

Databeskyttelsesforordningen og Det Digitale Indre Marked

*Kim Østergaard, professor mso., ph.d.,
Juridisk Institut, Syddansk Universitet*

og

*Hanne Marie Motzfeldt, lektor, ph.d.
Juridisk Institut, Aarhus Universitet*

1. Indledning

Formålet med databeskyttelsesforordningen – i folkemunde GDPR¹ – er ifølge mange lærde og den forkætrede retsakts egne ord at beskytte borgernes grundlæggende rettigheder til privatliv og beskyttelse af personoplysninger.²

Hensigten med nærværende blogindlæg er at rette blikket væk fra formålsbestemmelsernes ordlyd og det meget omtalte samspil med de ideelle tanker om menneske- og grundrettigheder.³ Fokus rettes i stedet mod de retsøkonomiske hensyn, der reelt ligger bag udviklingen af de internationale databeskyttelsesretlige regelsæt – den stamme, hvorpå OECD's guidelines meget sigende var det første, og GDPR er det nyeste skud.

OECD guidelines var det første internationale regelsæt inden for databeskyttelse. De oprindelige OECD Guidelines⁴ blev udarbejdet i slutningen af 1970erne. At OECD var den første organisation, der vedtog et sæt retningslinjer for databeskyttelse, er lige så sigende som baggrunden for deres revision i 2013. Af de reviderede guidelines fremgår, at arbejdet

- 1 Europa-Parlamentets og Rådets Forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
- 2 Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
- 3 Nærværende blog er en opdateret og justeret fremstilling af Østergaard, Kim og Motzfeldt, Hanne Marie, fortid, nutid og fremtid – om databeskyttelsesreformen i et retsøkonomisk perspektiv i Festskrift til Hans Viggo Godsk Pedersen, Clausen, Nis Jul, Kronborg, Anette, Dietz Legind, Nina og Mortensen, Bent Ole Gram (red.), DJØF. 2017, s. 597 ff.
- 4 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

med revisionen blev startet op på baggrund af Soul-deklarationen i 2008.⁵ Af Soul-deklarationen fremgår helt i tråd med den nedenfor beskrevne baggrund, at medlemsstaterne lover at fremme den internetdrevne (digitale) økonomi.

Formålet er vise, at GDPR ikke ensidigt skal læses som et regelsæt, der præciserer menneske- og grundrettigheder – men i lige så høj grad skal læses i sin retsøkonomiske kontekst og behovet for en stærk, datadreven økonomisk udvikling i Europa.

Indledningsvis præsenteres GDPR i afsnit 2. I afsnit 2.1. afdækkes den reelle bevæggrund; at skabe folkelig tryghed i forhold til digitale tjenester indenfor såvel den private som den offentlige sektor. Herefter ses i afsnit 2.2. på databeskyttelsesreformens indhold. Det vurderes, at den virkelige reformindsats ligger i udformningen af nye regler, der skal betrygge EU-borgerne og skabe tillid til digitale tjenester. Med denne vurdering som udgangspunkt – at fokus har været på skabelse af tryghed ved at sikre forudseelighed, troværdighed, tillid, efterlevelse og effektiv håndhævelse af de persondataretlige regler – vendes blikket i afsnit 3 mod den retsøkonomiske baggrund for reformen. Det konkluderes, at indsigt i de retsøkonomiske aspekter kan vejlede om, hvordan reglerne fremover vil blive forstået.

2. GDPR

GDPR blev vedtaget i 2016 efter en langstrakt lovgivningsproces og blev offentliggjort i EU-Tidende den 4. maj 2016. Forordningen er den ene af to retsakter, der udgør den unionsretlige databeskyttelsesreform, og den træder som bekendt i kraft 25. maj 2018.⁶ I Danmark er arbejdet med den supplerende lovgivning i gang, og forslaget til en ny databeskyttelseslov blev fremsat 25. oktober 2017.

5 Pkt. 20 i EXPLANATORY MEMORANDUM to OECD Guidelines, tilgængelig på <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>.

6 Den anden retsakt er Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne.

2.1. Databeskyttelsesreformens formål

Databeskyttelsesreformen er et af de lovgivningsinitiativer, der skal realisere Kommissionens strategi om Det Digitale Indre Marked.⁷ Reformen blev indsat som et centralt element i strategien på baggrund af en række undersøgelser, der viste udpræget grad af folkelig mistillid til digitale tjenester i Europa.⁸

Denne baggrund afspejler sig i de mange udmeldinger fra EU-institutionerne om regelsættet. I den formidlingsmæssigt lettere ende kan nævnes en pressemeddelelse fra Kommissionen om vedtagelsen af forordningen den 15. december 2015. Her citeres Andrus Ansip, næstformand for Kommissionen og ansvarlig for det digitale indre marked, for følgende:

