 2019.

[68] https://www.nsa.gov/Signals-Intelligence/FISA/

[69] Citat fra dommen:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=9714792

Delkonklusion Schrems II-dommen

Konklusionen i Schrems II-dommen er altså, at ganske vist er beskyttelsen af personoplysninger ikke en absolut ret, men skal ses i sammenhæng med proportionalitetsprincippet: omvendt fremgår det, at det ikke kan fastslås, at de overvågningsprogrammer, fx amerikanske FISA benytter, er begrænset til det strengt nødvendige og således værnes der ikke om privatlivets fred på en sådan måde, som det er defineret i Chartrets artikel 52, stk. 1, andet punktum.

Schrems II-dommen statuerer, at Privacy Shield-ordningen ikke er forenelighed med GDPR, art. 45, sammenholdt med EU's Charter om Fundamentale Rettigheder (Charteret) art. 7, 8 og 47 omhandlende privatliv, databeskyttelse og adgangen til effektive retsmidler. Dermed underkendes EU-Kommissionens vurdering om, at USA sikrer en tilstrækkelig beskyttelse af de personoplysninger, der overføres fra EU-området til certificerede amerikanske virksomheder under Privacy Shield-ordningen.

Andre eksempler på ikke-overholdelse af GDPR i Danmark

Af nedenstående artikel[70] fremgår det, at det danske politi ulovligt opsamler persondata, når de fotograferer nummerplader på udvalgte strækninger i Danmark. Formålet med billederne er at generere nummerpladescanninger mhp. at afsløre fx biltyve eller forsikringssvindlere, men derved kommer man også til at fotografere føreren af bilen. Også dette er i strid med både EMRKs artikel 8, stk. 2 om retten til privat – og familieliv og GDPRs artikel 9 vedr. behandling af personfølsomme oplysninger, herunder, som i dette tilfælde, opsamling af biometri. Tilsvarende skal GDPRs artikel 32, stk. 1a om behandlingssikkerhed som eksplicit nævner pseudonymisering og kryptering af personoplysninger iagttages. Og det strider også imod retshåndhævelsesdirektivets artikel 20, stk. 1, som handler om dataminimering og stk. 2, som handler om proportionalitetskravet. Og netop i den grundlæggende regulering for nummerpladescanningen - ANPG[71] - bekendtgørelsen, står der intet om, at man, i forbindelse med nummerpladescanningen, også må tage et billede af føreren. Der er derfor tre problematikker her, nemlig at bekendtgørelsen er upræcis, at proportionalitetskravet ikke overholdes og at trinlavere lovgivning, her dansk sektorlovgivning, får lov at underminere hhv. EMRK og GDPR.

Samlet konklusion

Eftersom dette projekt benytter sig af den retsdogmatiske metode, beskrives gældende ret, og der tilbydes ikke endegyldige svar. Der vil derfor altid være tale om konkrete vurderinger i forhold til alle afgørelserne, da de kan påklages til domstolene for et endeligt facit.

MitID og dataminimering: Som det er fremgået i analysen, overtræder MitID i sit design GDPR-artikel 25, stk. 1 om dataminimering. Kan dataminimeringskravet dernæst tilsidesættes, hvis proportionalitetshensyn i form af fx compliance, anti-crime, forskningshensyn eller andet kræver

[70] https://radarmedia.dk/politiet-tager-uden-tilladelse-et-billede-af-dit-ansigt-naar-de-scanner-din-nummerplade/
[71] Bekendtgørelse 2017-09-20 nr. 1080
om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG)

det? Her er det en væsentlig pointe, at netop det teknologiske stade gør, at det er muligt at dataminimere *uden* at tilsidesætte nogle af ovenstående hensyn. Det vil altså sige, at man kan opfylde de selvsamme behov på samme måde, som man kan teknologisk i dag, blot uden at indsamle og behandle ulovlige persondata samtidig[72].

Også af myndighedernes egen rapport fremgår det, at de skal dataminimere iht. state-of-the-art[73]. Af GDPRs artikel 32[74], stk. 1.a. fremgår det tilsvarende, at den dataansvarlige skal gennemføre pseudonymisering og kryptering iht. at dataminimere jf. state-of the-art.

