EUROPA-
KOMMISSIONEN

Bruxelles, den 10.1.2017
COM(2017) 9 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

"OPBYGNING AF EN EUROPÆISK DATAØKONOMI"

{SWD(2017) 2 final}

"OPBYGNING AF EN EUROPÆISK DATAØKONOMI"

1. INDLEDNING

Data er blevet en vigtig ressource for økonomisk vækst, jobskabelse og samfundsmæssige fremskridt. Dataanalyse letter optimeringen af processer, beslutningstagning, innovation og prognoser om fremtidige begivenheder. Denne globale tendens frembyder et enormt potentiale på forskellige områder, der strækker fra sundhed, miljø, fødevaresikkerhed, klima og ressourceeffektivitet til energi, intelligente transportsystemer og intelligente byer.

"Dataøkonomi"[1] er kendetegnet ved et økosystem af forskellige typer markedsaktører – f.eks. producenter, forskere og infrastrukturudbydere – som samarbejder for at sikre, at data er tilgængelige og anvendelige. Dermed får markedsaktørerne mulighed for at udvinde værdi af disse data ved at skabe forskellige applikationer med stort potentiale for at forbedre borgernes dagligdag (f.eks. trafikstyring, høstoptimering eller fjernbehandling i sundhedssektoren).

Værdien af EU's dataøkonomi blev i 2014 anslået til 257 mia. EUR, eller 1,85 % af EU's BNP[2]. Dette tal steg til 272 mia. EUR i 2015, svarende til 1,87 % af EU's BNP (årlig stigning på 5,6 %). Ifølge samme skøn forudses det, at værdien, hvis de politiske og lovgivningsmæssige rammer for dataøkonomien er på plads i tide, vil stige til 643 mia. EUR i 2020, hvilket svarer til 3,17 % af EU's samlede BNP.

I henhold til den generelle forordning om databeskyttelse[3], vil der fra maj 2018 være et enkelt fælleseuropæisk regelsæt i stedet for de aktuelle 28 sæt national lovgivning. Den nyoprettede one-stop-shop-mekanisme[4] vil sikre, at en enkelt databeskyttelsesmyndighed (DPA) vil være ansvarlig for tilsynet med grænseoverskridende databehandling, der foretages af en virksomhed i EU. Der vil blive sikret ensartethed i fortolkningen af de nye regler. Navnlig i grænseoverskridende tilfælde, hvor flere nationale databeskyttelsesmyndigheder er involveret, vil der blive vedtaget en enkelt afgørelse for at sikre, at der findes fælles løsninger på fælles problemer. Desuden skaber den generelle forordning om databeskyttelse lige konkurrencevilkår mellem EU-virksomheder og udenlandske virksomheder, i og med at virksomheder med hjemsted uden for EU vil

---

1 Dataøkonomien måler den generelle indvirkning, som datamarkedet (dvs. det marked, hvor digitale data udveksles som produkter eller tjenester afledt af rådata) har på økonomien som helhed. Det omfatter bl.a. generering, indsamling, lagring, forarbejdning, distribution, analyse, udvikling, levering og udnyttelse af de data, som de digitale teknologier frembyder (European Data Market study, SMART 2013/0063, IDC, 2016).

2 European Data Market study, SMART 2013/0063, IDC, 2016.

3 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/56/EF (generel forordning om databeskyttelse), EUT L 119 af 4.5.2016, s. 1.

4 Artikel 56 i den generelle forordning om databeskyttelse.

skulle anvende de samme regler som de europæiske virksomheder, hvis de tilbyder varer eller tjenesteydelser eller overvåger enkeltpersoners adfærd i EU. En styrkelse af forbrugernes tillid vil være til gavn for både EU og eksterne kommercielle aktører.

E-databeskyttelsesdirektivet omhandler fortroligheden af elektroniske kommunikationstjenester i EU. Det reviderede e-databeskyttelsesdirektiv, der foreslås sideløbende med denne meddelelse i form af en forordning[5], har til formål at sikre et højt beskyttelsesniveau i fuld overensstemmelse med den generelle forordning om databeskyttelse. Strenge databeskyttelsesregler skaber den tillid, der er nødvendig for, at den digitale økonomi kan udvikle sig på tværs af det indre marked.