“Dagens aftale er et stort skridt hen imod et digitalt indre marked. Den vil fjerne hindringer og skabe muligheder. Europas digitale fremtid kan kun baseres på tillid. Med solide fælles standarder for databeskyttelse kan folk være sikre på, at de har kontrol over deres personoplysninger, og samtidig drage fordel af alle de tjenester og muligheder, der ligger i et digitalt indre marked. Vi bør ikke opfatte privatlivets fred og databeskyttelse som hæmmende for økonomisk aktivitet. De udgør faktisk en væsentlig konkurrencemæssig fordel. Dagens aftale skaber et solidt grundlag, som skal hjælpe Europa med at udvikle innovative digitale tjenester. Vores næste skridt er nu at fjerne uberettigede hindringer, som begrænser de grænseoverskridende datastrømme: lokal praksis og undertiden national lovgivning, som begrænser lagring og behandling af visse oplysninger uden for det nationale område. Så lad os fortsætte fremad og opbygge en åben og blomstrende økonomi i EU – baseret på de højeste standarder for databeskyttelse og uden uberettigede hindringer.”⁹

7 Se om strategien for det digitale indre marked f.eks. COM(2015) 192 final, tilgængelig på

[http://www.eu.dk/samling/20151/kommissionsforslag/KOM\(2015\)0192/forslag/1251331/1528670/index.htm](http://www.eu.dk/samling/20151/kommissionsforslag/KOM(2015)0192/forslag/1251331/1528670/index.htm) og s. 7 i Det Europæiske Råds Konklusioner af 25. og 26. juni 2015, tilgængelig på <http://data.consilium.europa.eu/doc/document/ST-8672-2015-INIT-/da/pdf>, begge tilgået 9. juli 2016. Se også en kort beskrivelse i Trazaskowski, Jan m.fl. *Introduction to EU Internet Law*. Ex Tuto, 2015, s. 36 ff.

8 Pkt. 4.3. i Commission staff working document, A Digital Single Market Strategy for Europe – Analysis and Evidence (Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions), tilgængelig på <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015SC0100> tilgået 9. juli 2016.

9 http://europa.eu/rapid/press-release_IP-15-6321_da.htm, tilgået 9. juli 2016.

Ønsket om at skabe tillid til eksisterende og fremtidig informations- og kommunikationsteknologi fremgår da også af forordningens officielle tekst. F.eks. begrundes forordningens regler bl.a. i præamblen til databeskyttelsesforordningens betragtning 9. Af denne betragtning fremgår, at det nugældende persondatadirektiv ikke har været tilstrækkeligt til at hindre *“en udbredt offentlig opfattelse af, at der er betydelige risici for beskyttelsen af fysiske personer, navnlig i forbindelse med onlineaktivitet”*. Præambelens betragtning 7 må også betragtes som betydningsfuld. Efter en omtale af den stadig hastigere teknologiske udvikling og globalisering udtrykkes det klart i præambelens betragtning 7, at denne *“udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i Unionen, som understøttes af effektiv håndhævelse, fordi det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked.”*

Med andre ord har et af målene med reformen været at udarbejde et regelsæt, der kan fremme tryghed og tillid til digitale tjenester. I de følgende afsnit beskrives fire eksempler på, hvilke midler EU-lovgiver har taget i brug i forordningen.

2.2. Databeskyttelsesreformens indhold

Databeskyttelsesforordningen har den samme grundlæggende struktur som persondatadirektivet, og der er ikke umiddelbart iøjnefaldende ændringer af hverken behandlingsbetingelser eller behandlingsprincipper. Det fremgår da også af præambelens betragtning 9, at ophævelsen af persondatadirektivet ikke skyldes en afstandtagen til reglerne i direktivet – men direktivets mangel på effekt i forhold til efterlevelse og reel harmonisering af de databeskyttelsesretlige regler.

Visse elementer i reformen synes i særlig grad at have til hensigt at fremme borgernes tryghed ved at anvende digitale tjenester; i det følgende nævnes styrkelsen af ansvarlighedsprincippet, de udvidede informationsforpligtelser, justeringerne af kravene til gyldigt samtykke og harmoniseringen af sanktionerne i form af bøder.

2.2.1. Styrkelse af ansvarlighedsprincippet

For så vidt angår princippet om ansvarlighed – eller mere retvisende princippet om *accountability* – er dette et globalt anerkendt persondataretligt princip med et dobbelt sigte.¹⁰ Princippet sigter dels til at

10 F.eks. pkt 11 i International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners den 5. November 2009, http://privacyconference2011.org/htmls/adoptedResolutions/2009_-Madrid/2009_M1.pdf, tilgået 9. juli 2016.

sikre faktisk efterlevelse af de databeskyttelsesretlige regler i de dataansvarliges hverdag, dels at understøtte tilsynsmyndighedernes arbejde.