Igen må man spørge, om proportionalitetsprincippet evt. ville kunne tilsidesætte dette behov, men som udgangspunkt kan proportionalitetsprincippet ikke udgøre et legitimt hensyn her, fordi alle de processer, der fordres af MitID i dag, tilsvarende ville kunne opfyldes med dataminimering, hvis MitID understøttede pseudonymisering. Dette kan realiseres uden at give køb på indhold og tjenester svarende til dem, MitID dækker i dag, blot uden opsamling af persondata (fx compliance-tjenster)[75]. Endvidere hvis et hensyn – fx et økonomisk – skulle have indgået i statens digitaliserings-design, i forhold til at tilsidesætte borgernes privatretlige rettigheder, så skulle staten/MitID have fremlagt det. De har ikke dokumenteret noget som helst, og det skal staten: de skal dokumentere, at deres afvejning ligger inden for proportionalitetsprincippet, at det ikke går ud over det. Det er ikke nok at tilsidesætte vores privatretlige rettigheder uden dokumentation jf. EMRKs artikel 8, stk. 2[76], jf. EMRKs artikel 8, stk. 3.

Det kan tilsvarende konkluderes, at MitID i sit design og sin applikation forstøder mod GDPR-artiklerne 25, stk. 1 og 2, og 32, stk. 1a. Også MitID-pålogningen medfører, at man ikke kan undgå at skabe persondata og der er ingen mulighed for at skabe pseudonyme eller trustworthy[77] signaturer. Desuden fører SSO-teknologien til ulovlig, uhjemlet logning (man-in-the-middle data-retention). MitIDs måde at opsamle persondata på gør dertil, at det forhindres, at data kan behandles trustworthy anonymt.

Da den danske stat opgraderede til MitID, kan man således argumentere for, at man indførte en model, der rent sikkerhedsmæssigt, var af en ringere standard end NemID (Opsummerende er der ingen egenkontrol med nøgler, ingen pseudonyme signaturer) og den overholder ikke GDPR- og eIDAS-forordningerne som indført i mellemtiden.

---

[72] EDPS IPEN Workshop on Digital Identity - State-of-the-art / 2022 – June 22 (europa.eu), fx slide 9, "Problems that can be solved with Trustworthy PKI"

[73] https://www.version2.dk/artikel/faa-overblikket-4-centrale-begreber-der-faar-det-offentlige-til-rime-paa-cloud

[74] art. 5, stk. 1, litra f, jf. art. 5, stk. 2, og til art. 30, stk. 1, litra g

[75] EDPS IPEN Workshop on Digital Identity - State-of-the-art / 2022 – June 22 (europa.eu), se slide 12, "eIDAS & GDPR already in place Trustworthy PKI re-focus to solve the problems"

[76] Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres
ret og frihed.

[77] https://edps.europa.eu/system/files/2022-07/03_-_stephan_engberg_-_edps_trustworthy_pki_engberg_20220622_en_0.pdf, slide 7, "Trustworthy PKI extend and works the same as normal Trusted PKI – except no trusted party or backdoor"

Det må konkluderes, at dataminimeringskravet, som er det helt centrale begreb i GDPR, er bortfaldet i lovprocessen undervejs fra GDPR->DBL-> Lov om MitID. MitID er ikke en eIDAS-pki-model, hvilket vil sige, at den ikke er certifikatbaseret. Løsningen er sårbar, for hvis MitID fx går ned, så kan man som bruger ingenting. Uden papkortet[78] har MitID intet til at sandsynliggøre, at det ikke er MitID selv, der solgte dit hus, eller loggede på for at hente en kopi af dine data hos enhver serviceprovider, tilknyttet MitID.

Da der dertil i Danmark pt kun findes én offentlig anerkendt digital signatur, som giver adgang til alle offentlige platforme, nemlig MitID, gør dette MitID til et monopol. Det er derfor vigtigt at understrege, at de brud på hhv. GDPR-og eIDAS-forordningerne, som er påvist undervejs i projektet, får desto mere markant betydning, fordi det er en teknologi, som den danske befolkning er blevet pålagt at migrere til af myndighederne. Man kan således hævde, at de danske myndigheder påtvinger borgerne at få krænket - opsamlet og behandlet deres persondata - hver eneste dag.