Som Kommissionens formand Jean-Claude Juncker understregede i sin tale om Unionens tilstand den 14. september 2016, "*At være europæer betyder, at du har ret til at få dine personoplysninger beskyttet af stærk europæisk lovgivning. Europæerne bryder sig ikke om droner, der registrerer hvert skridt, de tager, eller om virksomheder, der registrerer hvert enkelt klik med musen. Derfor nåede Parlamentet, Rådet og Kommissionen i maj til enighed om en forordning om fælles europæiske databeskyttelsesregler. Der er tale om en stærk europæisk lov gældende for virksomheder, uanset hvor de ligger, og hvornår de behandler dine oplysninger. For privatlivets fred betyder noget i Europa. Det er et spørgsmål om menneskelig værdighed*."

I sin meddelelse fra 2012 om "Beskyttelse af privatlivets fred i en forbundet verden — En europæisk databeskyttelsesramme til det 21. århundrede"[6] og meddelelsen fra 2014 "Hen imod en blomstrende datadreven økonomi"[7] erkendte Kommissionen, at der er behov for moderne og kohærente regler i hele EU, for at data kan flyde frit fra den ene medlemsstat til den anden, og at den europæiske digitale økonomi har været langsom til at slutte sig til datarevolutionen sammenlignet med USA og også mangler en tilsvarende industriel kapacitet. Den konkluderede, at manglen på en retlig ramme, der er tilpasset handelen med data inden for EU, kan være medvirkende til, at der er utilstrækkelig adgang til store datasæt, at der forekommer eventuelle adgangsbarrierer for nye markedsdeltagere, og at innovationen hæmmes.

Det kan forventes, at uberettigede **begrænsninger for fri udveksling af data** vil hæmme udviklingen af EU's dataøkonomi. Disse begrænsninger vedrører krav, der pålægges af de offentlige myndigheder, for placeringen af data i forbindelse med lagring eller behandling. Spørgsmålet om fri udveksling af data vedrører alle typer data: virksomheder og aktører i dataøkonomien håndterer industrielle og maskingenererede data (både personoplysninger og andre data) samt data, som skabes gennem menneskers aktiviteter. I strategien for et digitalt indre marked meddelte Kommissionen, at den ville foreslå et initiativ for at fjerne de begrænsninger for fri udveksling af data, der skyldes andre faktorer end hensynet til beskyttelse af personoplysninger i EU, samt uberettigede restriktioner for placeringen af data med henblik på opbevaring eller forarbejdning. Sådanne begrænsninger omfatter bl.a. retsakter vedtaget af medlemsstaterne, administrative regler og praksis, der har samme virkning. Antallet vil stige, efterhånden som dataøkonomien vokser, hvilket skaber usikkerhed om, hvor data kan lagres eller

5 COM (2017) 10.

6 COM (2012) 9.

7 COM (2014) 442.

behandles. Dette kan påvirke alle sektorer i økonomien og både private og offentlige organisationer, som kan have svært ved at få adgang til mere innovative og/eller billigere datatjenester. Uberettigede restriktioner for placering af data udgør et indgreb i den frie udveksling af tjenesteydelser og etableringsfriheden, som er fastsat i traktaten, og er også i strid med den relevante afledte ret. Dermed risikerer man, at markedet fragmenteres, at brugerne gives en lavere servicekvalitet, og at konkurrenceevnen forringes for udbyderne af datatjenester, især hvis der er tale om mindre enheder.

Uberettigede datalokaliseringskrav indgår også i de drøftelser, der føres mellem EU og dets handelspartnere, i lyset af at data og datatjenester får stadig større betydning i den globale økonomi og på baggrund af tredjelandenes potentielle holdninger til dette spørgsmål. EU's databeskyttelsesregler kan ikke indgå som emne for forhandlinger i en frihandelsaftale. Som forklaret i meddelelsen om udveksling og beskyttelse af personoplysninger i en globaliseret verden[8] skal dialogerne om databeskyttelse og handelsforhandlingerne med tredjelande føres hver for sig. Derudover vil Kommissionen, som det er anført i meddelelsen om handel for alle[9], søge at anvende EU's handelsaftaler til at fastsætte regler for e-handel og grænseoverskridende datastrømme og bekæmpe nye former for digital protektionisme i fuld overensstemmelse med og uden at indskrænke EU's regler for beskyttelse af personoplysninger.

