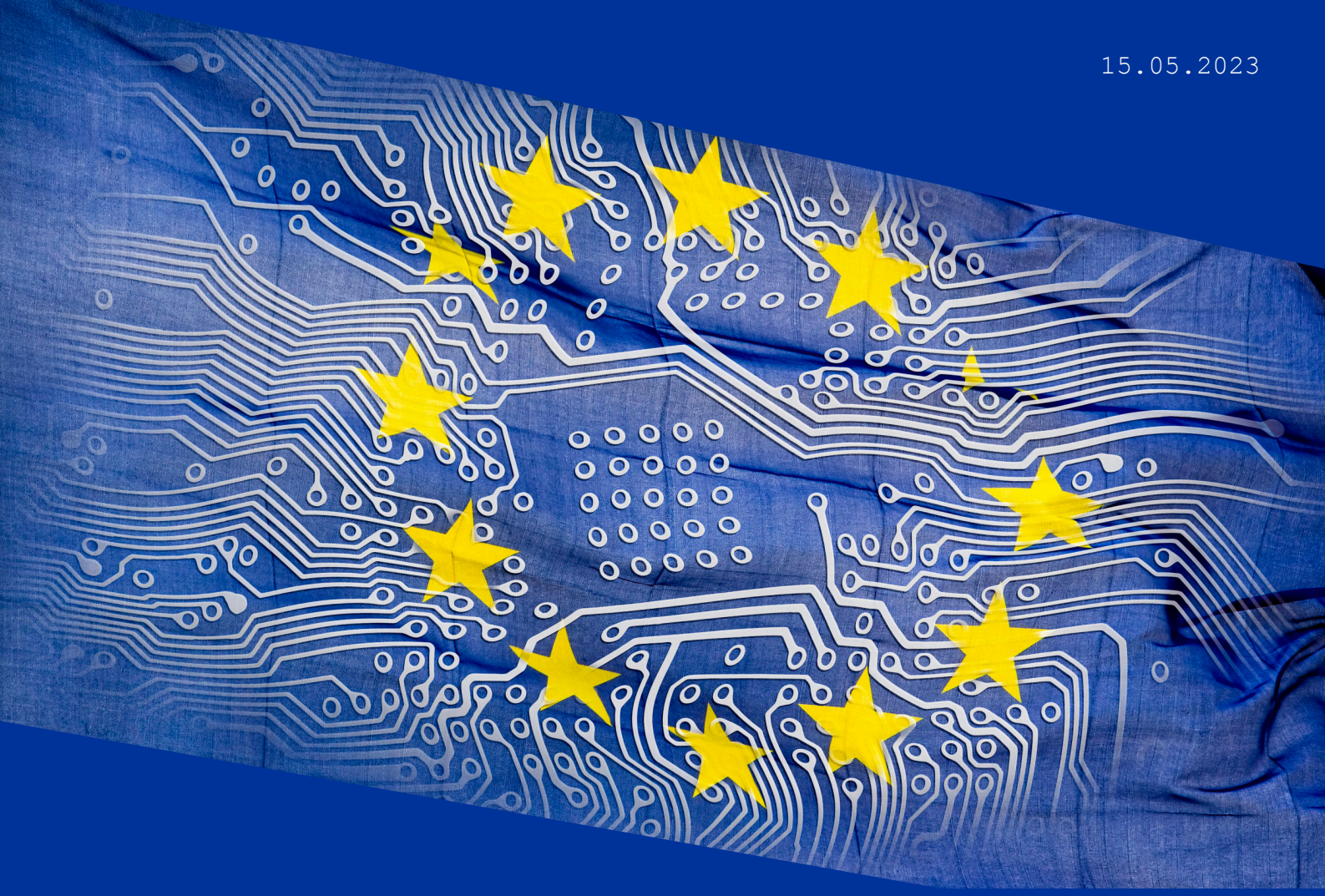
15.05.2023



Databeskyttelse i EU

Eyðvarður Mohr Iversen

Kandidatafhandling
Cand. merc. jur

Vejledere:
Camilla Kampmann
Jakob Olsson

Studienr.: 119732

Antal sider: 85
Antal anslag: 115.088

Abstract

The purpose of this thesis is to analyze GDPR compliance in relation to third country data transfers, how the balance between data protection and competitiveness affects decision-making in this regard, how fine sizes affect strategies and behavior, and what the EU-Commission can do in order to secure the optimal balance between data protection and competitiveness. EU law (GDPR) and economic theories, such as game theory, are used in the analysis. The legal analysis will analyze the current legal state of data transfers to third countries. The economic analysis will analyze how the balance between data protection and competitiveness affects the different stakeholders. The integrated analysis will analyze how the EU can mitigate the current shortcomings and optimize the balance between data protection and competitiveness.

Indholdsfortegnelse

Kapitel 1

1.1 Indledning

Siden internettet så dagens lys, er den teknologiske udvikling i denne sammenhæng gået med lysets hast. Udviklingen har ført til et hav af nyskabende og nyttige opfindelser. Det har dog ikke været uden udfordringer. En af disse udfordringer har været at lovgive om brug og begrænsninger af internettet over hele verden. I EU har udviklingen haft med sig blandt andet databeskyttelsesforordningen. I de enkelte medlemsstater er der også etableret love i forbindelse med databeskyttelse, og i Danmark, blandt andet, kender vi databeskyttelsesloven. Det er en helt central del af EU's arbejde er at beskytte borgernes personoplysninger. En anden central del af EU's arbejdsområde er at sikre EU's konkurrenceevne. Det er derfor ikke svært at se, at disse centrale elementer i EU kan komme til at stride imod hinanden, set i lyset af den hurtigt voksende digitale udvikling, som udspiller sig på verdensplan i dag. Balancen mellem databeskyttelse og konkurrenceevne kommer derfor til at spille en central rolle i den fremtidige udvikling af EU. Strammes lovgivningen for meget, går det ud over virksomhedernes konkurrenceevne, som i sidste ende går ud over økonomien i EU. Er lovgivningen for lempelig, risikerer man, at persondata om EU's borgere kan havne i forkerte hænder og bliver misbrugt til ukendte formål. Den digitale udvikling har ført med sig, at virksomheder kan operere på et globalt plan, særligt tech virksomheder. Dette har gjort det muligt for virksomheder at uddelegere opgaver på tværs af landegrænser. Denne uddelegering kan hjælpe virksomhederne med at fokusere mere på sin kerneviden i stedet for opgaver de nødvendigvis ikke har ekspertise i eller ressourcer til at varetage. På den anden side har dette medført, at der sker overførsler af persondata på tværs af landegrænser. Disse overførsler skaber udfordringer for beskyttelse af

EU borgeres persondata. I dette speciale kigges der nærmere på de gældende regler for persondataoverførelser til tredjelande (med udgangspunkt i USA), samt de økonomiske aspekter af hvordan EU kan sikre overholdelse af gældende lovgivning. Til sidst kigges der på, hvordan de nuværende mangler og udfordringer kan løses og forbedres, således at EU finder den bedst mulige balance mellem databeskyttelse og konkurrenceevne.

1.2 Juridisk problemformulering:

Hvordan sikrer EU, at dataansvarlige, databehandlere og underdatabehandlere overholder GDPR's krav om beskyttelse af personoplysninger i forbindelse med tredjelandsoverførsler?

1.3 Økonomisk problemformulering:

Hvordan påvirker balancen mellem databeskyttelse og konkurrenceevne beslutningstagningen for virksomheder og databehandlere, og hvilken betydning har bødestørrelser og for deres strategier og adfærd?

1.4 Integreret problemformulering:

Hvordan kan EU-kommissionen sikre en mere optimal balance mellem databeskyttelse og konkurrenceevne?

1.5 Afgrænsning

Der vil i den juridiske analyse tages udgangspunkt i persondataoverførsler til USA, da USA er landet hvor de store tech-virksomheder, som Amazon, Google, Meta og Microsoft, har hjemsted. Endvidere har disse virksomheder filialer inden for EU, og nogle af dem har modtaget store GDPR bøder, blandt andet i Irland og Luxembourg. Disse virksomhederne bliver benyttet af store som små virksomheder i EU til mange databehandler formål, det være sig servere, analytiske formål eller markedsføring, med mere. Analysen afgrænses til at omhandle EU-plan. Der bliver derfor ikke dykket ned i nationale love og tilsyn, men de kan dog blive nævnt i fald af de er relevante for analysen.

I den økonomiske analyse vælges der et simultant Bayesiansk spil hellere end et sekventielt, fordi det bedre afspejler, hvordan EU-virksomheder og databehandlere træffer deres beslutninger samtidigt, uden at kende hinandens strategier. Denne spil-variant afspejler en mere realistisk situation, hvor virksomheder og databehandlere ofte skal navigere i et komplekst og usikkert marked uden fuldstændig information om hinandens præferencer og handlinger.

1.6 Synsvinkel

Synsvinklen er EU- kommissionens synsvinkel. Denne synsvinkel ser problemformuleringerne ud fra et perspektiv der ønsker, at lovgivningen er så optimal som muligt, for alle parter i EU. EU Kommissionen er EU's udøvende magt. EU kommissionen foreslår ny lovgivning og kontrollerer, at medlemsstaterne overholder de gældende love og regler.

EU kommissionen beskriver sine formål som følgende:

"*Kommissionen udvikler og gennemfører EU's politikker ved at:*

fremsætte forslag om lovgivning til Europa-Parlamentet og Rådet for Den Europæiske Union
hjælpe medlemslandene med at indføre EU-lovgivning
forvalte EU's budget og tildele støtte
sikre, at EU-lovgivningen overholdes (sammen med Domstolen)
repræsentere EU uden for Europa (sammen med EU's diplomatiske tjeneste – Tjenesten for EU's Optræden Udadtil).
EU's politikker er udformet, så de er til gavn for borgere, virksomheder og andre interessenter i EU. Kommissionens initiativer til nye politikker skal vedtages internt i henhold til en fast procedure."[1]

EU-Kommissionens rolle og beføjelser er fastsat i traktaterne:
Traktaten om Den Europæiske Union (TEU): Artikel 17
Traktaten om Den Europæiske Unions Funktionsmåde (TEUF): Artikel 244-250

1.7 Metode

1.7.1 Juridisk metode

Formålet med det juridiske metodeafsnit er at præsentere og beskrive de juridiske forskningsmetoder, der er anvendt i dette speciale for at besvare den juridiske problemformulering. Afsnittet vil først præsentere den overordnede metodiske tilgang og derefter gå i dybden med de juridiske kilder og analysemetoder. Til sidst vil afsnittet tage fat på de etiske overvejelser og begrænsninger, der er forbundet med de valgte metoder.

[1] https://commission.europa.eu/about-european-commission/what-european-commission-does/strategy-and-policy_da

1.7.1.1 Metodisk tilgang

Dette speciale anvender en retsdogmatisk metodisk tilgang til at besvare den juridiske analyse. Denne tilgang er valgt, fordi den tillader en systematisk og struktureret analyse af juridiske kilder og regler. Da specialet tager udgangspunkt i EU-retten, anvendes den retsdogmatiske analyse i relation til denne. Rangordenen for regulering i EU retten er:

1. Regulering: Traktater, forordninger, direktiver og afgørelser
2. Retspraksis: EU-domme og afgørelser
3. Retsprincipper: En række generelle principper, som f.eks. proportionalitetsprincipper og princippet on EU-konform fortolkning

EU-rettens kilder deles op i henholdsvis den primære og den sekundære EU-ret.
Der benyttes i specialet både primære og sekundære retskilder. Desuden er der hard-law og soft-law i EU-retten.
Hard-law er juridisk bindende retsakter, som omfatter: traktater, forordninger, direktiver og afgørelser. Soft-law omfatter ikke-bindende retsinstrumenter, såsom meddelelser, retningslinjer, anbefalinger, osv.

1.7.1.2 Juridiske kilder

Juridiske kilder, der er anvendt i dette speciale, omfatter følgende:

Primære kilder:

TEUF art. 16 (hard-law): Anvendes fordi den indeholder bestemmelsen i art. 16, stk. 1.: ”*Enhver har ret til beskyttelse af personoplysninger om vedkommende selv.*”

Sekundære kilder:

GDPR (hard-law): Anvendes fordi det er den forordning der regulerer databeskyttelse.

Databeskyttelsesloven (hard-law): nævnes, men bruges ikke i analysen.

Schrems-II-dommen (Hard-law): Bruges i analysen.

En række domme (hard-law): Bruges i juridisk metode og juridisk analyseafsnittet.

Afgørelse fra det Østrigske datatilsyn om microtargeting[2] (hard-law): Bruges i analysen.

Afgørelse fra det Irske datatilsyn om Meta (hard-law): Bruges i analysen.

Afgørelse fra EDPB om Meta (hard-law): Bruges i analysen.

Vejledning fra Datatilsynet (soft-law): Bliver henvist til denne som led i et eksempel.

Juridisk litteratur, herunder bøger, artikler, rapporter og kommentarer, der diskuterer de relevante juridiske spørgsmål og regler. Disse kilder bruges til at supplere og uddybe analysen og til at præsentere og præcisere forskellige fortolkninger og argumenter.

1.7.1.3 Analysemetoder

Analysen af de juridiske kilder blev udført ved hjælp af følgende metoder:

Lovfortolkning: Systematisk analyse og fortolkning af relevante lovbestemmelser og principper i TEUF art. 16, GDPR og Databeskyttelsesloven med henblik på at afdække deres betydning og anvendelse i praksis.

[2] Microtargeting er brugen af online persondata til at skræddersy reklamebudskaber til enkeltpersoner baseret på identifikation af modtageres personlige træk.

Retspraksisanalyse: Undersøgelse af relevante domme, herunder *Schrems*-II-dommen og andre domme nævnt i specialet, samt afgørelser fra det Østrigske datatilsyn, for at identificere og sammenligne fortolkning og anvendelse af lovgivningen og juridiske principper.

Disse metoder og tilgange er valgt for at sikre en systematisk, struktureret og dybdegående analyse af de relevante juridiske spørgsmål og problematikker i overensstemmelse med specialets problemstillingen.

1.7.2 Økonomisk metode

Formålet med den økonomiske metode er at beskrive de metoder og analyseværktøjer, der er anvendt i dette speciale. Ved metodevalg benyttes explanans og explanandum[3], da der udvælges modeller ud fra, hvad der ønskes at undersøge på baggrund af problemformuleringen. Der anvendes neoklassisk økonomisk teori. Neoklassisk teori betragter virksomheden som profitmaksimerende, fuldt rationel og som en produktionsfunktion. Den anvender matematiske beskrivelser af økonomiske problemer og tager udgangspunkt i, at agenter er rationelle og har fuldstændig information.[4]

Statistikker om datamængde og økonomisk betydning af data præsenteres, for at danne et overblik over udviklingen og den økonomiske betydning af data i den europæiske økonomi. Dette gøres for at vise, at EU-kommissionen bør have en interesse i, at området er reguleret optimalt.

Der vil i den økonomiske analyse gøres brug af spilteori. Der opstilles to spil ud fra spilteorien, for at undersøge hvordan spillerne agerer ud fra de opsatte forudsætninger.

[3] Tvarnø & Denta (2018), s. 252
[4] Tvarnø & Nielsen (2017), s. 433

Det første spil er et spil med 3 spillere; EU-Kommissionen, EU-virksomheder og databehandlere. Spillet løses med Elimination of Strictly Dominated Strategies (IESDS) og best response.[5]

Det næste spil er et Bayesiansk simultan spil med to spillerne, EU-virksomheder og databehandlere. I dette spil lægges der til grund, at spillerne har asymmetrisk information og forskellige præferencer.

Sekventielt spil er fravalgt i analysen, fordi det simultane spil afspejler, at EU-virksomheder og databehandlere træffer deres beslutninger samtidigt uden at kende hinandens strategier. Dette afspejler en mere realistisk situation, hvor virksomheder og databehandlere ofte skal navigere i et komplekst og usikkert marked uden fuldstændig information om hinandens præferencer og handlinger.

Et sekventielt spil kan også være relevant i nogle situationer. I et sekventielt spil træffer spillerne beslutninger efter tur, således at den næste spiller allerede kender den første spillers beslutning, før han træffer sin egen. Dette kan give mening, hvis vi antager, at EU-virksomheder først vælger en strategi (f.eks., at prioritere databeskyttelse eller konkurrenceevne), og at databehandlerne derefter vælger deres strategi baseret på EU-virksomhedernes valg.

Til sidst bruges en økonomisk model fra *The Economic Theory of Public Enforcement of Law*[6]. Modellen søger at finde den optimale balance mellem håndhævelsesomkostninger og sanktioner for at minimere samfundets samlede omkostninger ved lovovertrædelser og håndhævelse, og dermed opnå effektiv offentlig retshåndhævelse. Modellen tilpasses til

[5] Baird et al (1994) kap., 1 & 2
[6] Polinsky & Shavell (1999), s. 4-6

specialet, da f for virksomheder kan have flere negative økonomiske konsekvenser udover en bøde, som f.eks. erstatning, sagsomkostninger, negativ omtale eller tab af kunder.