Ansvarlighedsprincippet forpligter de dataansvarlige til at træffe passende og effektive foranstaltninger, som kan sikre, at de persondataretlige regler overholdes i deres organisation. I forlængelse heraf forlanges, at de dataansvarlige efter anmodning skal kunne fremlægge dokumentation på denne overholdelse. Med andre ord indebærer princippet om ansvarlighed, at dataansvarlige skal udarbejde interne ordninger (politikker og procedurer) for at sikre, at al behandling af persondata sker i overensstemmelse med de gældende regler. De skal samtidig sikre, at der til enhver tid skal være dokumentation for organisationens databehandling, og at denne kan forelægges tilsynsmyndighederne.¹¹

Princippet om ansvarlighed har givet sig udslag i en række af bestemmelserne i GDPR.¹² Det drejer sig om bestemmelsen i artikel 5, stk. 2, om den dataansvarliges pligt til at sikre overholdelse af de persondataretlige principper. Den reelle styrkelse af princippet skal imidlertid findes i artikel 25 om databeskyttelse gennem design og standardindstillinger (by design og by default), i kravene om konsekvensvurderinger ved mere risikofyldte behandlinger, jf. artikel 35, samt kravet om fortegnelse over databehandling i artikel 30 og dokumentation af sikkerhedsbrud, jf. artikel 33, stk. 5.

Den mere konsekvente brug af princippet om ansvarlighed i GDPR må betegnes som et centralt tiltag, der har til formål at udvirke, at de dataansvarlige efterlever de persondataretlige regler – og at borgerne oplever en forandring i organisationernes tilgang til at overholde reglerne.

Det reelle sigte med justeringerne er således at opnå en højere grad af tillid til de dataansvarlige, der agerer inden for det Digitale Indre Marked.

2.2.2. Styrkelsen af de registreredes rettigheder

Databeskyttelsesforordningen styrker i vidt omfang de registreredes rettigheder. I den offentlige debat har fokus været rettet mod reglerne om dataportalitet og retten til at blive glemt. Her hævdes det, at der er lige så betydningsfulde ændringer gemt i forordningens artikel 12 og 13-14.

11 Artikel 29-gruppens udtalelse om princippet om ansvarlighed af 13. juli 2010, WP 173, s. 10 ff.

12 Princippet fremgår for nuværende af persondatadirektivets artikel 6, hvor første stykke regulerer oplysningers pålidelighed og andet stykke fastsætter, at det er den dataansvarliges ansvar at sikre, at bestemmelserne i første stykke overholdes. Tilsvarende ses i direktivets artikel 17, stk. 1, om sikkerhedskrav, hvorefter det er den dataansvarlige, der bærer forpligtelsen til at gennemføre de nødvendige tekniske og organisatoriske foranstaltninger.

Artikel 12 konkretiserer god databehandlingskik. De dataansvarlige pålægges at bruge et klart og enkelt sprog og sikre, at information mv. er forståelig og let tilgængelig, jf. artikel 12, stk. 1: De dataansvarlige skal også sikre praktiske procedurer, der gør det let for de registrerede at udøve deres rettigheder, jf. artikel 12, stk. 2, ligesom der fastsættes tidsfrister for svar i artikel 12, stk. 3-4, og rammer for, hvornår registrerede må afvises eller anmodes om yderligere oplysninger i artikel 12, stk. 5. I det hele synes bestemmelsen at være et tiltag, der skal øge de registreredes muligheder for at kunne over- og gennemskue den behandling af personoplysninger, der sker.

Tilsvarende er de informationer, der skal eller skal overvejes at give ved indsamling af oplysninger, udvidet i artikel 13, stk. 1-2 og artikel 14, stk. 1-2. Herudover er der indsat en ny regel om at kontakte den registrerede og informere vedkommende, hvis de afgivne oplysninger senere ønskes anvendt til et andet formål end oprindeligt oplyst. Heri ligger ikke, at sådan videreanvendelse hindres, da dette reguleres af formålsbestemthedsprincippet i artikel 5, stk. 1, litra c. De nye regler om information af de registrerede ved videre, ny brug af personoplysninger kræver alene en henvendelse herom. Dette sigter til at skabe gennemsigtighed og transparens i databehandlingen – de registrerede skal vide, hvad der senere sker med deres oplysninger og ikke være i tvivl om, hvad organisationerne foretager sig.

Det synes oplagt, at både artikel 12 og den nye regel om information om ny brug af oplysninger søger at skabe tryghed i forhold til borgerne og sikre, at de ikke er i tvivl om, hvad der sker med deres oplysninger.¹³

2.2.3. Skærpelse af kravene i samtykkesituationen

Som det også er nævnt ovenfor, er der i forordningen sket en justering af kravene til samtykke. Også denne ændring synes at have til formål at hindre uoverskuelighed. Borgernes oplysninger skal kun bruges i de sammenhænge, borgerne kender til. Der skal være åbenhed og gennemsigtighed – der må ikke være grund til at mistænke europæiske organisationer for at “luske” med deres udnyttelse af data.