Der er over 4.700.000[79] registrerede brugere af MitID, som således dagligt intetanende jf. GDPRs artikel 25, stk. 1 (om dataminimering) og 2 (lagring på 3.-parts-server), 32, stk. 1a (pseudonymisering og kryptering) og eIDAS, artikel 5.1 (GDPR skal respekteres) får opsamlet og lagret persondata, som fx hosten til 3.-parts-serveren har fri adgang til. Dette er gældende retstilstand på nationalt niveau i den digitale teknologi, om hvilken parterne bag skrev ”med MitID styrker vi sikkerheden”.

Schrems II i relation til MitID: Hvis MitID understøttede pseudonyme signaturer, som de er juridisk forpligtet til jf. GDPR artikel 32, stk 1.a., så kunne virksomheder gennemføre pseudonyme transaktioner også i US-cloud, fordi kontrollen i så fald ville forblive indenfor dansk juridsdiktion. Dette er i klar overensstemmelse med EDPB[80]s anbefalinger omkring Schrems II.

Som retstilstanden er nu, forhindrer MitID danske virksomheder i at overholdes Schrems II og således fører det til en formodning for, at MitID griber voldsomt ind i erhvervslivets muligheder for at udøve lovlige forretning og respektere borgernes rettigheder.

MitID i relation til Hildebrandt og Tielemans-artiklen: artiklen argumenterer for teknologineutralitet for at kunne følge med udviklingen inden for IT-områder. Men artiklen anbefaler samtidig en dynamisk måde at lovgive på i nationalstaterne, hvis man vil opretholde ”privacy by design” og lovgivningen har vi jo, i form af GDPR og eIDAS, men den understøttes ikke af MitIDs teknologidesign.

Uhjemlet fotografering-sagen i relation til MitID: Hvis borgerne i bilen kunne lave en trustworthy signatur, så kunne vedkommende gøre sig ansvarlig på en måde, som først kunne føre til identifikation, når det er verificeret, at en lov er overtrådt, altså hvis en borger fx er mistænkt. MitIDs manglende implementering af pseudonyme signaturer fører til uhjemlet persondataovergreb på andre områder. Og vel at mærke overgreb, som tidligere har kunnet designe sig ud af (NemID-medarbejdersignatur).

---

[78] Som fulgte med NemID-løsningen

[79] https://digst.dk/nyheder/nyhedsarkiv/2022/oktober/sluttidspunktet-for-udrulningen-til-mitid-naermer-sig/

[80] https://edpb.europa.eu/edpb_en, Det europæiske databeskyttelsesråd

Vedr. sagen om politiets ulovlige fotografering af førere af biler, skal det blive interessant at se, hvordan den sag går videre: EMRK er inkoopereret i Grundloven, mens GDPR tager afsæt i Chartret. Begge typer af lovgivning ligger trinhøjere i retskildehierarkiet end ANPG-bekendtgørelsen. Men alligevel gennembores de to trinhøjere typer af sektorlovgivning. Det vil derfor være nødvendigt at prøve lovmæssigheden af den uhjemlede fotografering.

Som sidste spørgsmål kan man reflektere over, hvorfor de relevante nationale styrelser, råd og tilsyn, herunder fx digitaliseringsstyrelsen, datatilsynet[81], rådet for digital etik m.fl. ikke har opdaget eller reageret på, at MitID indeholder nogle markante sikkerhedshuller ift. at opsamle og behandle persondata.

I forbindelse med udkast til ny logningslov fandtes til gengæld et høringssvar, som datatilsynet har afgivet til justitsministeriet ifm. logningsloven, og udkast til revision af loven og deraf fremgår det, at justitsministeren ønsker at bringe overensstemmelse mellem den nye lov og EU-retten som fortolket af EUD. I forlængelse af dette noteres det af datatilsynet, at selv om der lægges op til indskrænkninger ift. gældende regler, så er det datatilsynets opfattelse, at logningsreglerne stadig må forventes at indebære behandling af "store mængder personoplysninger"[82] (Min fremhævning, MHP). Det interessante er her, at datatilsynet faktisk skriver, at loven formentlig stadig, efter en revision, vil være på kanten af loven. Dette høringssvar åbner derfor op for, at i hvert fald Datatilsynet udtrykker et ønske om, at Danmark respekterer GDPR og eIDAS.