Modellen ser derfor således ud[7]: $g > p(f + (t \cdot \lambda))$

Modellen har følgende variabler:

$g = Opnået\ værdi\ af\ lovovertrædende\ handling$

$p = Sandsynlighed\ for\ at\ blive\ opdaget$

$f = Bøde\ (negative\ konsekvenser)$

$t = Straffens\ længde$

$\lambda = Marginal\ afskrækkelseseffekt$[8]

Modellen fastsætter, at $g > 0$ hvis en lovovertrædende handling skal være økonomisk fordelagtig. Hvis $g < 0$, er handlingen ikke fordelagtig, og dermed vil der ikke være nogen grund til at foretage handlingen. Hvis $g = 0$, vil en risikoneutral EU-virksomhed være indifferent med at foretage sig noget.

I den del af specialet, hvor der forekommer økonomiske beregninger i forbindelse med spilteori, er de baseret på antagelser. Specialet bliver udarbejdet ud fra den hypotetiske-deduktive forklaringsmodel, da der tages udgangspunkt i teorien og udledes en række

[7] Polinsky & Shavell (1999), s. 4-6

[8] Den marginale afskrækkelseseffekt angiver, hvor meget reduktion i skader forårsaget af lovovertrædelser der opnås ved at øge den forventede sanktion (sanktioner gange sandsynligheden for at blive fanget).

forudsigelser og antagelser. Antagelserne og afvigelserne gør, at resultatet af analysen har en vis usikkerhed. Usikkerheden vil derfor blive taget i betragtning i diskussionen.

Teorivalget og modelvalget bliver benyttet til at vise hvordan spillerne vil agere ud fra de givne antagelser. Ud fra EU-Kommissionens synsvinkel kan resultaterne bruges som en indikator på, hvordan spillerne reagerer på lovgivning.

1.7.3 Integreret metode

I den integrerede analyse tages der udgangspunkt i den økonomiske og juridiske analyse. Analyserne vil samle den økonomiske og juridiske del og skabe en sammenhæng mellem dem. Udgangspunktet i analysen vil være spørgsmålet om, hvorvidt den nuværende regulering er optimal set fra EU-kommissionens perspektiv. Der vil også vurderes om reguleringen kan laves mere optimalt.

Der kigges på GDPR's præambel for at få et billede af hensigten med GDPR.

Der benyttes retspolitisk teori til at overveje, hvordan retten bør være – *de lege ferenda*[9]. Den står i modsætning til den retsdogmatiske analyse, som er udtryk for, hvad en domstol vil komme frem til med de givne retskilder og brug af den retsdogmatiske analyse – *de lege lata*.[10]

Til sidst laves der en efficiensanalyse, som tager udgangspunkt i Kaldor/Hicks princippet. Efficiensanalysen vil redegøre for fordele og ulemper og diskutere om fordelene kan opveje de negative konsekvenser, og dermed finde ud af om der kan ske en optimering eller ikke ud fra Kaldor/Hicks princippet.

[9] Tvarnø & Nielsen (2017), s. 445-446
[10] Tvarnø & Nielsen (2017), s. 445-446

1.8 Struktur

Kapitel 1 indeholder en indledning til specialet og emnet. I forlængelse af dette beskrives en problemstilling om EU's beskyttelse af persondata. Herefter bliver selve problemformuleringen udformet på baggrund af indledningen og problemstillingen. Selve problemformuleringerne er delt i 3, henholdsvis en juridisk, en økonomisk og en integreret problemformulering. Dernæst er et afgrænsningsafsnit, og til sidst vil selve projektets metoder og teorier beskrives i et metodeafsnit, som bliver delt op i en juridisk, økonomisk og integreret del. I dette afsnit forklares den juridiske, økonomiske og integrerede metode, de benyttede teorier vil blive præsenteret og der vil blive begrundet for de valgte teorier.

Kapitel 2 indeholder projektets juridiske analyse. Kapitlet starter med at indlede den juridiske analyse. Herefter bliver der gennemgået, hvordan virksomheder i EU sikrer databeskyttelse i forbindelse med overførsel af data til USA, som der tages udgangspunkt i. Databeskyttelsesforordningen[11] (herefter "GDPR") vil være udgangspunkt i besvarelsen af hvordan beskyttelse af persondata sikres i forbindelse med overførsler. Efterfølgende vil der blive undersøgt nærmere om de mulige farer, som er forbundet med utilstrækkelig databeskyttelse. Der vil i den juridiske analyse blive inddraget relevante domme og afgørelser.

Kapitel 3 indeholder den økonomiske analyse. Kapitlet starter med en kort indledning, hvorefter der opstilles to spilteoretiske spil, som søger at redegøre for de pågældende aktørers beslutningstagen. Dernæst opstilles der en teoretisk økonomisk model, som søger at redegøre for hvordan virksomheder træffer beslutninger om databeskyttelse set i lyset af de nuværende

[11] Den Europæiske Union, Forordning (EU) 2016/679 (Generelle databeskyttelsesforordning), 2016, https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32016R0679

bødestørrelser. Derefter inddrages et eksempel fra virkeligheden, som bliver brugt til at analysere og diskutere de andre resultater i analysen. Til sidst kommer den økonomiske delkonklusion.

Kapitel 4 Indeholder den integrerede analyse. Kapitlet starter med en indledning. Derefter bliver der med udgangspunkt i GDPR's præambel diskuteret om databeskyttelse kontra konkurrenceevne. Endvidere bliver de nuværende mangler i GDPR præsenteret ud fra resultaterne i den juridiske og økonomiske analyse, og herefter vil de blive analyseret og diskuteret. Til sidst afrundes kapitlet på baggrund af den integrerede analyse med den integrerede delkonklusion.

Kapitel 5 indeholder specialets endelige konklusion, hvor der vil være en sammenfatning af de vigtigste pointer fra analyserne, og en besvarelse af problemformuleringerne.

Kapitel 2 - Juridisk analyse og delkonklusion

2.1 Indledning

Persondataforordningen - *General Data Protection Regulation* – herefter ”GDPR”- trådte i kraft den 25. maj 2018. GDPR’s formål er at beskytte de europæiske borgeres grundlæggende rettigheder og frihedsrettigheder, ved at sikre, at persondata behandles på en forsvarlig og ansvarlig måde. En af de centrale bestemmelser i GDPR er, at persondata kun må overføres til tredjelande, hvis tredjelandet har et tilstrækkeligt niveau af databeskyttelse. Bestemmelserne fremgår i GDPR kapitel 5.

Den juridiske analyse vil fokusere på overførsel af persondata til tredjelande, herunder USA. Analysen vil også undersøge de juridiske regler i forbindelse med hvordan virksomheder overfører data til tredjelande, når de bruger databehandlere og underdatabehandlere. Eksempler på dette kan være, at EU-virksomheder anvender store amerikanske tech virksomheder, såsom Meta eller Amazon, som databehandlere eller underdatabehandlere, og dermed overfører data ud af EU.

Analysen tager udgangspunkt i GDPR og anden relevant EU-lovgivning og praksis, samt nationale retlige rammer og praksis i EU-medlemsstater. Formålet med analysen er at give en dybere indsigt i de juridiske problemstillinger i forbindelse med overførsel af persondata til tredjelande.

2.2 Persondata

Persondatabeskyttelse er nævnt i TEUF - Traktaten om den Europæiske Unions Funktionsområde. Der er i TEUF art. 16, stk. 1 fastslået, at:

"*Enhver har ret til beskyttelse af personoplysninger om vedkommende selv.*"

I afsnittet stadfæstes den grundlæggende ret til beskyttelse af personoplysninger for alle personer med EU borgerskab. Princippet er en central del i EU's databeskyttelseslovgivning og danner grundlaget for GDPR.

2.3 Databeskyttelsesforordningen

Databeskyttelsesforordning/*The General Data Protection Regulation* (GDPR), er EU's omfattende lovgivning om beskyttelse af personoplysninger og privatlivets fred. GDPR har til formål at styrke og harmonisere databeskyttelsesreglerne i EU og give enkeltpersoner større kontrol over deres personoplysninger.
Persondata er defineret i GDPR's artikel 4, stk. 1., som:

"[...] *enhver form for information om en identificeret eller identificerbar fysisk person* [...][12].

GDPR's definition er bred og åben, hvilket kan gøre det indviklet at præcisere persondata i et konkret tilfælde. På den anden side sikrer den brede definition, at databeskyttelsesreglerne er

[12] Databeskyttelsesforordningen 2016/679

fleksible og i stand til at tage højde for nye teknologier og metoder til behandling af personoplysninger.
Definitionen af persondata er imidlertid blevet nærmere konkretiseret i en række EU-domme, som har bidraget til en yderligere forståelse af begrebet.

I **Sag C-582/14**, blev det fastslået, at dynamiske IP-adresser kan anses for at være persondata, hvis den kan kombineres med andre personoplysninger og dermed gøre det muligt at identificere en person, jf. præmis 49.

Sag C-434/16 fastslår, at eksamensbesvarelser og de tilknyttede kommentarer indeholdt persondata, fordi oplysningerne kunne tilknyttes en identificerbar person, jf. præmis 33-35.

Sag C-28/08 P fastslår, at navnene på personer der deltager i møder, er persondata, da de kan tilknyttes til en identificerbar person, jf. præmis 63.

Udover "almindelige" persondata findes der også en særlig kategori af persondata, som i modsætning til "almindelige" persondata er en udtømmende liste af sensitive/følsomme persondata.
GDPR art. 9 omhandler behandling af en særlig kategori af persondata, følsomme/sensitive personodata. De defineres i stk. 1, som oplysninger om:

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold

- Genetiske eller biometriske data - med det formål entydigt at identificere en fysisk person
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering

2.3.1 Behandlingsgrundlag

For at kunne behandle persondata og sensitiv persondata, skal der foreligge en lovlig begrundelse. Ifølge GDPR art. 6, er der seks lovlige grunde for behandling af persondata:

- Samtykke
- Kontrakt
- Juridiske foranstaltninger
- Vitale interesse
- Offentlig interesse eller myndighedsudøvelse
- Legitim interesse

For at kunne behandle persondata, skal der foreligge samtykke eller en aftale mellem den registrerede og den dataansvarlige, jf. GDPR art. 7, stk. 1., nr. 1. Samtykke skal gives frivilligt, informeret og utvetydigt. Det betyder, at den registrerede skal have tilstrækkelig information om, hvad data bliver brugt til, og den registrerede skal have mulighed for aktivt at give eller nægte samtykke.

Hvis der er tale om sensitiv persondata, skal de specifikke betingelser i art. 9, stk. 2 være opfyldt.

2.3.2 Dataansvarlige, databehandlere og underdatabehandlere

Der kigges nu nærmere på hvad persondata og følsomt persondata kan bruges til af virksomheder, leverandører og underleverandører - som i forbindelse med GDPR betegnes som henholdsvis dataansvarlig, databehandler og underdatabehandler - for at få en forståelse af hvorfor og hvordan data overføres til lande uden for EU.

Eksempel med almindeligt persondata: Det kunne være en bank der får persondata fra sine kunder for at kunne yde banktjenester til kunden. Banken gør brug af en række digitale løsninger i deres drift. En del af denne drift kan være uddelegeret til databehandlere, eksempelvis at de bruger server tjenester fra en anden virksomhed til at opbevare deres data. Dermed sker en overførsel fra banken (den dataansvarlige) til serverudbyderen (databehandleren).

Eksempel med følsomt/sensitivt persondata: Det kan være en medicinal produktionsvirksomhed, som udvikler høreapparater. I forbindelse med deres udvikling indsamler de scanningsbilleder af ører fra folk med smalle øregange (helbredsdata). Virksomheden beskæftiger sig kun med hvordan produktet skal udvikles, og står således ikke for selve produktionen af høreapparatet. Dem der står for produktionen, er en virksomhed uden for EU. For at produktionsvirksomheden uden for EU skal kunne udvikle produktet, har de behov for scanningsbillederne. Dem får de, og dermed er der sket en overførsel af følsomt/sensitivt persondata til en databehandler.

I enhver situation hvor persondata bliver overført til en databehandler eller underdatabehandler, skal det foregå i overensstemmelse med GDPR art. 28, 29, 32 og 33. Nogle af kravene er:

Skriftlig kontrakt: Dataansvarlige og databehandleren skal indgå en skriftlig kontrakt eller en anden juridisk bindende aftale, som fastlægger de specifikke opgaver, instruktioner og forpligtelser, databehandleren skal følge, jf. art. 28, stk. 3. Denne aftale kaldes almindeligt for en databehandleraftale.

Passende sikkerhedsforanstaltninger: Databehandlere skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau for de personoplysninger, de behandler, jf. art. 32.

Underdatabehandlere: Hvis en databehandler ønsker at anvende en underdatabehandler, skal databehandleren indhente forudgående skriftligt samtykke fra dataansvarlig. Desuden skal de samme krav, der gælder for dataansvarlige i deres aftale med databehandleren, også gælde for databehandlerens aftale med underdatabehandleren, jf. art. 28, stk. 2 og 4.

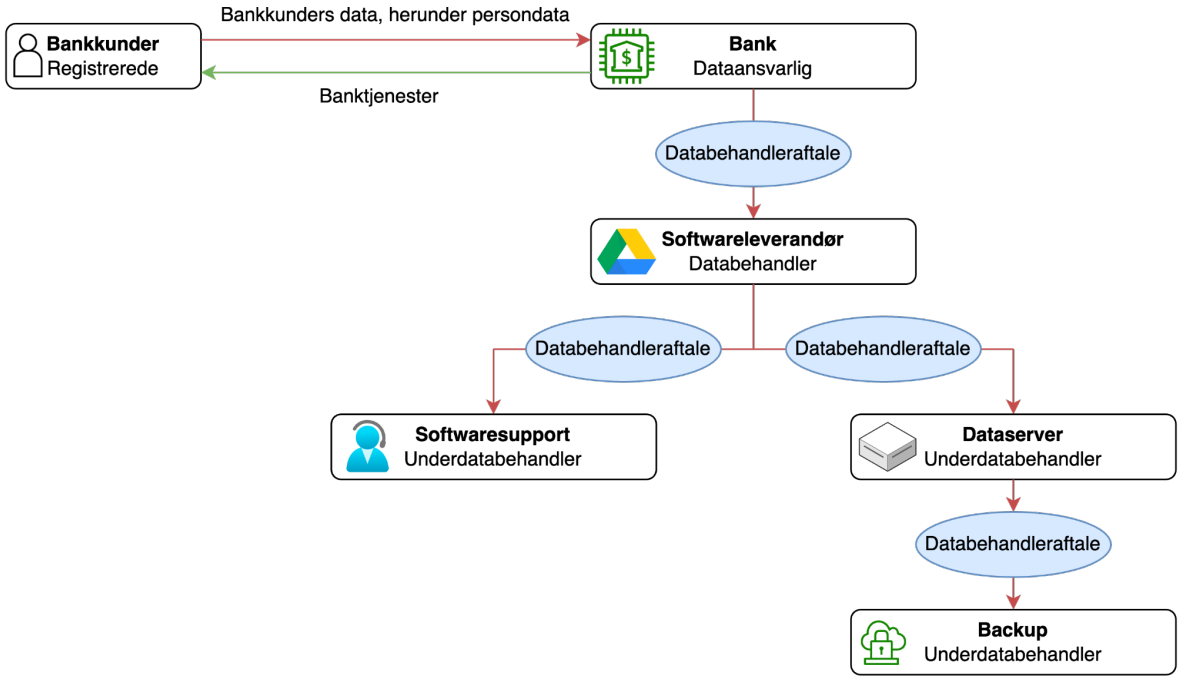
Bistand og samarbejde: Databehandlere skal bistå dataansvarlige i at overholde deres forpligtelser i henhold til GDPR, f.eks. ved at bistå i forbindelse med anmodninger fra registrerede om at udøve deres rettigheder, samt samarbejde med tilsynsmyndighederne, jf. art. 28, stk. 3.

Underretning om brud på persondatasikkerheden: Databehandlere skal underrette dataansvarlige uden unødig forsinkelse, efter at de er blevet bekendt med et brud på persondatasikkerheden, jf. art. 33, stk. 2.

2.3.3 Illustration af databehandlerkonstellation

Herunder ses en illustration af mulige konstellationer, der har databehandlere og underdatabehandlere inden for EU og EØS, samt en illustration af en konstellation med databehandlere og underdatabehandlere i USA.