Definitionen af samtykke er den samme som under direktivet, nemlig at et almindeligt “samtykke” fra den registrerede er enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling, jf. artikel 4, nr. 11. Er der tale om behandling af følsomme oplysninger, skal samtykket desuden være udtrykkeligt, jf. artikel 9, stk. 2,

¹³ Se for perspektivering af regelændringerne: Blume, Peter. *Persondataretten – i en brydningstid, store og små persondata: persondatarettens grundproblemer*. DJØF. 2014.

litra a. I modsætning til direktivet er forordningens regulering af samtykke imidlertid ikke udtømt hermed, idet artikel 7 er indsat. Artikel 7 indeholder særlige persondataretlige gyldighedsbetingelser. Opfylder et samtykke ikke disse krav, kan samtykke ikke være grundlag for behandling af personoplysninger.

I nærværende sammenhæng er særlig artikel 7, stk. 4, interessant. Af denne bestemmelse fremgår, at der ved vurderingen af, om et samtykke er frivilligt, tages størst muligt hensyn til bl.a. om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af denne kontrakt. Om bestemmelsen står i den danske betænkning, at det “er vanskeligt at fastlægge rækkevidden af denne bestemmelse på forhånd, og bestemmelsen vil utvivlsomt blive udviklet gennem praksis i de kommende år.”¹⁴

For nuværende står det dog klart, at bestemmelsen skærper åbenheden og gennemsigtigheden. Anderledes udtrykt lægger forordningen op til at hindre “misforståelser” ved, at den registrerede fokuserer på at købe den ønskede ydelse eller vare – og ikke opdager, at samtykket dækker både de oplysninger, der er relevante for denne aftale og andre oplysninger, som ikke har relevans for købet. Reglen presser omvendt den dataansvarlige til at modstå fristelsen til at benytte lejligheden til ubemærket at få flere oplysninger – andre oplysninger, der kan have en værdi ved videre brug.

I ovenstående ligger næppe, at der ikke kan indhentes “overflødige” oplysninger. Et eksempel kan være oplysninger til indgåelse og opfyldelse af kontrakter og oplysninger til efterfølgende markedsanalyser. Begge formål er legitime i databeskyttelsesretten og kan bære behandling af personoplysninger – men forordningens nye regel tilkendegiver, at lovgiver ikke ønsker en “sammenblanding”, som kan skabe uigennemsigtighed og dermed utryghed – og i hvert fald må borgerne ikke blive presset til at give oplysninger, der er uden betydning for købet; der skal være et frit valg.

Det reelle sigte med den nye regel synes således at være at skabe tryghed i forhold til anvendelse af personoplysninger i Det Digitale Indre Marked.

2.2.4. Sanktioner – bøder

For så vidt angår fastsættelse af bøder for overtrædelse af de persondataretlige regler, er der tale om en umiddelbart observerbar og markant ændring af retstilstanden. De facto har sanktionerne for overtrædelse af persondatadirektivet været overladt til medlemsstaterne – og i visse lande stort set været begrænset til kritik fra tilsynene. Dette ændres efter maj 2018 – efter det danske lovforslag både for private virksomheders og myndigheders vedkommende, om end bødestørrelserne er højere i den private sektor.

14 Betænkning nr. 1565 s. 180 ff.

Af forordningens artikel 83, stk. 4, litra a, følger f.eks., at overtrædelse af kravet om rimelig behandling af personoplysninger (god databehandlingsskik), sanktioneres i overensstemmelse med bestemmelsens andet stykke. Artikel 83, stk. 2, fastsætter niveauet som bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dennes samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere.¹⁵ Det danske lovforslag lægger op til bøder op til 16 millioner for offentlige myndigheder.

Ved fastlæggelse af en konkret bødes størrelse skal domstolene dels tage hensyn til de momenter, der er angivet i artikel 83, stk. 2, dels tage hensyn til Datatilsynets anbefalinger og samtidig sikre, at den pågældende sanktion er effektiv, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, jf. også forordningens præambels betragtning 151 og 152. Det fremgår således ganske direkte, at denne ændring af de databeskyttelsesretlige regler har til formål at sikre overholdelse af reglerne – og dermed øge trygheden i forhold til brug af personoplysninger i det Digitale Indre Marked.

2.3. Opsummering

Databeskyttelsesreformen kan ikke betegnes som en egentlig reform af reglerne om det retlige grundlag for behandling eller af de grundlæggende principper for lovlig og rimelig behandling af personoplysninger. Den reelle reformindsats ligger snarere i udformningen af bestemmelser, der skal sikre efterlevelse, troværdighed, gennemsigtighed, forudseelighed og effektiv håndhævelse af de persondataretlige regler – og dermed vinde borgernes tillid til digitale tjenester.