Efterhånden som den datadrevne omstilling når ind i økonomien og samfundet, genereres der stadig større mængder data af maskiner eller processer, der er baseret på nye teknologier, som f.eks. tingenes internet (IoT), fremtidens fabrikker og autonome netforbundne systemer. Netforbundne miljøer ændrer i sig selv den måde, hvorpå man kan få adgang til data: data, som der tidligere normalt var adgang til via fysiske forbindelser, kan man nu få fjernadgang til. Den store mangfoldighed af datakilder og -typer og de rige muligheder for at anvende indsigten i disse data på forskellige områder, bl.a. til udvikling af offentlige politikker, kan endnu kun anes. For at få fordel af disse muligheder skal både de offentlige og de private aktører på datamarkedet have adgang til store og forskelligartede datasæt. Spørgsmålene om adgang til og transmission af de data, der genereres af disse maskiner eller processer, er derfor af central betydning for udviklingen af en dataøkonomi og kræver en omhyggelig vurdering.

Andre nye spørgsmål vedrører anvendelsen af reglerne om ansvar for eventuelle skader som følge af en fejl i en netforbundet enhed eller en robot samt dataenes portabilitet og interoperabilitet. I forbindelse med nye teknologier som f.eks. tingenes internet eller robotteknik eksisterer der komplekse og sofistikerede indbyrdes afhængigheder, både internt i produkter (baseret på software og hardware) og mellem indbyrdes forbundne enheder. Desuden kan der opstå nye spørgsmål i forbindelse med autonome maskiner, som ved uventede og utilsigtede funktionsmåder kan medføre skader på personer og genstande. Disse fænomener kan skabe retlig usikkerhed med hensyn til anvendelsen af de eksisterende rammer for ansvar og sikkerhed.

Som bebudet i strategien for et digitalt indre marked er det Kommissionens mål at skabe klare og tilpassede politiske og retlige rammer for dataøkonomien ved at fjerne de resterende hindringer for den frie bevægelighed for data og afhjælpe de retlige

[8] COM (2017) 7.

[9] COM (2015) 497.

usikkerhedsmomenter, som de nye datateknologier har skabt. De øvrige mål, der ligger til grund for denne meddelelse, tager sigte på at skabe øget tilgængelighed og anvendelse af data, fremme nye dataforretningsmodeller samt forbedre vilkårene for adgang til data og udvikling af dataanalyse i EU. På den baggrund fremlægger Kommissionen fokuserede spørgsmål til drøftelse med henblik på "Opbygning af en europæisk dataøkonomi".

Derfor belyses følgende spørgsmål i denne meddelelse: frie datastrømme; adgang og overførsel i forbindelse med maskingenererede data; ansvar og sikkerhed i relation til nye teknologier; og ikke-personoplysningers portabilitet, interoperabilitet og standarder. Denne meddelelse indeholder også forslag til at eksperimentere med fælles forskriftsmæssige løsninger i praksis.

Kommissionen lancerer en bred dialog med interessenterne om de emner, som belyses i denne meddelelse. Det første skridt i denne dialog er en offentlig høring, der lanceres sideløbende med dataøkonomipakken[10].

2. FRIE DATASTRØMME

Hvis der skal skabes en velfungerende og dynamisk dataøkonomi, er det nødvendigt, at datastrømmene i det indre marked fremmes og beskyttes. I en kontekst med hurtig teknologisk udvikling medvirker sikre og pålidelige frie datastrømme til at beskytte de fire grundlæggende frihedsrettigheder i EU's indre marked, som er nedfældet i traktaterne (fri bevægelighed for varer, arbejdstagere, tjenesteydelser og kapital). Datatjenester er i hastig udvikling både i EU og på verdensplan. Hvis der skabes et effektivt og barrierefrit indre marked i denne sektor, vil det skabe betydelige muligheder for yderligere vækst og beskæftigelse.

Denne vækst og innovation i dataøkonomien og gennemførelsen af grænseoverskridende offentlige tjenester kan hæmmes af hindringer for den frie udveksling af data i EU, f.eks. i form af uberettigede datalokaliseringskrav, som de offentlige myndigheder har fastsat. Med datalokaliseringsforanstaltninger genindføres der i praksis digital "grænsekontrol"[11]. De spænder fra tilsynsmyndighedernes krav om, at finansielle tjenesteydere lagrer deres data lokalt, til gennemførelsen af reglerne om tavshedspligt, som indebærer lokal lagring eller behandling, og omfattende bestemmelser, der kræver lokal lagring af arkiverede oplysninger, der stammer fra den offentlige sektor, uanset hvor følsomme de er.