En databehandler-konstellation der sker inden for EU og EØS kan eksempelvis se således ud:



Kilde: Egen tilvirkning

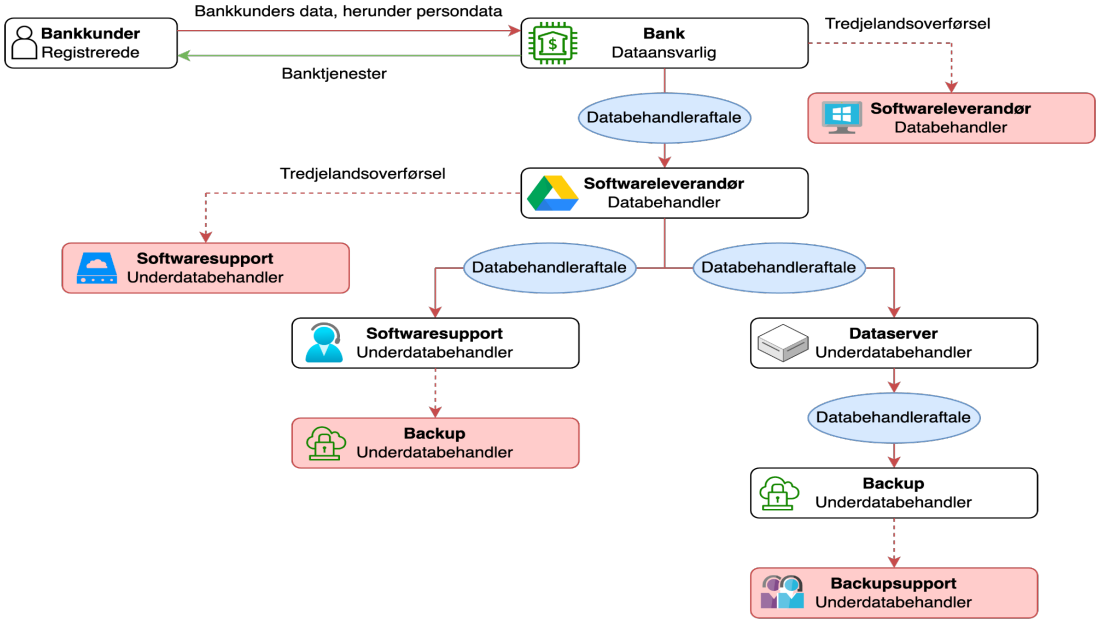
I diagrammet antages det, at der er tale om persondataoverførsler gennem hele kæden.

De røde pile symboliserer overførsler af persondata.

I eksemplet er der en underdatabehandler i første led. Der er ikke begrænsninger på hvor mange led af underdatabehandlere, der er tilladt i GDPR. Men eksempelvis kræves det fra det danske datatilsyn i en vejledning, at virksomheder har et komplet overblik over alle databehandlere og underdatabehandlere.[13] Datatilsynet har som eksempel udtalt[14], at de har set virksomheder med underdatabehandlere helt ned i 20. led. Det viser hvor komplicerede databehandlingskonstellationer kan være.

Databehandlerkonstellationer kan også indebære overførsler til tredjelande. Tredjelande defineres i GDPR art. 45.

En databehandlerkonstellation som indeholder tredjelandsoverførsler kan eksempelvis se således ud (det antages, at overførslen er til USA som tredjeland):



Kilde: Egen tilvirkning

[13] Vejledning om Cloud (2022), s. 15, Punkt 3.2.1, Særligt ad pkt. f) - https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

[14] https://dreambroker.com/channel/cqc3sjcb/iframe/jcxnv96f?autoplay=1, fra omkring minut 36:30

I diagrammet antages det, at der er tale om persondataoverførsler gennem hele kæden. De stiplede røde pile repræsenterer overførslerne til tredjeland. De røde kasser repræsenterer databehandlere i tredjeland.

Det relativt simple diagram viser, at en tredjelandsoverførsel principielt kan ske i alle led i kæden af databehandlere og underdatabehandlere.

2.3.4 Tredjelandsoverførsler

GDPR indeholder specifikke regler og krav for overførsel af personoplysninger til lande uden for EU og EØS. Tredjelandsoverførsler er reguleret i GDPR kapitel 5, art. 44 - 50. Persondata må kun overføres til et tredjeland eller en international organisation, hvis dataansvarlige og databehandlere overholder betingelserne i kapitel 5.

Artikel 44 - Generelle principper for overførsel:
Denne artikel understreger, at overførsel af personoplysninger til tredjelande eller internationale organisationer skal være underlagt GDPR's principper og krav. Desuden skal sådanne overførsler beskytte de registreredes rettigheder og friheder.

Artikel 45 - Overførsel på grundlag af en afgørelse om tilstrækkeligt beskyttelsesniveau:
Overførsel af personoplysninger til et tredjeland eller en international organisation kan finde sted, hvis EU-Kommissionen har afgjort, at landet eller organisationen har et tilstrækkeligt beskyttelsesniveau. Denne afgørelse tages på baggrund af landets eller organisationens

databeskyttelseslovgivning og evne til at håndhæve disse love. I *Den Europæiske Unions Tidende* offentliggør EU-kommissionen en liste over tredjelande, områder og specifikke sektorer i tredjelande samt internationale organisationer, som den har fastslået sikrer eller ikke længere sikrer et tilstrækkeligt beskyttelsesniveau, jf. Art. 45, stk. 8.

Artikel 46 - Overførsel med passende beskyttelsesforanstaltninger:

Hvis et tredjeland eller en international organisation ikke har en afgørelse om tilstrækkeligt beskyttelsesniveau, kan overførsel stadig finde sted, hvis der er passende beskyttelsesforanstaltninger på plads. Dette kan omfatte juridisk bindende og gennemførlige aftaler mellem offentlige myndigheder, standardkontraktbestemmelser vedtaget af EU-Kommissionen, eller godkendte adfærdskodekser og certificeringsmekanismer.

Artikel 47 - Bindende virksomhedsregler:

Bindende virksomhedsregler (BCR'er) er interne regler vedtaget af multinationale virksomheder for at sikre et tilstrækkeligt beskyttelsesniveau ved overførsel af personoplysninger inden for virksomhedsgruppen. BCR'er skal godkendes af den relevante tilsynsmyndighed og opfylde visse krav, som er beskrevet i denne artikel.

Artikel 48 - Overførsel eller videregivelse, der ikke er tilladt af unionsretten:

Denne artikel fastslår, at en overførsel eller videregivelse af personoplysninger til et tredjeland eller en international organisation ikke må finde sted, hvis den er i strid med EU-retten. Dette kan f.eks. gælde, hvis en udenlandsk domstol eller forvaltningsmyndighed anmoder om overførsel eller videregivelse af oplysninger uden at følge de rette kanaler.

Artikel 49 - Undtagelser for specifikke situationer:

I specifikke situationer kan overførsel af personoplysninger til tredjelande eller internationale organisationer finde sted, selv uden et tilstrækkeligt beskyttelsesniveau eller passende beskyttelsesforanstaltninger, hvis der er en af følgende undtagelser:

a) Den registrerede har udtrykkeligt samtykket til overførslen efter at være blevet informeret om de mulige risici.

b) Overførslen er nødvendig for at opfylde en kontrakt mellem den registrerede og dataansvarlige eller for at træffe foranstaltninger på den registreredes anmodning forud for indgåelse af en kontrakt.

c) Overførslen er nødvendig for indgåelse eller opfyldelse af en kontrakt, der er indgået eller skal indgås i den registreredes interesse mellem dataansvarlige og en anden fysisk eller juridisk person.

d) Overførslen er nødvendig af hensyn til vigtige grunde i det offentliges interesse.

e) Overførslen er nødvendig for konstatering, udøvelse eller forsvar af retskrav.

f) Overførslen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser, når den registrerede er fysisk eller juridisk ude af stand til at give samtykke.

g) Overførslen sker fra et offentligt register, der er lovligt tilgængeligt for offentligheden.

Det bemærkes, at disse undtagelser skal anvendes i begrænset omfang og kun i tilfælde, hvor ingen af de andre mekanismer, der er beskrevet i kapitel 5, kan anvendes.

Artikel 50 - Internationale samarbejdsprocedurer:
For at fremme internationalt samarbejde og ensartede beskyttelsesniveauer for personoplysninger opfordrer denne artikel EU-Kommissionen, tilsynsmyndighederne, og andre relevante organer til at samarbejde med tredjelandes og internationale organisationers databeskyttelsesmyndigheder. Dette samarbejde kan omfatte udveksling af oplysninger og bedste praksis, bistand i forbindelse med kontrolaktiviteter og gensidig bistand ved håndhævelse af lovgivningen.

2.4 USA som tredjeland

I analysen tages der udgangspunkt i overførsler til USA. USA er ikke medlem af EU eller EØS og betragtes derfor som et tredjeland ud fra EU's databeskyttelsesforordning. Derfor betragtes alle overførsler af persondata fra EU til USA som tredjelandsoverførsler.

En af de centrale udfordringer med overførsler til USA er deres behandling og håndtering af persondata. Særligt er det de amerikanske overvågningsprogrammer, der vækker bekymring hos de europæiske myndigheder. PRISM-programmet er et af disse overvågningsprogrammer.

De forskellige tilgange som EU og USA har til databehandling har gjort det vanskeligt at overføre persondata til USA, men med en række aftaler og foranstaltninger, som *Safe Harbor*

og *Privacy Shield,* har man gennem tiden forsøgt at gøre det nemmere at overføre persondata fra EU til USA.

Safe Harbor-aftalen var en aftale, der blev lavet mellem EU-kommissionen og myndighederne i USA i 2000. Den gik ud på, at persondata fra EU godt kunne opbevares og være tilstrækkeligt beskyttet i USA i overensstemmelse med databeskyttelsesdirektivet fra 1995, Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet), EFT L 281 af 23.11.1995 (gældende indtil maj 2018), selvom USA er betragtet som et usikkert tredjeland. På baggrund af *Schrems*-I-dommen, C-362/14, blev *Safe Harbor*-aftalen i 2015 erklæret ugyldig. Ugyldiggørelsen af *Safe Harbor* ledte til, at der i 2016 blev indgået en ny aftale - *Privacy Shield*-aftalen.

Imidlertid gav *Schrems*-I-dommen anledning til revurdering af databeskyttelsesdirektivet fra 1995. Revurderingen ledte til, at der i 2018 blev vedtaget en databeskyttelsesforordning, som trådte i kraft den 25. maj 2018, forordning 2016/679.

Privacy Shield-aftalen indeholdt forpligtelser for virksomheder der overfører data mellem EU og USA. Forpligtelserne omfattede blandt andet krav om gennemsigtighed i forbindelse med behandling af data, rettigheder til individer i form af adgang og rettelse af deres personlige oplysninger.

Men i 2020 blev *Privacy Shield*-aftalen erklæret ugyldig som følge af *Schrems-II*-dommen[15]. EU-domstolen fastlagde, at *Privacy Shield*-aftalen ikke længere er et gyldigt overførelsesgrundlag, da der vurderes, at ordningen ikke indeholder fornøden beskyttelse af persondata set i lyset af USA's lovgivning om national sikkerhed. Det er særligt amerikanske overvågningsprogrammer, såsom *PRISM* og *Upstream*, som vækker bekymring.

PRISM er et overvågningsprogram, der blev afsløret i 2013 af whistlebloweren Edward Snowden. Det er et hemmeligt program under USA's Nationale Sikkerhedsagentur (NSA), som indsamler og analyserer data fra internettjenester og elektroniske kommunikationsmidler. Programmet giver NSA adgang til e-mails, chatbeskeder, videoer, fotos, opkaldshistorik og andre typer data fra store tech-virksomheder som Google, Facebook, Microsoft og Apple. PRISM er en del af en række overvågningsprogrammer iværksat i kølvandet på 9/11-angrebene, og rettet mod udenlandske borgere, der er under mistanke for at udgøre en trussel mod USA's nationale sikkerhed.[16]

Upstream er et andet overvågningsprogram, som også blev afsløret af Edward Snowden i 2013. Det er en del af USA's Nationale Sikkerhedsagenturs (NSA) massive overvågningsindsats, der har til formål at indsamle og analysere data fra internationale telekommunikationskabler og infrastruktur. Upstream giver NSA mulighed for at aflytte data i realtid, mens den passerer gennem internetbackbone og fiberoptiske kabler. Programmet

[15] Sag C-311/18

[16] Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 7). NSA Prism program taps into user data of Apple, Google and others. The Guardian. Lokaliseret på https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data d. 14.05.2023

fokuserer primært på kommunikation mellem personer uden for USA og personer, der er under mistanke for at udgøre en trussel mod landets nationale sikkerhed.[17]

Overvågningsprogrammerne gav de amerikanske myndigheder adgang til persondata uden tilstrækkelig beskyttelse af de berørte personer. *Schrems-II*-dommen fastslog, at *Privacy-Shield*-aftalen ikke sikrer et tilstrækkeligt beskyttelsesniveau.
Dommen førte til, at det er blevet sværere at overføre persondata til USA og andre lande uden for EU. *Scherms-II*-dommen ugyldiggjorte ikke brugen af standardaftaler, men gjorde, at virksomheder, som bruger standardaftaler nu, skal foretage grundigere risikovurdering og eventuelt yderligere beskyttelsesforanstaltninger, for at sikre overholdelse af GDPR.

2.4.1 Efter *Schrems-II*-dommen

Som en konsekvens af Schrems-II dommen og afgørelsen om *Privacy Shield's* ugyldighed meddelte EU-kommissionen i december 2022, at man er gået i gang med at lave et nyt *EU-US* rammeværk*, Data Privacy Framework*, som skal gøre det muligt at overføre data fra EU til USA i overensstemmelse med GDPR. EU-kommissionen forventer, at rammeværket træder i kraft i juli 2023.

Da *Privacy-Shield*-aftalen ikke længere kan bruges som grundlag for overførsler til USA, må virksomheder i dag bruge andre mekanismer, såsom standard kontrakter - Standard Contractual

[17] Gallagher, R., & Greenwald, G. (2014, May 19). Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas. The Intercept. Lokaliseret på https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ d. 14.05.2023

Clauses (SCC) eller Bindende Virksomhedsregler - Binding Corporate Rules (BCR), til at overføre persondata til USA.

Dette har ført til, at man fra national side gennem databeskyttelsestilsyn har udarbejdet vejledninger i forbindelse med dataoverførsler, og hvordan disse kan gøres i overensstemmelse med GDPR. Nedenfor ses et eksempel på en tabel, som det danske datatilsyn[18] har udarbejdet:

Overførselsgrundlag	Målgruppe	Ulemper	Fordele
Standardbestemmelser	Både offentlige myndigheder og private virksomheder	• Begrænset mulighed for at foretage ændringer.	• Intet krav om godkendelse fra Datatilsynet. • Kan anvendes i de fleste overførselssituationer, og de enkelte moduler kan kombineres, så aftalen dækker flere overførselssituationer. • Der kan løbende tilføjes/fjernes parter. • Må gerne indarbejdes i databehandleraftale/hovedaftalen, så man kan nøjes med ét samlet aftaledokument.
Ad hoc kontrakt	Både offentlige myndigheder og private virksomheder	• Skal godkendes af Datatilsynet og EDPB. • Kan være ressourcekrævende at udarbejde.	• Anvendes typisk som alternativ til standardbestemmelserne. • Du har selv indflydelse på indhold og udformning, hvilket især er relevant, hvor man ønsker at fravige standardbestemmelserne.
Bindende virksomhedsregler	Større koncerner mv.	• Skal godkendes af Datatilsynet og EDPB. • Kan være ressourcekrævende at udarbejde. • Kan kun anvendes internt i koncernen.	• Kan dække alle overførsler internt i en koncern. • Kan indgå som del af koncernens samlede compliance set-up.
Retlig bindende instrument	Offentlige myndigheder	• Kan være ressourcekrævende at udarbejde.	• Intet krav om godkendelse fra Datatilsynet. • Kan dække alle overførsler mellem de involverede myndigheder.
Administrative ordninger Bilag 2	Offentlige myndigheder	• Skal godkendes af Datatilsynet og EDPB.	• Kan dække alle overførsler mellem de involverede myndigheder.

Schrems-II-dommen fremhævede, at amerikanske overvågningslove, såsom FISA Section 702[19] og Executive Order 12333[20], potentielt kan give amerikanske myndigheder adgang til EU-borgeres data uden tilstrækkelige beskyttelsesforanstaltninger og uden effektive retsmidler for de berørte personer.

[18] Datatilsynets vejledning (2022), s. 16, https://www.datatilsynet.dk/Media/637902777513932912/Vejledning%20om%20overf%C3%B8rsel%20til%20tredjelande.pdf

[19] https://www.govinfo.gov/content/pkg/PLAW-110publ261/html/PLAW-110publ261.htm

[20] https://www.archives.gov/federal-register/codification/executive-order/12333.html

Så længe der ikke eksisterer et nyt rammeværk mellem EU og USA, kan der være "hul" i lovgivningen, fordi en overførsel til USA muligvis ikke er i overensstemmelse med GDPR's krav om tilstrækkelig beskyttelse, selvom der anvendes SCC'er og BCR'er.

SCC'er og BCR'er kan indeholde strenge databeskyttelsesforpligtelser, men uanset hvor strenge forpligtelserne er, kan de ikke beskytte EU-borgeres data fra at blive overvåget af de amerikanske myndigheder under deres overvågningsprogrammer. Til gengæld kan et rammeværk mellem EU og USA skabe klare retningslinjer og beskytte mod overvågning fra USA.

2.5 Afgørelse fra det østrigske datatilsyn

En afgørelse fra det østrigske datatilsyn[21][22] viser hvordan der i praksis bliver begået ulovlige persondataoverførsler til USA.

Sagen omhandler en person, som i august 2020 besøgte en hjemmeside hos et østrigsk medie imens vedkommende var logget på sin personlige Facebook profil. Mediet gjorde på tidspunktet brug af et Facebook Login værktøj, som gør det muligt for brugere at få adgang til en hjemmeside via deres Facebook-konto, i stedet for at skulle oprette en ny konto hos det pågældende medie. Mediet benyttede også Facebook Pixel værktøjet, som gjorde det muligt at spore den besøgendes aktiviteter på hjemmesiden. Ifølge data-subjektet, var adgangen til hjemmesiden alene nok til at udløse en ulovlig overførsel af persondata til USA.