3. Databeskyttelsesreformens retsøkonomiske baggrund

I det følgende ses på, hvilke retsøkonomiske incitament der betingede databeskyttelsesreformen. Indledningsvis præsenteres Kommissionens undersøgelser af persondatadirektivets manglende effektivitet i forhold til at nå målet om at skabe tillid og tryghed i den europæiske befolkning. Herefter ses i afsnit 3.2. på den økonomiske betydning af data. Det tydeliggøres, at de nye regler i høj grad kan betragtes som et skridt på vejen til at etablere Det Digitale Indre Marked, og det vurderes, at reglernes udformning kan forklares med forudsigelserne om den fremtidige datadrevne økonomi. Herefter vurderes retshåndhævernes udfordring i forhold til at opnå målet om skabelse

¹⁵ Det er endnu uafklaret, om myndigheder skal kunne idømmes bøder i Danmark.

af tryghed med udgangspunkt i klassiske informations-økonomiske betragtninger, inden blikket i afsnit 4 vendes mod fremtidsperspektiverne.

3.1. Baggrunden for reformen

Uagtet at ethvert regelsæt kan trænge til justeringer og kodificering af praksis efter 20 år, synes katalysatoren for databeskyttelsesreformen snarere at være lovgivningsprogrammet om Det Digitale Indre Marked og en række undersøgelser af unionsborgernes (manglende) tillid til de digitale tjenester i Europa. Kommissionen lægger f.eks. ikke fingre imellem i strategien for det indre marked:

“Trust in the digital environment is undermined by concerns about whether fundamental rights, in particular the protection of personal data, are being respected. These difficulties stem from the sheer volume of data collected every day, and the fact that individuals are often not adequately informed that their data are collected, what happens to their personal data, what it is used for and/or whether previously collected data is reused with a different aim, potentially by new users. Although many people consider that disclosure of personal data is increasingly a part of modern life, they feel they are not in control of their data. A large majority (74%) would like to give their specific approval before their personal data is collected and processed. Moreover, trust in Internet companies is low: only 22% of individuals have full trust in service providers such as search engines, social networking sites and e-mail services. This feeling is exacerbated by the large number of personal data breaches and frequent identity theft and usurpation incidents reported, but also by fear of discriminatory treatment of individuals following profiling based on collected personal data.”¹⁶

Den citerede passage er en af mange, og det er således nærliggende at antage, at drivkraften bag reformen har været behovet for at imødegå unionsborgernes mistillid til de digitale tjenester i Europa. I dette lys kan databeskyttelsesreformens fokus på efterlevelse og håndhævelse forklares med det forhold, at den tidligere regulering havde fejlet i forhold til at opnå målet; borgernes tillid. Der er således en åbenbar diskrepans mellem det politisk orienterede ønske om Det Digitale Indre Marked og borgernes vurdering af de risici, der er forbundet med at videregive personhenførbare informationer.

16 Note 5.

3.2. Den økonomiske betydning af persondata

De håndhævelsesmidler, der indføres med databeskyttelsesreformen, må betegnes som ganske håndfaste. De dataansvarlige vil formentlig opleve kravene til interne politikker og procedurer, til fortegnelser over alle behandlinger kombineret med det høje bødeniveau, som væsentlige stramminger. Efterlevelsen af databeskyttelsesforordningen kommer således i et virksomhedsperspektiv til at indebære signifikante transaktionsomkostninger, og der kan selvsagt sættes spørgsmålstegn ved, om afholdelsen af sådanne transaktionsomkostninger er proportionale med de ideelle formål, databeskyttelsesforordningen angiver at forfølge.

Er hensynet “blot” ideelt – en grundrettighedstankegang – er den omstændighed, at den tidligere regulering ikke formåede at sikre borgernes tillid til de europæiske dataansvarlige, næppe i sig selv nok til at begrunde et så omfattende håndhævelsessystem, som databeskyttelsesforordningen etablerer. Hertil forudsættes normalt, at der er endda meget væsentlige, økonomiske interesser på spil. Denne er da også til stede i form af antagelsen om, at realiseringen af Det Digitale Indre Marked kan give signifikante muligheder for at maksimere det samlede økonomiske output i de europæiske medlemsstater, idet anvendelsen af relevant information i en data- og vidensbaseret økonomi indeholder grundlaget for at øge den økonomiske vækst.