Og hvad MitID angår, så skal det blive interessant at følge med i, om det skal prøves for en eller flere nationale og evt. internationale domstole.

Perspektivering

I Charlotte Bagger Tranbergs (CBT) Ph.D. fra 2007 om "Nødvendig behandling af personoplysninger" diskuterer hun i sin konklusion forskellige danske juristers forslag til danske myndigheders fortolkning af nødvendighedskriteriet ift. offentlige myndigheders interne anvendelse.

Det fremgår heraf, at EU-rets-eksperten Niels Fenger argumenterer for en hård/indgribende nødvendighedsvurdering, medens Ekspert i persondataret, Peter Blume, flere steder tilskrives en liberal fortolkning af nødvendighedskriteriet i forhold til offentlige myndigheders interne anvendelse[83] samt en lempelig fortolkning af nødvendighedskravet i de situationer, hvor ikke-fortrolige oplysninger videregives til andre offentlige myndigheder[84]. Endvidere reflekterer CBT, at "Det kan ikke udelukkes, at den milde eller lempelige vurdering af nødvendighedskriteriet har bund i de forhold, at de to forfattere beskuer udfyldningen af kravet fra henholdsvis forvaltnings- og registerretten. Dette udgangspunkt er ikke hensigtsmæssigt på et retsområde som det persondataretlige, hvor der grundlæggende set er tale om beskyttelse af fundamentale rettigheder, der for de almindelige oplysningers vedkommende kun må behandles, når et krav om

[81] Tilsynets primære funktion er at vurdere alle persondataretlige spørgsmål og træffe afgørelser om, hvorvidt en bestemt adfærd sker i overensstemmelse med Databeskyttelsesforordningen samt Databeskyttelsesloven.
[82] https://prodstoragehoeringspo.blob.core.windows.net/d8e3a213-4dbd-4050-8823-b923f869f0eb/Samlede%20h%C3%B8ringssvar%20-%20lovforslag.pdf, side 5

[83] Nødvendig behandling af persondata, side 528
[84] Ibid.

nødvendighed er opfyldt – medmindre der foreligger et samtykke fra den registrerede. Det er som udgangspunkt forbudt at behandle følsomme oplysninger, medmindre den registrerede har samtykket til behandlingen. I denne sammenhæng findes der ikke noget belæg for, at offentlige myndigheder som dataansvarlige skal behandles anderledes end andre dataansvarlige"[85].

Men det er bemærkelsesværdigt, at vi, selv i sådan et lille land som Danmark, tilsyneladende har så forskellige fortolkningsperspektiver på, hvordan GDPR skal fortolkes.

Især er det interessant i forhold til, at man allerede i 2011 vidste (de danske datamyndigheder, It- og Telestyrelsen), at " brugerne skal have mulighed for fuld kontrol over, hvilke data der afgives til hvilke løsninger, og kontrol over om deres data i forskellige løsninger kan kobles sammen" og man vidste også, at det var vigtigt at " informationer, der gemmes om brugere, må ikke kunne henføres direkte til deres fysiske identitet, medmindre dette er strengt nødvendigt og forhandlet. Der bør således anvendes virtuelle identiteter/pseudonymer frem for identificerende nøgler som eksempelvis CPR-numre"[86].

I henhold til problemerne med ulovlig logning som berørt i indledningen, skal det pointeres, at problemet med ulovlig logning kunne være løst med pseudonyme signaturer eller også som beskrevet i "Nye digitale sikkerhedsmodeller" fra 2011.