[21] Oversat og redigeret sammendrag fra GDPRHub https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2022-0.726.643

[22] Hele afgørelsen fra det østrigske datatilsyn kan læses på tysk her: https://noyb.eu/sites/default/files/2023-03/Bescheid%20redacted.pdf

Data-subjektet indgav derfor en klage mod mediet, hvori der klages om en overtrædelse af GDPR art. 44. Derudover hævdede data-subjektet, at Meta havde overtrådt GDPR art. 5, stk. 2, 28 og 29.

Under det østrigske datatilsyns undersøgelser hævdede den dataansvarlige at have deaktiveret Facebook-værktøjerne efter at klagen var indgivet. Desuden argumenterede den for, at den eneste direkte kontraktspart for den dataansvarlige var Meta Platforms Ireland Limited. Følgelig var efterfølgende overførsler, inklusive overførsler uden for EU, uden for dets kompetenceområde. Endelig erklærede virksomheden, at overførsler var berettiget i lyset af medieprivilegiet. Meta Platforms Inc. hævdede at være en simpel underdatabehandler på vegne af Meta Platforms Ireland Limited, hvortil GDPR ikke gælder.

Den registrerede gjorde indsigelse mod, at deaktivering af værktøjerne ikke var relevant, da overtrædelsen allerede var sket. Den registrerede understregede også, at den dataansvarlige ikke kunne stole på journalistiske undtagelser, givet karakteren og omstændighederne ved dataoverførslen. Endelig hævdede den registrerede, at GDPR kapitel 5 gælder for alle dataoverførsler, uagtet den subjektive kvalifikation af de involverede aktører.

Om Meta Platforms Inc.

Ifølge den østrigske DPA overtrådte Meta Platforms Inc. ikke art. 44 og følgende GDPR, da det blot var en dataimportør, der faldt uden for rammerne af GDPR kapitel 5. I forbindelse med overførslen afslørede Meta ikke data, men modtog dem kun. Meta var heller ikke ansvarlig i henhold til GDPR art. 5, stk. 2, da dette er en forpligtelse overfor den dataansvarlige. Det østrigske datatilsyn uddybede ikke den subjektive kvalifikation af Meta under GDPR, men den mente ikke at have tilstrækkeligt bevis i det aktuelle tilfælde for at betragte det som en

dataansvarlig. For så vidt angår GDPR art. 28 og 29, regulerer de kun forholdet mellem dataansvarlige og databehandlere og giver ikke en subjektiv rettighed til de registrerede.

Om det østrigske selskab

På den anden side fastholdt det østrigske datatilsyn klagen mod den dataansvarlige. For det første var det ikke tilstrækkeligt at selskabet deaktiverede Facebook-værktøjerne efter klagen for at udelukke en overtrædelse af GDPR art. 44 og følgende, da overtrædelsen allerede var sket.

Det østrigske datatilsyn præciserede også rækkevidden af den journalistiske undtagelse, som østrigsk lovgivning giver i overensstemmelse med GDPR art. 85. Ifølge Sag C-73/07:
"*behandles personoplysninger til journalistiske formål, hvis behandlingen udelukkende har til formål at udbrede information, meninger eller ideer til offentligheden*".
Facebook-værktøjer, som var tilgængelige på den dataansvarliges hjemmeside, blev derimod anvendt til sporing og for at lette login-proceduren. Desuden kunne data, når de var overført til Meta Ireland, anvendes til yderligere formål. Derfor gjaldt medieprivilegiet ikke for den sag, der var til behandling.

Herefter undersøgte det østrigske datatilsyn, om der var tale om international dataoverførsel i henhold til kapitel 5 i GDPR, og om denne var lovlig. Set i lyset af *Schrems II*-dommen giver GDPR art. 44 en subjektiv ret, der kan håndhæves gennem en klage i henhold til GDPR art. 77, stk. 1. Data, der blev overført til USA via Facebook-værktøjerne, var personoplysninger. Faktisk kunne Meta Platforms Ireland Limited - databehandleren - koble data overført fra hjemmesiden til data relateret til den registreredes Facebook-konto. EU-retspraksis viser, at det

ikke var nødvendigt, at hjemmesiden havde al den information, der kræves for identifikation af den registrerede. Det østrigske datatilsyn afviste også som irrelevant, argumentet om, at den dataansvarlige efter overførslen til Meta ikke længere ville have kontrol over yderligere behandling. Faktisk accepterede den dataansvarlige i henhold til art. 28, stk. 2, at databehandleren (Meta Platforms Ireland Limited) kunne bruge en underdatabehandler baseret uden for EU (Meta Platforms Inc.) til at behandle data. Derfor fandt en international dataoverførsel faktisk sted.

Vedrørende lovligheden af overførslen kunne det østrigske datatilsyn ikke finde noget juridisk grundlag. På den ene side blev EU-Kommissionens afgørelse om tilstrækkelighed for overførsel af data fra EU til USA erklæret ugyldig af *Schrems II*-dommen. Derfor kunne dataimportøren og dataeksportøren ikke støtte på GDPR art. 45. På den anden side implementerede Meta standardkontraktbestemmelser i henhold til GDPR art. 46 først efter tidspunktet for de omhandlede forhold. Derfor overførte den dataansvarlige ulovligt den registreredes persondata til USA og overtrådte dermed GDPR kapitel 5.[23]

Afgørelsen viser betydningen af *Schrems-II*-dommen. Den understreger, at virksomheder ikke længere kan bruge *Privacy-Shield*-aftalen mellem EU og USA som juridisk grundlag i forbindelse med dataoverførsler til USA.
Den understreger, at virksomheder der overfører persondata til tredjeparter (databehandlere og underdatabehandlere) der befinder sig i blandt andet USA, er ansvarlige for at sikre, at der foreligger et passende juridisk grundlag og passende sikkerhedsforanstaltninger i forbindelse

[23] Sammendrag af afgørelsen fra det østrigske datatilsyn. https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2022-0.726.643

med overførslen. Afgørelsen viser, at en dataansvarlig kan blive stillet til ansvar for ulovlig overførsel, selvom den direkte kontraktspart er en databehandler inden for EU. Desuden understreger dette vigtigheden af, at den dataansvarlige tjekker og har styr på alle led i kæden af eventuelle underdatabehandlere.

Afgørelsen understreger betydningen af at have gyldige SCC'er på plads når der overføres persondata ud af EU. Selvom Meta Platforms Inc. havde implementeret SCC'er efter forholdene, var det ikke tilstrækkeligt til at retfærdiggøre overførslen på tidspunktet for overtrædelsen.

Afgørelsen fastsætter, at journalistiske undtagelser ikke kan bruges som et generelt juridisk grundlag for overførsel af persondata, især når de overførte data bruges til andre formål, såsom sporing og til login-procedurer.

Afgørelsen viser, at GDPR gælder for alle dataoverførsler, uanset den subjektive kvalifikation af de involverede aktører. Selvom Meta Platforms Inc. hævdede at være en underdatabehandler, hvor GDPR ikke gælder, blev overførslen alligevel betragtet som ulovlig.

Samlet set viser denne afgørelse, at virksomheder skal være opmærksomme på deres ansvar og forpligtelser, når de overfører persondata til USA og andre tredjelande, og at de skal træffe de nødvendige foranstaltninger for at sikre overholdelse af GDPR.

Sagen fra det østrigske datatilsyn fandt sted efter *Schrems II*-dommen, hvilket betyder, at *Privacy Shield*-aftalen har været ugyldig på tidspunktet. Dette understreger vigtigheden af, at der foreligger SCC'er og en databehandleraftale, der tager højde for de risici, der er forbundet med overførsel af persondata til lande uden for EU, når der bliver indgået et dataansvarlig-databehandler samarbejde mellem virksomheder. Dette indebærer en vurdering af det

pågældende lands databeskyttelsesniveau, og om niveauet er tilstrækkeligt til at opfylde GDPR's krav.

Det er værd at bemærke, at afgørelsen fra det østrigske datatilsyns viser, at databehandlere og underdatabehandlere har et delt ansvar for at overholde GDPR's bestemmelser. Det fremhæver betydningen af et tæt samarbejde mellem parterne (dataansvarlig og databehandler og evt. underdatabehandlere) for at sikre, at de nødvendige garantier er på plads, og at der er en fælles forståelse af deres respektive roller og ansvar.

Afgørelsen viser, at der er udfordringer i samarbejdet mellem databehandlere og underdatabehandlere gennem fælles standarder, politikker og procedurer. Derudover er der måske manglende uddannelse og bevidstgørelse omkring GDPR's krav og databeskyttelsesprincipper i organisationerne.

Endvidere er der udfordringer, som små og mellemstore virksomheder (SMV'er) kan stå over for i forbindelse med at overholde GDPR, da de ikke nødvendigvis har samme ressourcer til at varetage GDPR compliance, som større virksomheder.

2.6 Juridisk delkonklusion

På baggrund af den juridiske analyse konkluderes det, at der er betydelige udfordringer ved at sikre, at dataansvarlige, databehandlere og underdatabehandlere overholder GDPR i forbindelse med tredjelandsoverførsler. Disse skal adresseres og forbedres, hvis overholdelsen af GDPR skal sikres. Afgørelsen fra det østrigske datatilsyn viser flere aktuelle problemer og mangler. Manglerne inkluderer utilstrækkelig gennemsigtighed og åbenhed omkring dataoverførsler mellem virksomheder og deres kunder, samt manglende overvågning og opdatering af databeskyttelsespolitikker og procedurer hos virksomheder.

Samarbejdet mellem nationale datatilsynsmyndigheder inden for EU og tredjelande er også problematisk, hvilket fører til en inkonsekvent håndhævelse af GDPR og juridiske usikkerheder.

Fra EU-Kommissionens synsvinkel er der også mangler i samarbejdet med internationale partnere, hvilket fører til utilstrækkelig beskyttelse af personoplysninger på globalt plan. Der er behov for at forhandle aftaler eller rammeværk med tredjelande, herunder USA, som sikrer et passende beskyttelsesniveau for personoplysninger. Det at man på nuværende tidspunkt baserer overførsler til USA på SCC'er og BCR'er er også en risiko i sig selv, da disse ikke nødvendigvis kan forhindre, at EU-borgeres persondata bliver overvåget af amerikanske overvågningsprogrammer.

Derfor skal EU sikre, at der rettes op på de nuværende mangler, da manglerne i sidste ende udgør en risiko for, at borgernes rettigheder og personoplysninger ikke er tilstrækkeligt beskyttet i den digitale tidsalder.

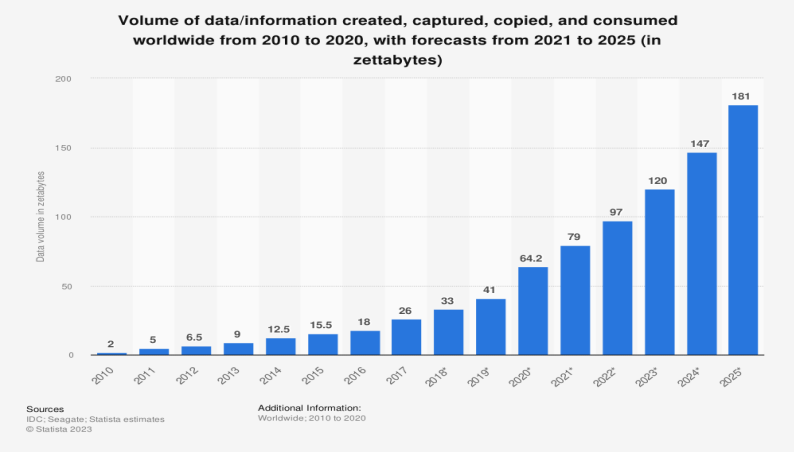
Kapitel 3 - Økonomisk analyse og delkonklusion

3.1 Indledning

I takt med den digitale udvikling er data, herunder perondata, blevet en vigtig ressource og en stigende værdifuld vare, både for virksomheder og myndigheder. Mængden af data som indsamles, behandles og anvendes, er vokset eksponentielt over de seneste år (se tabeller nedenfor), og dermed også dens økonomiske betydning. I den økonomiske analyse kigges der på den økonomiske udvikling og betydning af data. Dernæst laves der en spilteoretisk analyse af, hvordan aktørerne, EU-kommissionen, EU-virksomheder og databehandlere, agerer, for at illustrere hvordan aktørerne træffer beslutninger om databeskyttelse og konkurrenceevne. Til sidst analyseres sager fra den virkelige verden, hvor der er blevet udstedt bøder, som kan give en kontekst for, hvordan regelovertrædelser og databeskyttelsesstandarder håndhæves i praksis, og hvilken betydning det har for EU-virksomheder og databehandlere.

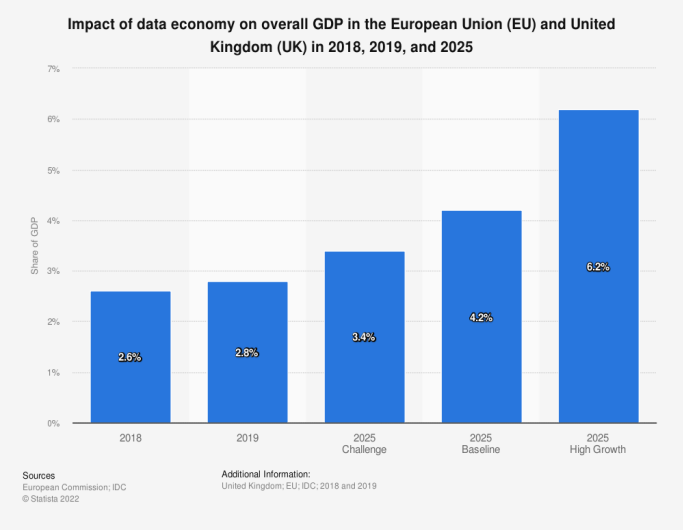
3.2 Digitalisering

Den digitale udvikling kan tydeligt ses, hvis der kigges på statistikker over hvor meget data der bliver indsamlet i EU over tid. Nedenfor ses en tabel, som viser udviklingen over tid.



Kilde: www.statistica.com[24]

Endvidere viser en tabel fra statistica den samlede indvirkning, data har haft på bruttonationalproduktet i EU og Storbritannien i 2018, 2019 og så en prognose for 2025:



Kilde: www.statistica.com[25]

Den digitale udvikling har gjort det muligt at indhente enorme mængder data, hvilket har åbnet op for muligheden til at benytte disse data til sine egne formål i forbindelse med forbedring af produkter, tjenester, effektivitet, informeret beslutningstagning og konkurrence. Dette ses blandt andet i forbindelse med markedsføring, som ved hjælp af data personaliseres til specifikke målgrupper og dermed giver bedre resultater for de virksomheder, der gør brug af disse værktøjer.

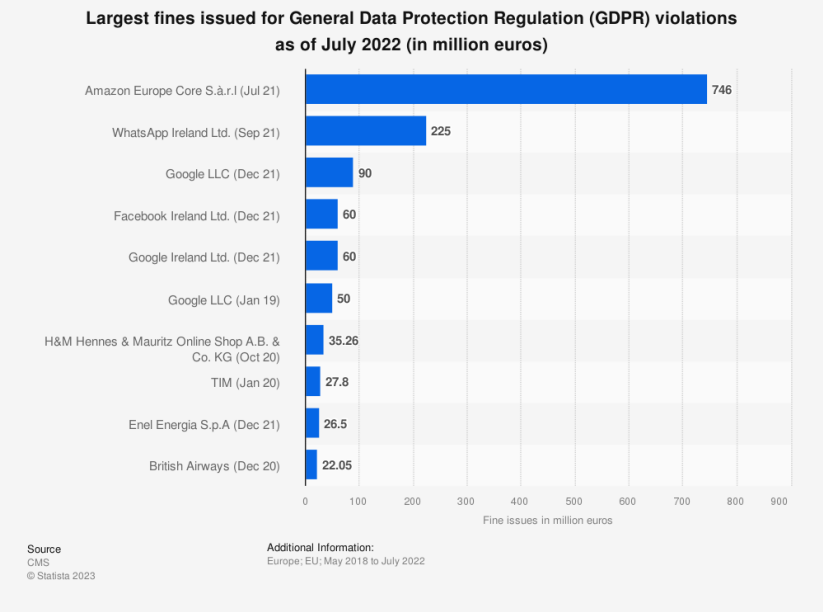
[24] https://www-statista-com.esc-web.lib.cbs.dk/statistics/871513/worldwide-data-created/?locale=en besøgt d 14.05.2023
[25] https://www-statista-com.esc-web.lib.cbs.dk/statistics/1135014/impact-of-data-economy-on-gdp-eu-uk/ besøgt d. 14.05.2023

Ved at overholde GDPR, kan virksomheder opnå en række gevinster, som indirekte kan have betydning for deres ydeevne (performance):

- Styrket kundetillid
- Reduktion af risici
- Forbedret sikkerhedskultur

Generelt kan virksomheder drage fordel af at have de fornødne data-beskyttelsesforanstaltninger implementeret, da det kan give adgang til markeder, hvor dette er et krav. Disse foranstaltninger kan, f.eks., også give virksomheder der ligger uden for EU adgang til EU-markedet.

På den anden side indebærer indsamlingen og behandlingen af persondata en øget risiko for misbrug og overtrædelse af personlige rettigheder, som kan have økonomiske konsekvenser for dem der bruger og/eller behandler data, og ikke mindst personlige konsekvenser for dem, hvis data er blevet misbrugt.
Grafen nedenfor viser de største bøder, som er blevet udstedt i forbindelse med GDPR - overtrædelser i EU.