Denne bagvedliggende antagelse fremgår af flere tilkendegivelser relateret til det lovgivningsprogram, der skal realisere Det Digitale Indre Marked.¹⁷ I Jean Claude Junkers dagsorden for job, vækst, retfærdighed og demokratisk forandring, lyder det sådan:

*“Ved at skabe et forbundet digitalt indre marked kan vi i den kommende Kommissions valgperiode generere yderligere vækst i Europa i størrelsesordenen op til 250 mia. EUR og således skabe hundredtusindvis af nye job, især for de unge jobsøgende, og et dynamisk vidensbaseret samfund.”*¹⁸

I en anden kontekst nævnes det bl.a., at der er gevinster svarende til en yderligere forøgelse af EU's BNP på 415 mia. euro ved at realisere Det

¹⁷ For en umiddelbar betragtning kan man naturligvis indvende, at ideologiske hensigter alene kan have motiveret databeskyttelsesreformen. Det fremgår da også af forordningens tekst, at reglerne skal sikre overholdelse af de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger, jf. Den Europæiske Unions Charter artikel 7 og 8 og TEUF artikel 16.

¹⁸ Åbningstale til Europa-Parlamentets plenarforsamling af 15. juli 2014, http://ec.europa.eu/priorities/sites/beta-political/files/pg_da.pdf.

Digitale Indre Marked.¹⁹ Med andre ord har Kommissionen vurderet, at der er et uforløst økonomisk potentiale i en overgang til en digital økonomi. I den sammenhæng er det Kommissionens opfattelse, at data har en stærkt stigende økonomisk betydning. Under overskriften “Opbygning af en dataøkonomi” skrev Kommissionen i 2015 sådan:

“Big data, cloud computing og tingenes internet har central betydning for EU’s konkurrenceevne. Data betragtes ofte som en katalysator for økonomisk vækst, innovation og digitalisering i alle økonomiske sektorer (navnlig for SMV’er og nystartede virksomheder) og i samfundet som helhed. Big data og højtydende databehandling er også med til at ændre den måde, der drives forskning og udveksles viden på, som led i overgangen til en mere effektiv og hurtigt reagerende “åben forskning.””²⁰

Af samme meddelelse fremgår, at databeskyttelsesreformen – og opnåelse af borgernes tillid – betragtes som en forudsætning for en række tiltag, der skal styrke den datadrevne økonomi i Europa. Om disse tiltag, der skal følge efter forordningen, lyder det i uddrag sådan:

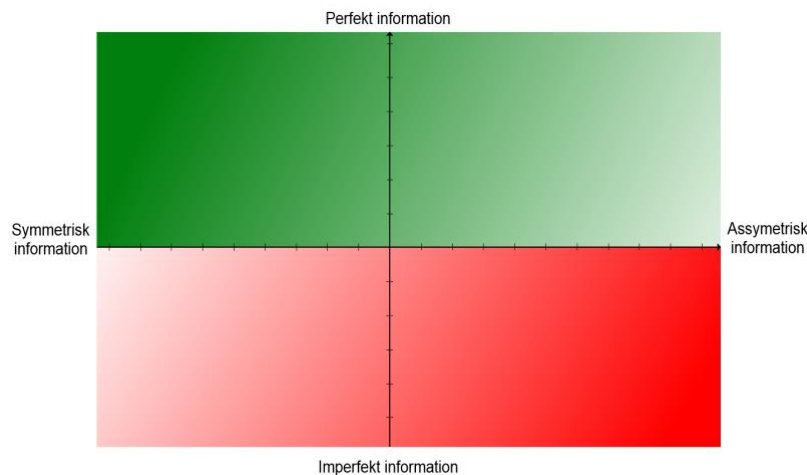
“Kommissionen vil i 2016 foreslå et europæisk initiativ om “frie datastrømme” ... Initiativet vil omfatte aktuelle emner som ejerskab, interoperabilitet, anvendelighed og adgang til data i forskellige sammenhænge (virksomhed-til-virksomhed, virksomhed-til-forbruger, maskingenererede data, maskine-til-maskine). Endvidere vil der blive taget skridt til at lette adgangen til det offentlige data for at fremme innovation. Kommissionen vil lancere et europæisk initiativ vedrørende cloud computing, der skal omfatte certificering af cloud-tjenester, kontrakter, muligheden for at skifte cloud-tjenesteudbydere og etablering af en “forskningssky” til fremme af “åben forskning.””²¹

Med andre ord er et centralt omdrejningspunkt for realiseringen af Det Digitale Indre Marked adgangen til persondata – og dermed borgernes vilje til at afgive deres personoplysninger og lade dem anvende i forskellige sammenhænge. Der er således næppe tvivl om, at et centralt formål med

19 Pkt. 1 i *En strategi for et digitalt indre marked i EU*, Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske økonomiske og sociale udvalg og Regionsudvalget af 6. maj 2015, COM(2015), tilgængelig på, [http://www.eu.dk/samling/20151/-kommissionsforslag/KOM\(2015\)0192/forslag/1251331/1528670/index.htm](http://www.eu.dk/samling/20151/-kommissionsforslag/KOM(2015)0192/forslag/1251331/1528670/index.htm), tilgået 9. juli 2016.

20 Note 21: Pkt. 4.1.

21 Ibid.



reformen er at skabe tryghed og sikre de dataansvarliges efterlevelse af de persondataretlige regler.