Bekymringerne vedrørende beskyttelsen af fortrolige oplysninger er legitime, men bør ikke anvendes af de offentlige myndigheder som begrundelse for at begrænse den frie udveksling af data på en uberettiget måde. Som anført ovenfor udgør den generelle forordning om databeskyttelse en samlet lovgivning med en høj grad af beskyttelse af personoplysninger i hele EU. Det styrker forbrugernes tillid til onlinetjenester og sikrer en ensartet anvendelse af reglerne i alle medlemsstater gennem stærkere nationale databeskyttelsesmyndigheder. Den generelle forordning om databeskyttelse fremmer den nødvendige tillid til databehandling og er grundlaget for fri udveksling af personoplysninger i EU. Den generelle forordning om databeskyttelse indeholder

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

[11] OECD, "Emerging Policy Issues: Localisation Barriers to Trade", 2015, og igangværende arbejde.

desuden forbud mod begrænsninger af den frie udveksling af personoplysninger i Unionen, hvis disse begrænsninger er baseret på årsager, der vedrører beskyttelsen af personoplysninger[12]. Imidlertid er begrænsninger, som er baseret på andre årsager end beskyttelsen af personoplysninger, f.eks. lovgivning om beskatning eller regnskabsaflæggelse, ikke omfattet af den generelle forordning om databeskyttelse. Desuden er ikke-personoplysninger, dvs. data, der ikke vedrører en identificeret eller identificerbar fysisk person[13], fortsat ikke omfattet af anvendelsesområdet for den generelle forordning om databeskyttelse og kan vedrøre f.eks. ikke-personlige maskingenererede data.

Der kan opstå restriktioner for datalokalisering som følge af retsforskrifter eller administrative retningslinjer eller praksis, der kræver lagring eller behandling af data[14] i en elektronisk form[15], der er begrænset til et bestemt geografisk område eller en bestemt jurisdiktion. Undertiden indføres der begrænsninger af medlemsstaterne i den tro, at tilsynsmyndighederne lettere kan kontrollere lokalt lagrede data. Lokalisering bruges også som indikator for garantier med hensyn til privatlivets fred, revision og retshåndhævelse samt datasikkerhed. I praksis bidrager disse foranstaltninger dog sjældent til de mål, de tager sigte på at nå.

Informationssikkerhed afhænger af en række faktorer, ud over hvor dataene rent fysisk er lagret, f.eks. bevarelse af dataenes fortrolighed og integritet, når de er tilgængelige uden for lagerfaciliteten. I denne forbindelse er det, som reelt skaber muligheder inden for sikker datalagring og -behandling, ikke så meget restriktioner for datalokalisering, men derimod aktuel bedste praksis inden for IKT-forvaltning på et plan, der rækker langt ud over individuelle systemer. For at sikre, at data opbevares i sikkerhed for lokaliserede naturkatastrofer eller cyberangreb, kan datalagringsfaciliteter i forskellige medlemsstater f.eks. supplere hinanden og udnytte de tekniske og organisatoriske foranstaltninger, der er omhandlet i direktivet om sikkerhed for net- og informationssystemer[16] (NIS-direktivet). Desuden vil disponibiliteten af data til regulerings- eller tilsynsmæssige formål, som der ikke på nogen måde stilles spørgsmålstegn ved, blive sikret bedre ved at styrke samarbejdet mellem de nationale myndigheder indbyrdes eller mellem disse myndigheder og den private sektor end ved lokaliseringsrestriktioner. På områder, der er

---

12 Artikel 1, stk. 3. F.eks. vil en dynamisk IP-adresse, der registreres af en udbyder af onlinemedietjenester, når en person besøger et websted, som udbyderen gør tilgængelig for offentligheden, blive betragtet som personoplysninger i forhold til den nævnte udbyder, når vedkommende råder over de retlige midler, der gør det muligt at identificere den registrerede med yderligere data, som udbyderen af internettjenester har om den pågældende person. Se dom i sag C-582/14, Breyer, ECLI:EU:C:2016:779, præmis 49.