Kilde: www.statistica.com[26]

Grafen viser, at der eksempelvis er udstedt bøder til henholdsvis Amazon på EUR 746 millioner og WhatsApp for EUR 225 millioner. Bøderne viser, at myndighederne er parate til at udstede store bøder for overtrædelser af GDPR. For virksomhederne, særligt de store, betyder det, at de i høj grad må tage databeskyttelse i betragtning, når de udfører sit arbejde, hvis de ikke vil risikere at få en bøde af denne størrelsesorden.

I et databeskyttelsesperspektiv betyder det, at dataansvarlige, databehandlere og underdatabehandlere må være meget opmærksomme på indholdet og rammerne i GDPR.

3.3 Spilteoretisk analyse

For at analysere problemstillingen imellem EU-virksomheder (dataansvarlige), databehandlere og EU-Kommissionen vil der anvendes spilteori, der er en gren inden for økonomi, der beskæftiger sig med at analysere interaktioner mellem beslutningstagere i forskellige

[26] https://www-statista-com.esc-web.lib.cbs.dk/statistics/1133337/largest-fines-issued-gdpr/ besøgt d. 14.05.2023

situationer. Spilteori kan hjælpe os med at forstå, hvordan aktørerne i denne situation træffer beslutninger i forhold til databeskyttelse, konkurrenceevne og regulering.
Der undersøges hvordan EU-virksomheder, databehandlere og EU-kommissionen navigerer i dette komplekse landskab, og hvilke strategier de kan vælge for at opnå deres mål.

Der opstilles et simultant spil med tre aktører: EU-virksomheder (spiller 1), databehandlere (spiller 2) og EU-kommissionen (spiller 3). Hver aktør har to strategier at vælge imellem: at prioritere databeskyttelse (strategi A) eller at prioritere konkurrenceevne (strategi B). EU-virksomhederne skal vælge mellem databehandlere med strenge eller lempelige databeskyttelsesstandarder, mens databehandlerne skal vælge, om de vil implementere yderligere sikkerhedsforanstaltninger eller tilbyde mere gennemsigtighed og kontrol over data overfor deres kunder. EU-kommissionen skal vælge mellem at implementere strenge eller lempelige reguleringer, afhængigt af om de vil fokusere på at beskytte EU-borgeres data eller sikre EU's konkurrenceevne.

Ved at opstille spillet i en matrice og analysere de forskellige kombinationer af strategier og deres respektive payoffs, kan Nash-ligevægten identificeres, som er den situation, hvor ingen af spillerne har incitament til at skifte strategi, givet de andre spilleres valg. Dette kan give indsigt i, hvordan aktørerne vil optræde i et miljø med fuldkommen information, og hvilke resultater der kan forventes.

Analysen er relevant for EU-Kommissionen, virksomheder og forbrugere, da den kan hjælpe med at forstå, hvordan de forskellige aktører træffer beslutninger og prioriterer mellem

databeskyttelse og konkurrenceevne. Resultaterne af analysen kan informere om både virksomhedernes strategier og politikernes beslutninger om regulering af databeskyttelse.

Analyse er baseret på et teoretisk spil og indeholder dermed visse forenklinger og antagelser. I praksis vil aktørerne stå over for en række faktorer og usikkerheder, der kan påvirke deres beslutninger og adfærd. Derudover er det vigtigt at tage højde for dynamiske aspekter og forandringer i det økonomiske landskab, teknologiske fremskridt og lovgivningsmæssige ændringer, som alle kan have indflydelse på aktørernes strategier og beslutninger.

3.3.1 Aktørerne beskrives som følgende:

EU-virksomhederne: Kan vælge databehandlere med strenge databeskyttelses-standarder for at opnå større tillid fra kunder og myndigheder, men disse tjenester kan da være forbundet med højere omkostninger. På den anden side kan virksomheder vælge databehandlere med lempelige standarder for at spare penge og øge deres konkurrenceevne, men dermed med en højere risiko for databrud (lækager) og potentielle bøder.

Databehandlere: Kan vælge at implementere yderligere sikkerhedsforanstaltninger eller tilbyde mere gennemsigtighed og kontrol over data for deres kunder. På denne måde kan databehandlere differentiere sig fra konkurrenterne og tilbyde strenge eller lempelige databeskyttelses-standarder, selvom de stadig overholder den gældende lovgivning. En databehandler, der tilbyder strenge standarder, garderer sig udover de lovmæssige krav for at beskytte persondata, mens en databehandler, der tilbyder lempelige standarder, kun opfylder de grundlæggende krav i lovgivningen.

EU-kommissionen: Kan vælge mellem streng eller lempelig regulering, afhængigt af om de vil fokusere på at beskytte EU-borgeres data, eller om de i større grad vil sikre EU's konkurrenceevne, og dermed gå på kompromis med databeskyttelse.

3.3.1.1 Strategier:

- EU-virksomheder (spiller 1) har to strategier:
    - Strategi A: Prioritere databeskyttelse
    - Strategi B: Prioritere konkurrenceevne
- Databehandlere (spiller 2) har to strategier:
    - Strategi A: Tilbyde strenge databeskyttelsesstandarder
    - Strategi B: Tilbyde fleksible databeskyttelsesstandarder
- EU-kommissionen (spiller 3) har to strategier:
    - Strategi A: Implementere strenge reguleringer
    - Strategi B: Implementere lempelige reguleringer

Spillet opstilles i en matrice:

Spiller 3 spiller strategi A		Spiller 2	
		A	B
Spiller 1	A	(6, 5, 7)	(3, 7, 3)
	B	(8, 3, 3)	(4, 4, 5)

Spiller 3 spiller strategi B		Spiller 2	
		A	B
Spiller 1	A	(5, 5, 2)	(1, 4, 3)
	B	(8, 3, 6)	(4, 4, 2)

Payoffs

3.3.1.2 Nash-ligevægt

For at finde Nash-ligevægten i dette spil skal vi identificere de situationer, hvor ingen af spillerne har incitament til at skifte strategi, givet de andre spilleres valg. Spillet løses med Elimination of Strictly Dominated Strategies (IESDS).

Spiller 1 har en strengt dominerende strategi ved at vælge B og vælger derfor aldrig A.

Givet, at spiller 1 altid spiller B, har spiller 2 en strengt dominerende strategi ved at spille B.

Givet at spiller 1 og spiller 2 begge spiller B uanset hvad, er best response hos spiller 3, at spille strategi A.

Nash ligevægten (i pure strategies) er derfor: (B, B, A) med payoffs (4, 4, 5).

I Nash-ligevægten (B, B, A), hvor spiller 1 vælger strategi B (prioritere konkurrenceevne), spiller 2 vælger strategi B (tilbyde fleksible databeskyttelsesstandarder) og spiller 3 vælger strategi A (implementere strenge reguleringer), er payoffs for spillerne som følger:

Spiller 1 (EU-virksomheder): Payoff er 4. Dette repræsenterer, at EU-virksomhederne opnår en vis konkurrencefordel ved at prioritere konkurrenceevne, men samtidig bliver de nødt til at navigere i et miljø med strengere reguleringer, hvilket kan begrænse gevinsten.

Spiller 2 (databehandlere): Payoff er 4. Databehandlerne tilbyder fleksible databeskyttelsesstandarder, hvilket gør dem mere attraktive for virksomheder. Dog er de nødt til at tilpasse sig de strengere reguleringer implementeret af spiller 3, hvilket kan medføre ekstra omkostninger og begrænse deres samlede gevinst.

Spiller 3 (EU-kommissionen): Payoff er 5. EU-kommissionen implementerer strenge reguleringer, hvilket sikrer et højt niveau af databeskyttelse for borgere og virksomheder. Selvom dette kan påvirke konkurrenceevnen for nogle virksomheder, betragtes det som en

værdig trade-off for at beskytte borgernes data og opretholde tilliden til EU's digitale økosystem.
Nash-ligevægt balancerer hensynet til konkurrenceevne og databeskyttelse, og alle spillerne får en payoff, der afspejler deres prioriteringer og de kompromiser, de måtte indgå.

I denne situation er alle spillerne tilfredse med deres valg og har ikke incitament til at ændre deres strategi. EU-virksomhederne opnår en payoff på 4, hvilket betyder, at de har et fornuftigt niveau af succes, mens de balancerer databeskyttelse og konkurrenceevne. Databehandlere opnår også en payoff på 4, hvilket indikerer, at de er i stand til at tilbyde tjenester, der imødekommer virksomhedernes behov, samtidig med at de overholder reguleringerne. EU-Kommissionen får en payoff på 5, hvilket betyder, at de er i stand til at opretholde en høj grad af databeskyttelse og forbrugerrettigheder, selvom virksomheder og databehandlere prioriterer fleksibilitet og konkurrenceevne.

For at illustrere hvordan EU-virksomheder og databehandlere indgår aftaler, kan der opstilles et Bayesian-spil med asymmetrisk information. For at illustrere hvordan aktørerne agerer, antages det, at virksomheder lægger større vægt på konkurrenceevne end på databeskyttelse, mens databehandlere har intentioner om at have en høj databeskyttelse eller at bluffe om deres databeskyttelsesniveau. Udfaldet af spillet, kombineret med antagelserne, kan give en indikation på, hvad EU-kommissionen kan forvente af en henholdsvis streng eller lempelig lovgivning.

3.3.2 Bayesian spil

I det Bayesianske spil undersøges, hvordan EU-virksomheder indgår aftaler med databehandlere, samtidig med at de tager hensyn til konkurrenceevne og databeskyttelse. Der opstilles et simultant Bayesian spil med principal-agent-perspektiv[27] for at modellere beslutningstagning, og der inkluderes asymmetrisk information, risiko og omkostningerne ved at bluffe om databeskyttelsesstandarder.

I et bayesianske spil med principal-agent-perspektiv er EU-virksomheder og databehandlere de to aktører, der træffer beslutninger på usikkert grundlag og asymmetrisk information. EU-virksomhederne fungerer som principaler og skal vælge mellem to strategier, hvor strategi A er fokus på databeskyttelse, og strategi B er fokus på konkurrenceevne. Databehandlerne, som fungerer som agenter, kan være af to typer; type 1, som har høje databeskyttelsesstandarder, og type 2, som har lave databeskyttelsesstandarder.

Asymmetrisk information opstår, når EU-virksomhederne ikke kender databehandlernes præcise type. Dette fører til, at virksomhederne skal træffe beslutninger uden fuldstændig information om databehandlernes standarder og præferencer. EU-virksomhederne skal således balancere deres præferencer for databeskyttelse og konkurrenceevne med de mulige omkostninger og risici forbundet med at arbejde med databehandlere, som ikke opfylder deres forventninger.

I spillet er principal-agent-forholdet mellem EU-virksomheder og databehandlere centralt for at forstå, hvordan de interagerer og træffer beslutninger. For eksempel kan EU-virksomhederne vælge at arbejde med databehandlere, der formodes at have høje standarder, men som i virkeligheden har lave standarder - moral hazard[28]. Dette kan resultere i ineffektive udfald,

[27] Hart & Holmström (1987), s. 71-155
[28] Hart & Bengt (1987), s. 75-76

hvor virksomhederne ender med at betale højere omkostninger for databeskyttelse, end de ellers ville have gjort, hvis de havde fuldstændig information om databehandlernes standarder. I det bayesianske spil er den bayesianske Nash-ligevægten det punkt, hvor ingen af aktørerne har en grund til at ændre deres strategi, givet hvad de tror om de andre aktørers strategier. den bayesianske Nash-ligevægten afhænger af aktørernes præferencer, forventninger og omkostninger, og den kan påvirkes af ændringer i lovgivning, markedet og teknologiske fremskridt.

Ved at analysere spillet med principal-agent-perspektiv, fås indsigt i, hvordan EU-virksomheder og databehandlere interagerer i en situation med usikkert grundlag og asymmetrisk information, og hvordan de træffer beslutninger i forhold til databeskyttelse og konkurrenceevne. Denne indsigt kan hjælpe med at identificere mulige ineffektive udfald og potentielle løsninger på udfordringerne forbundet med asymmetrisk information.

Når principal-agent-teorien tages i betragtning, kan det give en forståelse af de mulige incitamenter og adfærdsmønstre hos både EU-virksomheder og databehandlere. For eksempel kan databehandlere have incitament til at fremstå som mere databeskyttende, end de faktisk er, for at tiltrække EU-virksomheder, mens EU-virksomheder kan have incitament til at fokusere på konkurrenceevne på bekostning af databeskyttelse.

Det bayesianske spil med principal-agent-perspektiv bruges til at analysere interaktionen mellem EU-virksomheder og databehandlere i forhold til databeskyttelse og konkurrenceevne. Ved at forstå aktørernes præferencer, forventninger og omkostninger, samt hvordan asymmetrisk information påvirker deres beslutninger, kan der identificeres potentielle udfordringer mellem databeskyttelse og konkurrenceevne.

Spillet består af to aktører: EU-virksomheder (principal) og databehandlere (agent):

Databehandlere er opdelt i to typer:

Type 1, som faktisk har strenge databeskyttelsesstandarder.

Type 2, som bluffer om deres standarder.

Spillet opstilles i en matrice:

Payoff matricen for spillet ser nu sådan ud:

		Databehandlere	
		Type 1 (strenge standarder)	Type 2 (Bluffer om standarder)
EU-virksomhed	Strategi A	(2,3)	(1,4-p*M)
	Strategi B	(4,1)	(3,2-p*M)

Payoffs

3.3.2.1 Strategier:

EU-virksomhederne (principal):

Strategi A: prioriterer databeskyttelse.

Strategi B: prioriterer konkurrenceevne.

Databehandlerne (agent) har to strategier, som varierer afhængigt af deres type (type 1 eller type 2):

Type 1 databehandlere (faktisk strenge standarder):

Strategi A: Markedsføre høje standarder og forsøge at tiltrække virksomheder, der prioriterer databeskyttelse.

Strategi B: Markedsføre lempelige standarder og forsøge at tiltrække virksomheder, der prioriterer konkurrenceevne.

Type 2 databehandlere (bluffer om standarder):

Strategi A: Bluffe ved at markedsføre høje standarder og forsøge at tiltrække virksomheder, der prioriterer databeskyttelse, selvom de i virkeligheden har lempelige standarder.

Strategi B: Markedsføre lempelige standarder og forsøge at tiltrække virksomheder, der prioriterer konkurrenceevne.

For type 2 databehandlere (bluffer om standarder) skal vi sammenligne udbetalingerne under Strategi A og Strategi B, idet vi tager højde for sandsynligheden for at blive opdaget og de negative konsekvenser:

Udbetaling ved at spille Strategi A: $4 - p \cdot M$

Udbetaling ved at spille Strategi B: 2

Type 2 databehandlere vil vælge Strategi A (markedsføre høje standarder), hvis:

$4 - p \cdot M > 2$ Det vil sige hvis: $p \cdot M < 2$

Så længe sandsynligheden for at blive opdaget ganget med omkostningerne ved at blive fanget i at bluffe $p \cdot M$ er mindre end 2, vil type 2 databehandlerne fortsætte med at vælge Strategi A og markedsføre høje standarder, selvom de faktisk har lempelige standarder.

Hvis $p \cdot M > 2$, vil type 2 databehandlerne vælge Strategi B (markedsføre lempelige standarder), da risikoen og omkostningerne ved at blive opdaget i at bluffe er for høje.

For at $p \cdot M > 2$, skal sandsynligheden for at blive opdaget p ganget med den negative udbetaling ved at blive fanget i at bluffe *M* være større end 2.

Hvis værdierne for sandsynligheden og den negative udbetaling ved at blive fanget i at bluffe antages til at være følgende:

Sandsynligheden for at blive opdaget antages at være 50%, hvilket giver:

$p = 0.5$

Den negative udbetaling ved at blive fanget i at bluffe antages at være 5, hvilket giver:

$M = 5$

$p \cdot M = 0.5 \cdot 5 = 2.5$

Derfor vil databehandlerne vælge strategi B, da risikoen og omkostningerne ved at blive opdaget i at bluffe er for høje.

For at finde den bayesianske ligevægt i spillet, skal sandsynlighedsfordelingen overvejes overfor databehandlerne og de forventede udbetalinger for hver strategi hos EU-virksomhederne. Det antages, at der er en sandsynlighed q for, at en databehandler er af type 1 (faktisk strenge standarder) og en sandsynlighed $1 - q$ for, at en databehandler er af type 2 (bluffer om standarder). Derefter beregnes EU-virksomhedernes forventede udbetaling for hver strategi, idet højde tages for sandsynlighedsfordelingen over databehandlerne.

Forventede udbetalinger for EU-virksomhederne:

Strategi A forventet udbetaling:

$E(U_A) = q \cdot Udbetaling\ fra\ type\ 1 + (1 - q) \cdot Udbetalingfra\ type\ 2 = q \cdot 2 + (1 - q) \cdot 1$

Strategi B forventet udbetaling:

$$E(U_B) = q \cdot Udbetaling\ fra\ type\ 1 + (1-q) \cdot Udbetalingfra\ type\ 2 = q \cdot 4 + 1(1-q) \cdot 3$$

For at finde den bayesianske ligevægt skal EU-virksomhederne vælge den strategi, der maksimerer deres forventede udbetaling, givet deres tro om sandsynlighedsfordelingen over databehandlerne. EU-virksomhederne vil vælge Strategi A, hvis:

$$q \cdot 2 + (1-q) \cdot 1 > q \cdot 4 + (1-q) \cdot 3$$

Efter at have løst denne ulighed, får vi:

$$q > 0.5$$

Dette betyder, at EU-virksomhederne vil vælge Strategi A (prioritere databeskyttelse) i den bayesianske ligevægt, hvis de mener, at sandsynligheden for at møde en databehandler med faktisk strenge standarder (type 1) er større end 0.5. Ellers vil de vælge Strategi B (prioritere konkurrenceevne).