3.3. Rationalet for at afgive persondata

Det er nødvendigt at inddrage en informationsøkonomisk vinkel for at vurdere de udfordringer, databeskyttelsesforordningen skal imødekomme; borgernes tillid.

I et virksomhedsperspektiv indebærer en øget adgang til information, at dette trækker i retning af en mindre grad af imperfekt information og en højere grad af symmetrisk information. Set fra et borgersynspunkt vil afgivelsen af persondata derimod normalt ikke indebære samme mulighed for en mindre grad af imperfekt information og en højere grad af symmetrisk information. Nedenstående figur illustrerer, at afgivelsen af persondata trækker i retning fra anden kvadrant til fjerde kvadrant set fra virksomhedens synsvinkel:

Der synes næppe at være belæg for, at den ideale tilstand om perfekt og symmetrisk information kan opnås. Dette rejser et centralt bagvedliggende informationsøkonomisk problem. Hvilket rationale er der overhovedet for at videregive personhenførbare information set fra et borgersynspunkt?

I den sammenhæng synes det umiddelbart relevant at sondre mellem, hvorvidt der i den givne situation foreligger en indgåelse af en elektronisk kontrakt²² (eller adgang til en offentlig ydelse), eller dette ikke er tilfældet. I

22 En elektronisk kontrakt forstås i denne sammenhæng som værende, at der mellem virksomheden og forbrugeren anvendes elektroniske kommunikationsmidler til at indgå kontrakten, uagtet om realydelsen kan karakteriseres som digital eller ej. Det centrale er, at der benyttes elektroniske kommunikationsmidler, der ikke nødvendiggør, at parterne mødes fysisk.

de tilfælde, hvor der indgås en elektronisk forbrugerkontrakt mellem en virksomhed og en forbruger, er det økonomiske rationale, at dette sker som led i, at virksomheden profitmaksimerer, og forbrugeren nyttemaksimerer. I en sådan situation har forbrugeren i den ideelle digitale økonomi et incitament til at afgive de fornødne informationer til virksomheden med henblik på, at der sker rigtig opfyldelse af den elektroniske kontrakt.

I de situationer, hvor der ikke er tale om kontraktindgåelse, men borgeren blot bliver bedt om at afgive persondata, f.eks. i forbindelse med de hyppigt anvendte spørgeundersøgelser ved besøg på virksomheders hjemmesider, synes det ikke åbenbart, at borgeren har interesse i at afgive persondata, da afgivelsen heraf ikke umiddelbart medvirker til den enkelte borgers nyttemaksimering. Afgivelsen vil umiddelbart kun tjene til, at virksomheden kan anvende data som led i at profitmaksimere – det vil sige, at der opretholdes en situation med imperfekt og asymmetrisk information.²³ I sådanne situationer, hvor borgeren bliver bedt om at afgive persondata, uden det vedrører opfyldelsen af en elektronisk kontrakt, er det umiddelbart svært at tilvejebringe noget økonomisk rationale herfor.²⁴

Med andre ord burde borgeren – som beskrevet ovenfor – være villig til at afgive personoplysninger ved indgåelse af elektroniske kontrakter, hvor der er en mindre grad af imperfekt information og en højere grad af symmetrisk information. Kun i de tilfælde, hvor afgivelse ikke umiddelbart bidrager til den enkelte borgers velfærd og dermed nyttemaksimering, er det svært at udlede noget rationale for, at borgeren skulle være villig til at afgive personhenførbare data.

Imidlertid er borgeren som udgangspunktet risikoavers og begrænset rationel.²⁵ Den udprægede mistillid til digitale tjenester og disses håndtering af persondata har ifølge Kommissionen medført, at borgerne direkte fravælger indgåelse af elektroniske kontrakter og i stedet vælger mere

23 Se Michael Rothschild & Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, The Quarterly Journal of Economics, Vol. 90, no. 4, 1976, s. 629-649. På s. 629 fremfører forfatterne: “...Furthermore, if individuals were willing or able to reveal their information, everybody would be better off. By their very being, high-risk individuals cause an externality; the low-risk individuals are worse off than they would be in the absence of the high-risk individuals. However, the high-risk individuals are no better off than they would be in the absence of the low-risk individuals.”

24 Det ses derfor også ofte i praksis, at virksomhederne lokker med, at besvarelsen af et spørgeskema indebærer deltagelsen i lodtrækningen om en eller flere præmier.