[85] Ibid., side 529

[86] Stephan Engberg om statslig rapport: Det mest positive udspil i mange år | Version2
(Linket der henviser til dig.styr. er slettet i foråret 2023, kopi af rapporten kan tilgås her: Nye sikkerhedsmodeller - final version.docx (privacytrust.eu)

Litteraturliste:

Blume, Peter "Retssystemet og juridisk metode", 3. udgave, 2016. Jurist- og Økonomforbundets Forlag.

Blume, Peter "Databeskyttelsesret" 5. udgave, 2018. Jurist- og Økonomforbundets Forlag.

Blume, Peter "Den nye persondataret – Forordning 2016/6798 om persondatabeskyttelse" 1.

udgave, 2016. Jurist- og Økonomforbundets Forlag. Side. 56-79

Christensen, Bent, Forvaltningsret, Jurist- og økonomforbundets forlag, 2010

Christoffersen, Jonas m.fl., EUs Charter om Grundlæggende Rettigheder med kommentarer, 2. udgave, 1. oplag, 2018

Fenger, Niels, EU-rettens påvirkning af dansk forvaltningsret, 3. udgave, Jurist- og Økonomforbundets Forlag, 2018

Neergaard, Ulla og Nielsen, Ruth, EU-ret, 8. Udgave, Karnov, 2020

Rytter, Jens-Elo: Individets grundlæggende rettigheder, Karnov, 2019

Tvarnø, Christina D. og Nielsen, Ruth, Retskilder og retsteorier, 5. reviderede udgave, 1. oplag, 2017

Afgørelser:

Oprettelse af sag hos EMD, Foreningen ulovlig logning mod Danmark

https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-222958%22]}

Datatilsynet, risikovurdering, persondatabehandling

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/mar/risikovurdering-ved-videregivelse-af-personoplysninger?fbclid=IwAR2__lw7HyfXMorZL6W-c1oCDcBv3bayNrCLcGU2F0ScuHpq8dljCKTEScU

Domme

Schrems II-dommen:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=9714792

G.D. mod Commissioner of An Garda Síochána,
Minister for Communications, Energy and Natural
Resources (Om ulovlig logning)
https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=325817

Ladsretsdom, ulovlig logning, Foreningen ulovlig logning vs tidligere justitsminister Nick Hækkerup
https://ulovliglogning.dk/landsretsdom

Højesteretsdom
Foreningen ulovlig logning vs tidligere justitsminister Nick Hækkerup
https://ulovliglogning.dk/assets/docs/hrdom.pdf

EUD-dom om EUs logningsdirektiv

https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=6699129https://curia.europa.eu/juris/document/docu

ment.jsf?text=&docid=257242&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=325817

Videnskabelige artikler og projekter

Tranberg, Charlotte Bagger, Nødvendig behandling af personoplysninger, Forlaget Thomson, 2007

https://jura.ku.dk/jurabog/pdf/juridiske-monografier/Tranberg_Nodvendig_behandling_af_personoplysninger_2007.pdf

Fly Steensen, Lars og Svansø Laursen, Jeppe:

Databeskyttelsesforordningens princip om dataminimering, herunder sletning set i forhold til forvaltningslovens regler

https://projekter.aau.dk/projekter/files/414767617/Kandidat_speciale___Fardigt.pdf

Internetkilder

https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvad-er-personoplysninger

https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf

Justitsministeriet.dk ”Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565”

Laursen, Hanne Biehl ”Delt dataansvar”

https://gdprguide.arkivo.dk/vaelg-emne/ansvar-roller/faelles-ansvar

(Sidst tilgået 11.05 - 2023)

https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/betaenkning_1565_del_i_bind_1.pdf (Sidst tilgået 11.05-2023)

Nielsen, Aske og Sørensen Rasmus. ”GDPR.dk”

https://gdpr.dk/databeskyttelsesforordningen/kapitel-8-retsmidler-ansvar-og-sanktioner/artikel-83-generelle-betingelser-for-paalaeggelse-af-administrative-boeder/ (Sidst tilgået 11.05-

2023)

Mortensen, Henning ” GDPR: Hvorfor er privacy vigtigt?”, 2019

https://wiredrelations.com/gdpr-hvorfor-er-privacy-vigtigt/ (Sidst tilgået 11.05-2023)