Under antagelsen af, at $p \cdot M > 2$, vil type 2 databehandlerne vælge Strategi B (markedsføre lempelige standarder), mens type 1 databehandlerne fortsat vælger Strategi A (markedsføre høje standarder).

Derfor afhænger den bayesianske ligevægt i spillet af EU-virksomhedernes tro q om sandsynlighedsfordelingen over databehandlerne og deres valg af strategi baseret på tro.

Det antages, at en EU-virksomhed tror, at der er en 60% chance for, at en databehandler er en type 1 databehandler, og dermed en 40% chance for, at databehandleren er en type 2 databehandler (dem der bluffer om standarder), vil $q = 0.6$.

For at finde den bayesianske ligevægt i dette spil når $q = 0.6$, skal der først findes de forventede udbetalinger for EU-virksomhederne, når de vælger hver af deres strategier (Strategi A og Strategi B). Vi skal også tage højde for databehandlernes strategier og udbetalinger.

Forventet udbetaling ved at vælge Strategi A (prioritere databeskyttelse):

$E(U_A) = q \cdot U_{A1} + (1 - q) \cdot U_{A2}$

$E(U_A) = 0.6 \cdot 2 + 0.4 \cdot 1$

$E(U_A) = 1.2 + 0.4$

$E(U_A) = 1.6$

Forventet udbetaling ved at vælge Strategi B (prioritere konkurrenceevne):

$E(U_B) = q \cdot U_{B1} + (1 - q) \cdot U_{B2}$

$E(U_B) = 0.6 \cdot 4 + 0.4 \cdot 3$

$E(U_B) = 2.4 + 1.2$

$E(U_B) = 3.6$

Da $E(U_B) > E(U_A)$, vil EU-virksomhederne fortsat vælge Strategi B, hvilket prioriterer konkurrenceevnen.

For at finde den bayesianske ligevægt skal der tages hensyn til databehandlernes strategivalg og q (tro). I dette tilfælde er der tidligere konkluderet, at type 1 databehandlere vil vælge Strategi A (markedsføre høje standarder), mens type 2 databehandlere vil vælge Strategi B (markedsføre lempelige standarder) under de givne betingelser.

Den Bayesianske ligevægt i dette spil under de antagede q (tro) er:

EU-virksomheder vælger Strategi B (prioritere konkurrenceevne)

Type 1 databehandlere vælger Strategi A (markedsføre høje standarder)

Type 2 databehandlere vælger Strategi B (markedsføre lempelige standarder)

Selv med q (tro) taget i betragtning, vil EU-virksomhederne stadig vælge Strategi B, og udfaldet af spillet ændrer sig ikke i denne situation.

Spillet viser hvordan EU-virksomheder og databehandlere træffer beslutninger i forhold til databeskyttelse og konkurrenceevne. I dette specifikke spil er det fundet i den bayesianske ligevægt, at EU-virksomheder prioriterer konkurrenceevne over databeskyttelse, mens type 1 databehandlere (dem med faktisk strenge databeskyttelsesstandarder) markedsfører deres høje standarder. Type 2 databehandlere (dem der bluffer om deres standarder) markedsfører lempelige standarder, da omkostningerne og risikoen ved at blive opdaget i at bluffe er for høj. Spillet viser, at EU-virksomheder i nogle tilfælde kan prioritere konkurrenceevne over databeskyttelse, hvilket kan føre til en større sandsynlighed for at vælge databehandlere med lempeligere databeskyttelsesstandarder. Dette kan skyldes, at EU-virksomhederne har en tro på, at strenge databeskyttelsesstandarder er mindre almindelige, eller at de vurderer, at konkurrencefordele ved at vælge en billigere databehandler opvejer risikoen for at overtræde databeskyttelsesreglerne.

Spillet viser også, at strenge konsekvenser for databehandlere, der bluffer om deres standarder, kan ændre deres adfærd og dermed reducere sandsynligheden for at de bluffer om deres standarder. Hvis omkostningerne og risikoen ved at blive opdaget i at bluffe er høj, vil databehandlere, der bluffer om deres standarder, være mere tilbøjelige til at markedsføre

lempelige standarder for at undgå negative konsekvenser. Dette kan gøre det lettere for EU-virksomheder at skelne mellem databehandlere med strenge og lempelige standarder og dermed potentielt forbedre deres valg i forhold til databeskyttelse.

Derudover kan ændringer i EU-virksomhedernes præferencer og deres tro på sandsynligheden for strenge databeskyttelsesstandarder påvirke deres valg og udfaldet af spillet. Hvis EU-virksomhederne vægter databeskyttelse højere, eller hvis de tror, at det er mere sandsynligt, at databehandlere har strenge standarder, kan de vælge at prioritere databeskyttelse over konkurrenceevne.

Hvis variablerne i spillet ændrer sig, kan udfaldet også ændre sig. For eksempel, hvis sandsynligheden for at blive opdaget under tilsyn ændrer sig, kan dette påvirke type 2 databehandleres valg af strategi. Hvis omkostningerne og risikoen ved at blive opdaget i at bluffe bliver mindre, vil type 2 databehandlerne vælge at bluffe og markedsføre høje standarder, hvilket gør det sværere for EU-virksomhederne at skelne mellem type 1 og type 2 databehandlere.

Endvidere kan EU-virksomhedernes præferencer ændrer sig, og hvis de vægter databeskyttelse højere, kan de vælge at prioritere databeskyttelse over konkurrenceevne. Dette vil ændre udfaldet af spillet og sandsynligvis føre til øget efterspørgsel efter type 1 databehandlere.

Endelig kan ændringer i q-værdierne, som repræsenterer EU-virksomhedernes tro på, at en databehandler, har strenge standarder, også påvirke deres forventede udbetalinger og potentielt deres valg af strategi. Hvis EU-virksomheder tror, at det er større sandsynlighed for, at databehandlere har strenge standarder, kan de vælge at prioritere databeskyttelse.

Ved at ændre variabler og sandsynligheder i spillet, kan man analysere, hvordan forskellige faktorer påvirker beslutningstagningen for både EU-virksomheder og databehandlere, og

hvordan det kan påvirke udfaldet i forhold til databeskyttelse og konkurrenceevne. Dette hjælper med at få en bedre forståelse af, hvordan politikker og ændringer i markedet kan påvirke adfærden hos virksomheder og databehandlere i forhold til databeskyttelse.

3.4 Bøder

Hvis der holdes fast i antagelserne om, at virksomheder prioriterer konkurrenceevne fremfor databeskyttelse, kan EU-kommissionen ved at indføre højere bøder påvirke EU-virksomhederne i retning af at prioritere databeskyttelse højere. Størrelserne på bøderne, som virksomheder kan få i dag for ikke at overholde GDPR reguleres i artikel 83.

Artikel 83, stk. 1 fastsætter, at bøder skal stå i rimelige forhold til overtrædelsen og have en afskrækkende virkning. Bøderne er delt op i to kategorier.
For mindre alvorlige overtrædelser kan en bøde på op til 10 millioner euro eller 2% af den globale årlige omsætning for det foregående regnskabsår pålægges - alt efter hvilket beløb, der er højere. Disse overtrædelser kan f.eks. være manglende overholdelse af kravene om oplysningspligt, manglende samarbejde med tilsynsmyndighederne eller manglende gennemførelse af en konsekvensanalyse.
For mere alvorlige overtrædelser kan en bøde på op til 20 millioner euro eller 4% af den globale årlige omsætning for det foregående regnskabsår pålægges - alt efter hvilket beløb der er højere. Disse overtrædelser kan f.eks. omfatte ulovlig behandling af personoplysninger, manglende overholdelse af den registreredes rettigheder, eller overførsel af persondata til tredjelande eller internationale organisationer uden passende beskyttelsesforanstaltninger.

3.5 Økonomisk konsekvens af lovovertrædelse

Ud fra modellen fra *The Economic Theory of Public Enforcement of Law*[29] kan der undersøges nærmere om virksomheder kan have incitament til at begå en bevidst lovovertrædelse. Princippet i modellen er, at en virksomhed begår en lovovertrædelse, hvis det i sidste ende er fordelagtigt.

Der opstilles et hypotetisk eksempel med Meta som virksomhed.

Det antages, at Meta med en lovovertrædelse kan opnå en fordelagtig værdi af €100 millioner, inklusiv eventuelle transaktionsomkostninger.

Det antages, at Meta med lovovertrædelsen kan opnå en besparelse i form af udgifter til compliance/legal på €10 millioner pr. år.

Det antages, at sandsynligheden for at blive afsløret er rimelig stor, da Meta's handlinger generelt er forbundet med stor interesse, og at Meta i det hypotetiske eksempel opererer i EU. Sandsynligheden vurderes til at være 25%.

Omkostninger er bødestørrelse + (gennemsnits erstatning x antal af skadelidte) + juridiske omkostninger. I eksemplet benyttes erstatning ikke. Ifølge GDPR artikel 83, udgør bøden en størrelse på 4% af det sidste års omsætning. Der tages udgangspunkt i 2020, hvor Meta omsatte for €75,649 milliarder[30], hvorfor en bødestørrelse ville være på €3 milliarder.

Det antages, at de juridiske omkostninger forbundet med en eventuel sag er €5 millioner.

Omkostninger forbundet med dårlig omtale antages at være €15 millioner.

[29] Polinsky & Shavell (1999)

[30] I 2020 hed Meta stadigvæk Facebook, 2020 omsætningen ses på s. 50 her: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001326801/000132680121000014/fb-20201231.htm#i5d2898d61ccf450cbccb20a5c73005f3_91

Modellen kan således beregnes:

$$100.000.000 + 10.000.000 > 0.25 \cdot (3.000.000.000 + 5.000.000 + 15.000.000) + 10.000.000 =$$

$$110.000.000 > 738.000.000$$

Ud fra beregningen af det hypotetiske eksempel er en lovovertrædende handling langt fra fordelagtig for Meta. Beregningen giver et klart indtryk af, at det er utænkeligt, at en virksomhed ville foretage en bevidst lovovertrædelse ud fra de antagelser og faktorer, der spiller ind i eksemplet. Men dette afspejler ikke virkeligheden, fordi der er eksempler på, at virksomheder overtræder GDPR. Senere i analysen kigges der på et eksempel fra Meta, der viser dette.

Derfor kan det ikke udelukkes, at mindre virksomheder også kan drage fordel af at overtræde GDPR. Et eksempel kunne være danske SMV-virksomheder, som under alle omstændigheder er EU-virksomheder. Der kan endvidere tilføjes til eksemplet, at virksomheden er en fintech virksomhed. Fintech virksomheder kan ofte kendetegnes ved, at de outsourcer mange opgaver, og i den forbindelse har mange databehandlere og underdatabehandlere. Til forskel fra Meta, Google og Amazon, tiltrækker en mindre fintech SMV virksomhed ikke lige så stor opmærksomhed og lige så mange overskrifter, hvorfor chancen for at blive opdaget er mindre for dem. Endvidere kan besparelser på eksempelvis compliance området have større betydning for den økonomiske situation i en lille virksomhed sammenlignet med de tre førnævnte.

Der kan opstilles et eksempel med en hypotetisk dansk fintech SMV-virksomhed. Virksomheden overvejer i forbindelse med udvidelse til et andet EU-land, om de skal overtræde GDPR eller ikke.

Værdien af lovovertrædelsen antages at være 2.500.000 DKK. For at operationen skal lykkes, er der behov for en konsulent, der har brancheerfaring i og bekendtskab til begge lande.

Konsulenten tager honorar på 2.500kr i timen, og der er behov for 15 konsulenttimer, som giver en omkostning på $2500 \cdot 15 = 37.500$ DKK.
Virksomheden vurderer, at de kan opnå en besparelse på compliance området på 200.000 DKK.

Virksomheden er relativt usynlig i mediernes og offentlighedens øjne. Endvidere vurderer virksomheden, at overtrædelsen er relativt svær at opdage. Virksomheden har et relativt lavt antal registrerede, som ligger under 50.000. Men virksomheden er ikke helt klar over den reelle chance for at blive opdaget, og de påregner derfor honorar-omkostninger til en konsulent for udregning af det præcise tal. Konsulenten finder frem til, at chancen for at blive opdaget er 4%. Omkostninger i form af honorar til konsulenten er igen $2500 \cdot 15 = 37.500$ DKK.

I eksemplet tages der udgangspunkt i en bøde på de 4% af årsomsætningen.

Virksomheden omsatte sidste år for 7 millioner DKK, hvorfor bøden ville være $0.04 \cdot 7.000.000 = 280.000$

Modellen kan således beregnes: $2.500.000 + 200.000 > (0.04 * 280.000) + 200.000 + (2 \cdot 37.500) =$
$2.700.000 > 286.200$

Ud fra eksemplet og de antagelser ses altså, at det for en mindre virksomhed kan være fordelagtigt at lave en bevidst overtrædelse af GDPR.

3.6 Bøde til Meta

En afgørelse fra det irske datatilsyn resulterede i en bøde på mellem 28 og 36 millioner euro til Meta. Afgørelsen er sidenhen blevet underkendt af EDPB (European Data Protection Board) med en bindende afgørelse[31]. Den bindende afgørelse resulterede i, at det irske datatilsyn traf en ny afgørelse, hvor den samlede bøde til Meta endte med at blive 390 millioner euro. Sagen omhandlede Meta's forsøg på at undgå samtykkereglerne i GDPR art. 6. Der bliver i denne analyse kigget nærmere på de økonomiske aspekter af afgørelsen. Den juridiske del af afgørelsen bliver ikke behandlet i denne analyse.

Klagerne blev indgivet i maj 2018, hvilket betyder, at afgørelsen først er truffet 4,5 år efter indgivelsen. Hos NOYB – European Center for Digital Rights, som er en non-profit-organisation placeret i Wien, argumenterer man for, at bøden til Meta i virkeligheden er alt for lille[32].

På overfladen lyder en bøde på €390 millioner som en meget stor bøde. Men *NOYB* omtaler bøden som en gave eller besparelse for Meta på €3,97 milliarder. De argumenterer som følgende:

"*Max Schrems: "The maximum cap of 4% of global turnover was easily overrun by the revenue from unlawful processing in the past 4.5 years. It is easy to show from public information that the revenue factor alone would have required imposing the maximum fine."*

Public information and a spreadsheet. Meta, being a publicly listed company, publishes most of the relevant financial data. According to reports by Meta itself, it made € 84,7 billion (US$ 91,59 billion) from advertising on the European continent between Q3 2018 and Q3 2022. Adjusted for user numbers in the EU only, this amounted to roughly € 72,5 billion (US$ 78,4 billion). While "behavioural advertisement" does not make up all the revenue of Meta's overall advertising, it is clear that in any realistic scenario, the revenue from "behavioural advertisement" in the EU overshot the maximum fine of € 4.36 billion.

[31] https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf besøgt d. 14.05.2023

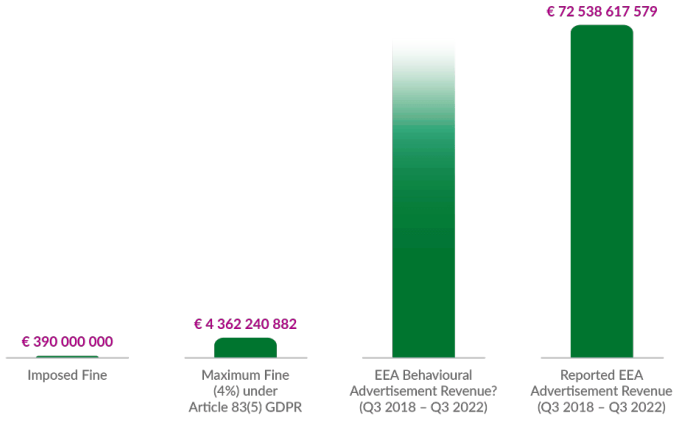
[32] https://noyb.eu/en/irish-data-protection-authority-gives-eu-397-billion-present-meta besøgt d. 14.05.2023

Max Schrems: "By not even checking publicly available information, the DPC gifted € 3.97 billion to Meta. It took us an hour and a spreadsheet to make the calculation. I am sure the Irish taxpayers would not mind having that extra cash, if a DPC employee would have just opened a search engine and done some research."

Meta still makes up to € 68,17 billion from violating the GDPR. Even if the maximum fine of 4% would have been imposed, Meta would still have made up to € 68 billion from the violation of the GDPR since 2018, if it is assumed that basically every advertisement on Meta is currently "behavioural advertisement". This is mainly because the procedure was massively delayed by the DPC and took 4.5 years, while the maximum fine may only be calculated based on a single year. Meta's violation also likely overshot the 4% in each year, meaning that the revenue far exceeded the maximum fine per year.