25 Om denne adfærdsantagelse i den ny-institutionelle økonomi, se Jacob Lyngsie og Kim Østergaard, *Methodological Differences Between Legal Dogmatics and New Institutional Economics*, s. 187 ff. i Rets- og kontraktøkonomi – En antologi, Kim Østergaard, Jacob Lyngsie & Bent Ole Gram Mortensen, Jurist- og Økonomforbundets Forlag, 2016.

traditionelle kontraktformer – især når der er tale om grænseoverskridende aktiviteter. Borgerne viger altså – selv hvor der eksisterer et informationsøkonomisk rationale – tilsyneladende tilbage fra at anvende moderne teknologi. Dermed synes der at være tale om en ganske betydelig udfordring for både EU-lovgiver og de håndhævende myndigheder; der skal opnås en situation, hvor borgeren er betrygget i, at der kun afgives de oplysninger, som bidrager til borgerens egen nyttemaksimering.

Man kan herefter spørge, om sådanne betragtninger overhovedet har interesse for den fremtidige retsudvikling, herunder om de kan indgå som momenter i fortolkningen og udfyldningen af bestemmelserne i GDPR. Som eksempel i det følgende er først og fremmest valgt de ovenfor beskrevne justerede samtykkeregler. Af den ovenfor i afsnit 3.2.3 beskrevne nye gyldighedsbetingelse i artikel 7, stk. 4, følger at udbydere af den digitale tjeneste kun kan skaffe sig lige netop de oplysninger, der kræves for at indgå og gennemføre en kontrakt. Med andre ord søger EU-lovgiver at mindske borgernes mistillid ved at sikre, at udbydere af de digitale tjenester ikke så at sige “benytter lejligheden” til at skaffe sig ekstra oplysninger om borgeren.

Følges dette bagvedliggende rationale, skal gyldighedsbetingelsen i forordningens artikel 7, stk. 4, formentlig forstås sådan, at en kontraktpart ikke kan stille krav om afgivelse af personoplysninger, der er overflødige for at opfylde kontrakten. Omvendt kan et samtykke udemærket anvendes som grundlag for behandling af personoplysninger, blot afgivelsen ikke stilles som krav for kontraktens indgåelse: Dette naturligvis forudsat en klar adskillelse mellem den indsamling af oplysninger, der er relateret til kontrakten og den indsamling, der er båret af et andet formål, f.eks. en tillægstjeneste eller en form for konkurrence.

4. Opsummering og konklusion

Kommissionen konstaterede i starten af 2010'erne, at der til trods for den (stadig) gældende regulering forsat var betydelig mistillid til digitale tjenesters håndtering af persondata.²⁶ Databeskyttelsesreformen blev gennemført for at rette op herpå. Dette afspejler sig indholdsmæssigt især i styrkelsen af ansvarlighedsprincippet, de nye informationsregler, justeringen af samtykkekravet og harmoniseringen af sanktionerne i form af bøder. Sigtet er, at borgerne fremover skal have veldefinerede rettigheder, som efterleves og håndhæves med passende retsmidler, når de afgiver

26 Note 6.

personhenførbare information – hvad enten dette sker i forbindelse med opfyldelse af en kontrakt eller ej.²⁷

Databeskyttelsesreformen er dog at betragte som et middel til at fremme et andet mål end fremme af grundrettighederne, nemlig realiseringen af Det Digitale Indre Marked. Det Digitale Indre Marked antages af Kommissionen at indeholde signifikante muligheder for at maksimere det samlede økonomiske output i de europæiske medlemsstater. Baggrunden er en formodning for, at anvendelsen af relevant information i en data- og vidensbaseret økonomi er et potentielt grundlag for at øge den økonomiske vækst betydeligt. Et centralt omdrejningspunkt i denne kontekst er adgang til og brug af personoplysninger – og en forudsætning herfor er, at de europæiske borgere er villige til at afgive deres personoplysninger digitalt. De europæiske borgeres manglende tillid til digitale løsninger er imidlertid særdeles indgroet ifølge Kommissionens undersøgelser – og borgerne tøver derfor med at afgive deres personoplysninger. Denne tilbageholdenhed giver sig udslag, selv hvor der ud fra et informationsøkonomisk synspunkt består mindre grad af imperfekt information og en højere grad af symmetrisk information, samtidig med at de dataansvarlige profitmaksimerer og borgerne nyttemaksimerer.

Inddrages denne baggrund for databeskyttelsesforordningen af de nationale datatilsyn, det kommende Databeskyttelsesråd, Kommissionen og EU-Domstolen, er det ikke urealistisk, at der vil blive stillet høje krav til de dataansvarliges dokumentation, til gennemsigtighed og åbenhed – men der vil være mindre grund til at frygte hindringer for at bruge personoplysninger til legitime (herunder forretningsmæssige) formål – blot der ikke “luskes” hermed.

27 Der må selvsagt i den forbindelse sondres mellem, hvorvidt retsmidlerne er knyttet til misligholdelse af en given kontrakt mellem parterne, hvor løsningen herpå skal ske med udgangspunkt i en fortolkning af kontraktgrundlaget og/eller ved aftalesuppleringen via obligationsrettens almindelige eller specielle del, eller vedrører en krænkelse af databeskyttelsesforordningen.