Max Schrems: "Bottom line, it absolutely paid off for Meta to violate the GDPR and the Irish DPC made it even more profitable for Meta to violate EU law."[33]

En illustration fra NOYB, illustrerer forholdene imellem bødestørrelsen og deres argumenter:



Argumenterne fremsat af NOYB står i kontrast til de tidligere teoretiske beregninger vedrørende store virksomheder og overtrædelser af GDPR. Beregningerne antydede, at det ikke ville være økonomisk fordelagtigt for store virksomheder, såsom Meta, at overtræde GDPR-

[33] https://noyb.eu/en/irish-data-protection-authority-gives-eu-397-billion-present-meta besøgt d. 14.05.2023

reglerne. Imidlertid peger NOYB's udregninger på, at det under visse omstændigheder faktisk kan være økonomisk fordelagtigt for virksomheder at overtræde GDPR.

Udover selve bødebeløbet er der flere aspekter, der skal tages i betragtning, når man vurderer omkostningerne og gevinsterne ved at overtræde GDPR. For det første har Meta formået at udsætte sagen i 4,5 år, hvilket har givet dem mulighed for at fortsætte med at generere indtægter fra deres overtrædelser af GDPR. NOYB påpeger, at det irske datatilsyn muligvis er underlagt påvirkning fra Meta gennem lobbyisme og andre metoder, hvilket kan have bidraget til denne forsinkelse.[34]

For det andet har store selskaber som Meta ressourcer til at opbygge og vedligeholde juridiske afdelinger, der arbejder målrettet på at opnå juridiske fordele for virksomheden. Selvom det kan være en betydelig omkostning at have en sådan juridisk afdeling, er det uklart, om disse omkostninger nogensinde vil overstige den økonomiske gevinst, som NOYB hævder, at Meta har opnået ved at overtræde GDPR i denne sag.

Der er en række faktorer, der indikerer, at det under visse betingelser kan være økonomisk fordelagtigt for store virksomheder at overtræde GDPR. NOYB's argumenter og beregninger udfordrer den teoretiske antagelse om, at overtrædelse af GDPR altid ville medføre en økonomisk ulempe for virksomhederne. Det rejser så igen spørgsmålet om, hvorvidt det nuværende system for håndhævelse af GDPR er tilstrækkeligt effektivt og retfærdigt, og om der er behov for yderligere reformer for at sikre, at virksomheder overholder lovgivningen.

[34] https://noyb.eu/en/second-noyb-advent-reading-facebookdpc-documents besøgt d. 14.05.2023

3.7 Kritik af analyse

I den økonomiske analyse er der benyttet spilteori og en teoretisk økonomisk model fra *The Economic Theory of Public Enforcement of Law*. Det er vigtigt at understrege, at disse teorier reducerer komplekse, virkelige problemstillinger til enkelte økonomiske variabler. En simplificering af virkeligheden medfører et tilsvarende usikkert resultat.

Spilteori kan bidrage til en forståelse af en kompleks situation og give indsigt i hvordan spillerne kan træffe beslutninger i en given situation. Men spilteori kan ikke medtage al information om situationen og kan heller ikke medtage menneskelig adfærd, i form af uforudsigelighed, adfærd og kompleksitet. Generelt antager spilteori ofte, at spillerne er rationelle og har fuldstændig information. Rationaliteten er antaget i analysen, men der er benyttet et Bayesiansk spil for at inkorporere asymmetrisk information/ufuldstændig information. Men i virkeligheden har mennesker og virksomheder ofte begrænset information og bliver påvirket af følelser, fornemmelser og andre faktorer, som ikke er rationelle.

En simplificering af virkeligheden gør sig også gældende i *The Economic Theory of Public Enforcement of Law*. Teorien fastsætter, at lovovertræderen handler rationelt, og tager dermed ikke i menneskers irrationelle adfærd og følelser i betragtning. Teorien fokuserer primært på offentlig retshåndhævelse og undlader derfor at betragte den rolle, som privat retshåndhævelse og selvregulering kan spille. I analysen er der et eksempel om privat retshåndhævelse - NOYB - som har spillet en stor rolle i de GDPR bøder, der er udstedt til blandt andet Meta i Europa.

3.8 Økonomisk delkonklusion

Den økonomiske analyse viser, på baggrund af de teoretiske antagelser, at virksomheder træffer beslutninger ud fra et profitoptimerende perspektiv, hvilket kan føre til overtrædelse af GDPR,

hvis det giver virksomhederne en økonomisk fordel. Bødestørrelserne spiller en rolle i beslutningsprocessen, men har ikke altid en afskrækkende effekt efter hensigten, især fordi store virksomheder har ressourcerne til at bære sådanne omkostninger. Dette, sammen med eksempler fra virkeligheden, indikerer, at balancen mellem databeskyttelse og konkurrenceevne påvirker beslutningstagningen for virksomheder og databehandlere, og at de nuværende bødestørrelser ikke nødvendigvis er tilstrækkelige til at sikre overholdelse af GDPR. For at skabe en bedre balance mellem databeskyttelse og konkurrenceevne bør lovgivningen og håndhævelsen af GDPR måske justeres, således at bøder og andre sanktioner får en større afskrækkende effekt, særligt for store virksomheder. Analysen har visse begrænsninger, som følge af dens simplificering af komplekse problemstillinger gennem brug af spilteori. Blandt disse begrænsninger er antagelsen om rationel adfærd og udeladelse af menneskelig adfærd, såsom kompleksitet og uforudsigelighed. Derudover fokuserer analysen primært på offentlig retshåndhævelse og undlader at betragte den rolle, som privat retshåndhævelse og selvregulering kan spille.

Kapitel 4 - Integreret analyse og delkonklusion

4.1 Indledning

Beskyttelse af persondata og EU's konkurrenceevne i det internationale marked er to vigtige mål for EU. I det internationale marked er konkurrencen fra andre store økonomier, deriblandt USA og Kina, stærk, hvorfor emnet er noget som EU bør forholde sig til. På den ene side skal EU borgernes persondata sikres. Persondatabeskyttelse er en helt central del af EU lovgivning,

der fremgår i TEUF, art. 16, stk. 1. Derfor har EU et stort fokus på persondatabeskyttelse. Databeskyttelse er en central del i, at EU borgeres data ikke bliver misbrugt.

På den anden side skal EU-konkurrencedygtighed i det internationale marked sikres. Derfor er det vigtigt, at de regulatoriske foranstaltninger i forbindelse med sikring af persondata ikke bliver for stramme og svækker EU's konkurrencedygtighed på det internationale marked.

Den integrerede analyse vil undersøge balancen mellem databeskyttelse og konkurrenceevne, herunder fordele og udfordringer ved de nuværende regler og praksis. Analysen præsenterer mulige løsninger og kompromiser for at finde en passende balance mellem beskyttelse af persondata og EU's konkurrencedygtighed på det internationale marked. Til sidst laves der en efficiensanalyse, for at se om Kaldor/Hicks princippet kan blive opfyldt.

4.2 GDPR's præambel

I GDPR's præambel nævnes databeskyttelse og konkurrenceevne. Præambel nr. 9 adresserer manglerne i databeskyttelsesdirektivet fra 1995 og siger følgende:

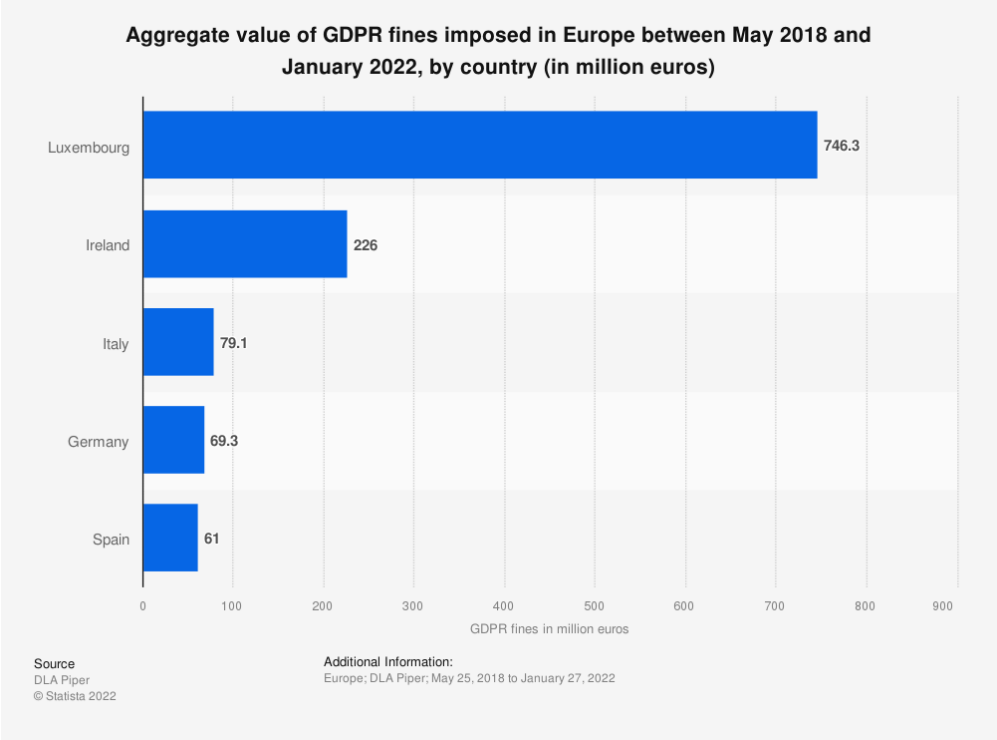
"*Forskelle i niveauet for beskyttelsen af fysiske personers rettigheder og frihedsrettigheder, navnlig retten til beskyttelse af personoplysninger, i forbindelse med behandling af personoplysninger i medlemsstaterne, kan forhindre fri udveksling af personoplysninger i Unionen. Disse forskelle kan derfor udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på EU-plan, virke konkurrenceforvridende og hindre myndighederne i at varetage de opgaver, de er pålagt i medfør af EU-retten. En sådan forskel i beskyttelsesniveauet skyldes forskelle i gennemførelsen og anvendelsen af direktiv 95/46/EF.*"

Endvidere siger præambel nr. 10, at disse hindringer bør fjernes for at sikre et ensartet og højt niveau for beskyttelse af fysiske personer. Præambel 13 nævner et effektivt samarbejde mellem tilsynsmyndighederne i medlemsstaterne. Det viser, at der har været klare hensigter med GDPR om, at både databeskyttelse og konkurrenceevne skal spille en rolle i udmøntningen af lovgivningen. Men selvom hensigten har været der, er det ikke altid, at virkeligheden udformes i overensstemmelse med de hensigter man har haft. Derfor kigges der på de nuværende mangler, som gør sig gældende på området i dag.

4.3 Nuværende mangler

Den akutte mangel på et rammeværk eller en aftale mellem EU og USA angående databeskyttelse er en vigtig problemstilling, der kræver EU-Kommissionens opmærksomhed. Et sådant rammeværk ville kunne styrke samarbejdet mellem de to økonomiske magter og sikre bedre beskyttelse af persondata på tværs af grænser. Men som nævnt i analysen, er der også nogle underliggende udfordringer med GDPR, som skal adresseres for at sikre en mere effektiv databeskyttelsespolitik i EU.

En af disse udfordringer er spørgsmålet om ensartethed i håndhævelsen af GDPR inden for EU. Når man ser på den økonomiske analyse og statistikkerne over de største bøder, kan man konkludere, at der er en vis grad af variation i håndhævelsen af GDPR blandt medlemslandene. Luxembourg og Irland skiller sig ud som de lande, hvor de største bøder udstedes, hvilket kan indikere en mangel på EU-konformitet. Det kan ses på statistikker, der viser, at der særligt i Irland og Luxembourg udstedes store bøder.



En mulig forklaring på dette fænomen kan være de lempelige selskabsskatter og pro-business politikker i disse lande, som tiltrækker store teknologivirksomheder, som vil åbne afdelinger inden for EU. Dette fører til, at disse landes datatilsyn har et større ansvar for at håndhæve GDPR over for disse virksomheder, og dermed udstede større bøder ved overtrædelser.

På den anden side kan denne koncentration af store GDPR-bøder i Luxembourg og Irland også tyde på, at nogle medlemslande er mere tilbøjelige til at indgå i et tættere samarbejde med tech-giganterne. Eksempelvis hævder NOYB i en artikel[35], at der har foregået lobbyisme fra Facebooks side. Artiklen fortæller, at dokumenter, som de har fået indsigt i, viser, at der er blevet afholdt 10 møder mellem Facebook og det irske datatilsyn. Endvidere viser dokumenterne, at det irske datatilsyn har forsøgt at påvirke EDPB til at lave et "bypass" i sine retningslinjer. Forsøget blev mødt med hård kritik fra EDPB.

[35] https://noyb.eu/en/second-noyb-advent-reading-facebookdpc-documents besøgt d. 14.05.2023

Dette kan potentielt føre til en skævvridning af konkurrencen og underminere EU's mål om ensartet databeskyttelse. Det er derfor vigtigt, at EU-Kommissionen arbejder på at styrke samarbejdet mellem medlemslandene og fremme ensartet håndhævelse af GDPR, samtidig med at den søger at etablere et rammeværk med USA for at beskytte borgernes persondata på globalt plan.

Noget andet der kan tyde på en mangel, er det irske datatilsyns afgørelse i Meta sagen. NOYB hævder i en artikel[36], at det irske data tilsyn har ignoreret sine beføjelser:

"[...] *the European Data Protection Board (EDPB) ordered the DPC to quantify how much revenue Meta had generated by infringing the GDPR, and to factor that sum into its fine. However, the DPC simply ignored the unlawful revenue made by Meta and claimed that "the Commission is unable to ascertain an estimation of the matters" and that it is therefore "unable to take these matters into account". This is despite having the power to demand such information from Meta under Article 58(1) GDPR.*

Max Schrems, Chair of noyb: "We all know about Meta's enormous revenue. It's astonishing that this was not taken into account by the DPC. The DPC didn't even use its statutory powers to ask Meta for the information.[...]"

Det er bemærkelsesværdigt, at en tilsynsmyndighed ikke benytter sine beføjelser i GDPR art. 58, stk. 1., hvilket kunne tyde på, at der ikke er helt overensstemmelse mellem hvad datatilsynet gør og burde gøre.

[36] https://noyb.eu/en/irish-data-protection-authority-gives-eu-397-billion-present-meta besøgt d. 14.05.2023

4.4 Fordele og ulemper med strengere regler

En måde at reducere GDPR overtrædelser på er at skærpe reguleringen, men deri ligger en risiko for overregulering. En overregulering af persondata kan føre til øgede omkostninger for virksomheder i EU. Dette skyldes, at virksomhederne skal bruge ressourcer på at implementere og overholde de regulatoriske krav, hvilket kan medføre en øget administrativ byrde. Endvidere kan det begrænse en virksomheds evne til at innovere, hvis de bliver nødt til at allokere kapital fra, blandt andet, innovation til compliance.

Overregulering kan medføre, at EU's virksomheder får sværere ved at tiltrække udenlandske investeringer. Investorer kan blive afskrækket af de strenge regler og frygte, at de vil reducere virksomhedernes indtjeningspotentiale og vækstmuligheder. Ydermere kan overregulering af persondata begrænse mulighederne for international dataudveksling og samarbejde mellem virksomheder. Dette kan være særligt problematisk i forhold til virksomheder, der er afhængige af global dataudveksling.

På den anden side er der også potentielle fordele ved at have stramme regulatoriske foranstaltninger på persondataområdet.

Beskyttelse af persondata kan styrke forbrugernes tillid til virksomheder og deres produkter og tjenester. Dette kan resultere i øget efterspørgsel efter produkter og tjenester fra EU-virksomheder.

Stramme regulatoriske foranstaltninger på persondataområdet bidrager til at skabe et mere retfærdigt konkurrencegrundlag mellem virksomheder. Dette skyldes, at virksomheder, der ikke overholder reglerne, kan blive pålagt bøder og sanktioner, hvilket kan afskrække dem fra at benytte sig af ulovlige metoder til at opnå konkurrencefordele.

For det tredje kan beskyttelse af persondata potentielt fungere som en konkurrencefordel for EU-virksomheder på det internationale marked. Høje standarder for databeskyttelse kan differentiere EU-virksomheder fra konkurrenter i andre regioner, hvor persondata måske ikke beskyttes i samme omfang. Dette kan tiltrække kunder, der lægger vægt på beskyttelsen af persondata og være særligt relevant for virksomheder, der opererer i sektorer med høj følsomhed over for databeskyttelse, såsom finansielle tjenester, sundhedssektoren og uddannelsesområdet.

Stramme regulatoriske foranstaltninger på persondataområdet kan potentielt fremme innovation og teknologisk udvikling i EU. Dette skyldes, at virksomhederne kan blive nødt til at finde nye og mere sikre måder at behandle og beskytte persondata på, hvilket igen kan føre til udvikling af nye teknologier og forretningsmodeller. I artiklen *How Data Protection Regulation Affects Startup Innovation* fandt man, at der i to cases var tale om virksomheder, som havde udviklet innovative de-identifikation- og anonymiserings teknologier, som de kunne tilbyde sine kunder[37]. Endvidere konkluderer artiklen, at undersøgelserne viste, at reguleringen ikke havde en overordnet positiv eller negativ effekt; hellere havde reguleringen modstridende effekt:

"[...] *but rather a variety of partly countervailing effects, driven by the way specific stipulations and principles in the regulation interacted with the structural features of particular business models. We identified six concrete firm responses to data protection regulation. Three of these tend to have positive, innovation-stimulating effects: compliance innovation, regulation-exploiting innovation, and "buying European". In contrast, three other responses have more negative, innovation-constraining effects: abandonment, entrepreneurial discouragement, and data minimization. Overall, the regulation clearly stimulated a certain amount of innovation*

[37] How Data Protection Regulation Affects Startup Innovation (2019), s. 1318

and market opportunities, but it also appears to obstruct certain business models and technologies, in ways that policy makers probably did not intend."[38]

Sammenfattende er der både tydelige fordele og ulemper med et eventuelt strategivalg i EU, og det kan i sidste ende vise sig, at en valgt strategi kan påvirke markedet på måder, som eller ikke var en del af hensigten.

4.5 Optimering af nuværende situation

For at optimere håndhævelsen og sikringen af GDPR i EU og minimere forskelle i fortolkning og håndhævelse mellem medlemslandene, kan en række tiltag sættes i værk.

Det Europæiske Databeskyttelsesråd (EDPB) kan fortsætte med at fremme samarbejdet mellem nationale tilsynsmyndigheder og sikre, at de deler viden, erfaringer og bedste praksis. Dette kan bidrage til en mere ensartet og konsistent håndhævelse af GDPR i hele EU.

EDPB kan udarbejde og udstede detaljerede retningslinjer og vejledninger om fortolkning og håndhævelse af GDPR, som alle nationale tilsynsmyndigheder skal følge. Dette vil bidrage til at sikre, at tilsynsmyndighederne i forskellige lande har en fælles forståelse af GDPR's krav og håndhæver dem på en ensartet måde. EDPB har udarbejdet retningslinjer, det tyder på, at der stadigvæk er behov for retningslinjer, som kan assistere de involverede aktører.

For at sikre, at nationale tilsynsmyndigheder formår at håndhæve GDPR effektivt og upartisk, kan deres uafhængighed og ressourcer styrkes. Dette kan omfatte øget finansiering, bedre adgang til ekspertise og teknologi, samt beskyttelse mod politisk indflydelse.

For at øge tilliden til tilsynsmyndighederne og deres beslutninger, kan der lægges større vægt på gennemsigtighed og ansvarlighed. Dette kan omfatte offentliggørelse af

[38] How Data Protection Regulation Affects Startup Innovation (2019), s. 1321

tilsynsmyndighedernes beslutninger, metoder og kriterier for håndhævelse, samt regelmæssige evalueringer og rapportering om deres aktiviteter og resultater.
Udadtil kan EU-Kommissionen også arbejde med at fremme internationalt samarbejde om databeskyttelse, for at fremme en global harmonisering af databeskyttelsesregler, således at der sikres et højt niveau af databeskyttelse i de tilfælde hvor persondata overføres ud af EU.

Endvidere kan der overvejes, om EU-retten bør træffe afgørelser i stedet for tilsynsmyndighederne.
At lade EU-retten træffe afgørelser og udstede bøder i stedet for de nationale myndigheder ville betyde en centralisering af håndhævelsesprocessen og en ændring af den nuværende decentraliserede tilgang. Sådan en tilgang ville have både fordele og ulemper. Den ville også stride imod den nuværende lovgivning, og derfor kræve en lovændring. Men fordelene og ulemperne kan være:

Fordele:
En centraliseret håndhævelse gennem EU-retten kunne føre til mere ensartede og konsistente afgørelser og bøder på tværs af medlemslandene, hvilket kunne reducere forskelle i fortolkning og praksis.

EU-retten kunne være mere uafhængig af nationale politiske interesser og pres, hvilket kunne bidrage til at sikre en upartisk og retfærdig håndhævelse af GDPR.
Endvidere kunne en centralisering være med til at sikre, at virksomheder ikke valgte at oprette filialer i EU-lande hvor de har størst fordele og størst mulighed for at påvirke potentielle afgørelser.

EU-retten kunne få adgang til ressourcer og ekspertise på europæisk niveau og dermed potentielt øge effektiviteten i behandlingen af sager og udstedelse af bøder.

Ulemper:

En centraliseret håndhævelse gennem EU-retten kunne føre til, at beslutningstagere er længere væk fra lokale forhold og det nationale retssystem. Dette kunne gøre det vanskeligere at tage højde for nationale forskelle og tilpasse håndhævelsen til lokale omstændigheder. Det ville også stride imod nærhedsprincippet.

Centraliseringen kan øge bureaukratiet og føre til langsommere beslutningsprocesser, hvilket kan forsinke afgørelser og bøder.

Der kan endvidere opstå en kapacitetsbegrænsning, hvor EU-retten kan blive overbelastet med sager og mangle kapacitet og ressourcer til effektivt at håndtere alle overtrædelser og udstede bøder.

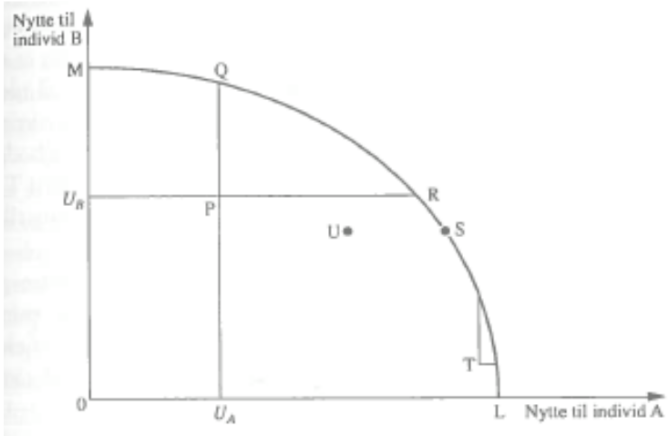
Manglende nærhed til borgere og virksomheder kan reducere nærheden mellem håndhævelsesinstansen og de berørte parter og virksomheder, hvilket kunne gøre det vanskeligere at skabe dialog og samarbejde mellem parterne.

4.6 Efficiensanalyse

Der udføres nu en Kaldor/Hicks efficiensanalyse. Kaldor/Hicks princippet indebærer, at der skal udføres et tiltag, hvis tiltaget udgør en større fordel for en part, end ulempe for en anden part. Princippet bygger ikke på, at der skal ske kompensation til den værre stillede part, hvorfor det kan benyttes i situationer hvor der ikke sker kompensation.[39]

[39] Raaschou-Nielsen & Foss (1997), s. 14

Efficiensanalysen gennemføres med EU-Kommissionen som den ene part og nationale tilsyndmyndigheder som den anden part. Valget er baseret på deres centrale roller i håndhævelsen af GDPR.



Kaldor/Hicks princippet[40]

EU-Kommissionen:

Fordele: Styrkelse af samarbejdet mellem nationale tilsynsmyndigheder og EDPB vil kunne bidrage til en mere ensartet håndhævelse af GDPR i hele EU, hvilket er i tråd med EU-Kommissionens mål. Med internationalt samarbejde om databeskyttelse vil EU-Kommissionen kunne arbejde for en global harmonisering af databeskyttelsesregler, hvilket kan styrke EU's position på det internationale marked. En eventuel centralisering af håndhævelsen og udstedelse af bøder via EU-retten kan skabe mere ensartede og konsistente afgørelser og bøder på tværs af medlemslandene.

Ulemper: Øget finansiering og ressourcer til nationale tilsynsmyndigheder kan medføre øgede omkostninger for EU og/eller medlemslandene. En eventuel centralisering af håndhævelsen og udstedelse af bøder via EU-retten kan øge bureaukratiet og føre til langsommere beslutningsprocesser.

[40] Eide & Stavang (2008), s. 109

Nationale Tilsynsmyndigheder:

Fordele: En styrkelse af uafhængighed og ressourcer vil øge nationale tilsynsmyndigheders evne til effektivt og upartisk at håndhæve GDPR. EDPB's udarbejdelse og udstedelse af detaljerede retningslinjer og vejledning vil hjælpe nationale tilsynsmyndigheder med at håndhæve GDPR mere ensartet og konsistent.

Ulemper: En eventuel centralisering af håndhævelsen og udstedelse af bøder via EU-retten kan føre til, at nationale tilsynsmyndigheder mister en del af deres autonomi og indflydelse i håndhævelsesprocessen.

Efficiensanalysen viser, at de foreslåede tiltag for at optimere håndhævelsen og sikringen af GDPR i EU øger den samlede velfærd for EU-Kommissionen og nationale tilsynsmyndigheder. For EU-Kommissionen vil der være en øget ensartethed i håndhævelsen af GDPR og en styrkelse af EU's internationale position, mens nationale tilsynsmyndigheder vil få styrket deres uafhængighed og ressourcer. Selvom der er nogle potentielle ulemper, deriblandt øgede omkostninger og øget bureaukrati, kan disse ulemper opvejes af de samlede fordele for parterne.

Baseret på denne analyse, opfylder scenariet Kaldor-Hicks efficienskriteriet, da de samlede fordele ved de foreslåede tiltag opvejer de potentielle ulemper for både EU-Kommissionen og nationale tilsynsmyndigheder.

4.7 Kritik af analyse

Der er en række aspekter i analysen, som kan kritiseres. For det første er der antagelsen om, at et øget samarbejde mellem nationale tilsynsmyndigheder og EDPB vil føre til en mere ensartet håndhævelse af GDPR i hele EU. Selvom samarbejde kan bidrage til dette, er det vigtigt at anerkende, at der stadig kan være nationale forskelle og udfordringer, der skal tages højde for. Særligt hvis man tænker på, at der kan være konkurrerende interesser og magtforhold mellem lande, som kan gøre det vanskeligt at nå til enighed om fælles regler og standarder. Analysen lægger vægt på håndhævelsesmekanismer og bøder, men det er vigtigt at huske, at præventive tiltag og samarbejde mellem virksomheder, tilsynsmyndigheder og databeskyttelsesansvarlige også er centrale aspekter af GDPR. At skabe et miljø, hvor parterne arbejder sammen for at sikre overholdelse af GDPR, kan være lige så vigtigt som at håndhæve reglerne og udstede bøder.

I forbindelse med Kaldor/Hicks efficiensanalysen er det vigtigt at bemærke, analysen er en forenkling af virkeligheden, og der kan være yderligere aktører og konsekvenser, som kan tages i betragtning, hvorfor resultatet af analysen hviler på en vis usikkerhed. For eksempel kunne virksomheder opleve øgede omkostninger som følge af skærpede krav og øget kontrol fra tilsynsmyndighederne. Derfor kunne det i den virkelige verden overvejes om virksomhederne ville kunne blive kompenseret af gevinsterne hos EU-Kommissionen og tilsynsmyndighederne.

4.8 Integreret delkonklusion

Det konkluderes, at for at sikre en mere optimal databeskyttelse, skal EU-kommissionen fokusere på en holistisk tilgang, der omfatter både lovgivning, samarbejde og teknologi. Først og fremmest skal der arbejdes på harmonisering af databeskyttelsesregler og styrkelse af

tilsynsmyndigheder for at skabe et ensartet og effektivt regelsæt, der kan dække hele EU. Dette vil gøre det nemmere for både borgere og virksomheder at forstå og overholde reglerne og skabe et højere niveau af beskyttelse.

Internationalt samarbejde er afgørende for at imødegå globale udfordringer og sikre, at persondata beskyttes på tværs af grænser. Dette kan indebære at arbejde sammen om at udvikle fælles standarder og løsninger, som kan styrke databeskyttelsen globalt. Efficiensanalysen viser, at en øget indsats for harmonisering og samarbejde vil føre til en større fordel for EU-kommissionen og nationale tilsynsmyndigheder end ulemperne ved øgede omkostninger og bureaukrati. Det bemærkes, at efficiensanalysen forenkler virkeligheden, hvilket giver en vis usikkerhed i resultatet.

Det skal det påpeges, at nationale forskelle og udfordringer kan gøre det vanskeligt at opnå fuldstændig ensartethed og samarbejde. Præventive tiltag og samarbejde mellem virksomheder, tilsynsmyndigheder og databeskyttelsesansvarlige kan være lige så vigtige som håndhævelse af reglerne og udstedelse af bøder.

Kapitel 5 - Konklusion

Den samlede konklusion viser, at der på nuværende tidspunkt er akutte mangler i databeskyttelse i forbindelse med persondataoverførsler til USA – det vil sige et manglende rammeværk mellem EU og USA. Den juridiske analyse viser, at der i øjeblikket er en vis usikkerhed i beskyttelse af europæiske borgeres persondata, blandt andet fordi tredjelandsoverførsler til USA på nuværende tidspunkt alene baseres på SCC'er, hvor der er eksempler på, at virksomheder ikke anvender gyldige SCC'er.

Endvidere viser den økonomiske analyse, at virksomheder har incitament til at begå overtrædelser af GDPR, da det fører til en sådan økonomisk fordel, at den opvejer eventuelle negative konsekvenser. Dette tyder på, at konkurrenceevnen på nuværende tidspunkt prioriteres på bekostning af databeskyttelse, hvilket ikke er helt optimal, når EU-Kommissionens synsvinkel tages i betragtning. De nuværende bødestørrelserne ser i virkeligheden ikke ud til at have den ønskede virkning, hvorfor de ikke bidrager med en afskrækkende effekt, som blandt andet var hensigten.

Den integrerede analyse viser, at de akutte mangler i den nuværende lovgivning, måske er et resultat af underliggende mangler i håndhævelsen af GDPR. Det kan være, at der er behov for overvejelser i forbindelse med de grundlæggende principper i GDPR. Måske er der behov for en omstrukturering, som kan mitigere de nuværende udfordringer med utilstrækkelig ensartethed og således være med til at man opnår en optimal stilling imellem databeskyttelse og konkurrenceevne.

Kapitel 6 - Litteraturliste

6.1 Bøger

Tvarnø, Christina D. & M. Denta, Sarah, *Få Styr på Metoden*, København: Ex Tuto Publishing A/S, 2018.

Neergaard, Ulla & Nielsen, Ruth, *EU-RET Fri bevægelighed*, 3. udgave/1.plag, København: Karnov Group Denmark A/S, 2018.

Tvarnø, Christina D. & Nielsen, Ruth, *Retskilder og retsteorier*, 5. Reviderede udgave, 1. oplag, København: Jurist- og Økonomforbundets Forlag, 2017.

Raaschou-Nielsen, Agnete & Juul, Nicolai Foss, *Indledning til Rets- og kontraktsøkonomi*, 1. udgave, 1. oplag, København: GadJura, 1997.

Baird, D. G., Gertner, R. H., and R. Picker, *Game theory and the Law,* Cambridge: Harvard University Press, 1994.

Eide, Erling & Stavang, Endre, *Rettsøkonomi*, Oslo: Cappelen akademisk forlag, 2008.

Fudenberg, Drew & Tirole, Jean, *Game Theory*, Cambridge: The MIT Press, 1991

6.2 Artikler

A. Mitchell Polinsky, Steven Shavell (1999), NBER Working Paper Series no.6993, *The Economic Theory of Public Enforcement of Law*.

Hart, Oliver; Holmström, Bengt (1987). *The theory of contracts*. In Bewley, T. (ed.). Advances in Economics and Econometrics. Cambridge University Press. pp. 71–155.

How the Irish DPC tried to lobby Facebook's "GDPR bypass" into European Guidelines. (2021, december). Lokaliseret på: https://noyb.eu/en/second-noyb-advent-reading-facebookdpc-documents

Meta prohibited from use of personal data for advertising (2023, januar). Lokaliseret på https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising

Irish Data Protection Authority gives € 3.97 billion present to Meta (2023, januar). Lokaliseret på https://noyb.eu/en/irish-data-protection-authority-gives-eu-397-billion-present-meta

Datatilsynet Vejledning om Cloud (2022), s. 15, Punkt 3.2.1, Særligt ad pkt. f). Lokaliseret på: https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

Greenwald, G., MacAskill, E., & Poitras, L. (2013, juni 7). *NSA Prism program taps into user data of Apple, Google and others. The Guardian*.
Lokaliseret på: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Gallagher, R., & Greenwald, G. (2014, mai 19). *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas. The Intercept.*

Lokaliseret på: https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

6.3 Hjemmesider

www.karnov.dk (besøgt d. 14.05.2023)

www.noyb.eu (besøgt d. 14.05.2023)

www.statistica.com (besøgt d. 14.05.2023)

https://commission.europa.eu/index_en (besøgt d. 14.05.2023)

www.retsinformation.dk (besøgt d. 14.05.2023)

6.4 Forkortelser

TEUF - Traktaten om den Europæiske Unions Funktionsmåde

GDPR - The General Data Protection Regulation

EU - Den Europæiske Union

EDPB - European Data Protection Board

DPA - Data Processing Agreement

SCC - Standard Contractual Clauses

BCC - Business Contractual Clauses

6.5 Domme og afgørelser

Sag: C-582/14

Sag: C-434/16

Sag: C-28/08 P

Sag: C-311/18

Sag: C-73/07

Sag: C-362/14

Bindende afgørelse fra EDPB: https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf

Afgørelse fra det østrigste datatilsyn om ulovlige persondataoverførsler til USA (på tysk): Lokaliseret på: https://noyb.eu/sites/default/files/2023-03/Bescheid%20redacted.pdf, besøgt d. 14.05.2023