13 Som defineret i artikel 4,stk. 1, i den generelle forordning om databeskyttelse.

14 Både privatejede og offentligt ejede data.

15 Herunder kopier af datasæt.

16 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EUT L 194 af 19.7.2016, s. 1.

præget af et tæt samarbejde mellem tilsynsmyndigheder, f.eks. finansielle tjenesteydelser, kan datalokaliseringskrav nemlig vise sig at virke mod hensigten[17].

Datalokaliseringskrav kan dog være berettigede og forholdsmæssige i bestemte sammenhænge eller i relation til visse data, navnlig før der indføres et effektivt grænseoverskridende samarbejde, f.eks. ved at der sikres en sikker behandling af visse data vedrørende kritisk energiinfrastruktur, eller adgang til elektroniske beviser (f.eks. lokaliserede kopier af datasæt) for retshåndhævende myndigheder eller lokal lagring af data i visse offentlige registre.

Desværre går tendensen både på verdensplan og i Europa i retning af mere datalokalisering, ofte baseret på den fejlagtige opfattelse, at lokaltilpassede tjenester automatisk er sikrere end grænseoverskridende tjenester. Desuden er datatjenestemarkedet stærkt mærket af manglen på gennemsigtige regler og en stærk opfattelse af, at der er behov for at lokalisere data. Det kan medføre, at virksomheder og organisationer i den offentlige sektor kun får begrænset adgang til billigere og mere innovative datatjenester, eller at virksomhederne tvinges til at operere på tværs af grænserne for at håndtere overskydende datalagrings- og databehandlingskapacitet. Det vil også kunne hæmme datadrevne virksomheder, navnlig nystartede virksomheder og SMV'er, i deres bestræbelser for at øge deres aktiviteter, trænge ind på nye markeder (f.eks. ved at skulle investere i datacentre i 28 medlemsstater) eller centralisere data- og analysekapacitet med henblik på at udvikle nye produkter og tjenester.

I øjeblikket er 84 % af den endelige efterspørgsel i Europa rettet mod "IKT-relaterede" tjenester (rådgivning, hosting, udvikling) internt i EU. Hvis disse tjenester også kan operere på tværs af grænserne inden for EU, ved at datalokaliseringsrestriktionerne fjernes, kan dette medføre BNP-gevinster på op til 8 mia. EUR om året i omkostningsbesparelser og effektivitetsgevinster[18].

Datalokalisering lægger også hindringer i vejen for en større udbredelse af cloud-lagring og -computing. Dette vil også kunne få bredere samfundsmæssige virkninger. En mere effektiv udnyttelse af IKT-ressourcer kan bidrage til at nedbringe energiforbruget og kulstofemissionerne med mindst 30 % netto. En lille virksomhed, der går over til cloudcomputing, kan mindske sit energiforbrug og sine kulstofemissioner med mere end 90 % ved at lade sine erhvervsapplikationer fungere via en cloud i stedet for gennem sin egen infrastruktur. Det globale energieffektive datacentermarked forventes at vokse til næsten 90 mia. EUR frem til udgangen af 2020. Et fragmenteret datatjenestemarked vil forhindre, at disse mere energieffektive tjenester udvikles fuldt ud i EU, og vil også kunne medføre risiko for at hæmme viljen til at investere.

Med henblik på at løse ovennævnte problemer og begrænsninger og udnytte det fulde potentiale i den europæiske dataøkonomi, bør alle medlemsstaternes tiltag, der påvirker

---

[17] En række af EU's bestemmelser om finansielle tjenesteydelser og det europæiske finanstilsynssystem kræver, at tilsynsmyndighederne har adgang til data om finansielle institutioner og transaktioner i hele EU's område. Krav om, at data skal opbevares i et bestemt nationalt område, eller om betingelserne for den tilsynsmæssige adgang til administrative procedurer kan mindske tilsynsmyndighedernes adgang til data, som er væsentlige for, at de kan varetage deres opgaver.

[18] "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", ECIPE, 2016, beregning baseret på øget konkurrencepres under vilkår med fuldt ud prisgennemsigtig "industriel" efterspørgselsstyring.

datalagring eller -behandling, styres af et "**princip om fri udveksling af data inden for EU**" som en naturlig følge af deres forpligtelser inden for rammerne af traktatens bestemmelser om fri udveksling af tjenesteydelser og fri etableringsret og den relevante afledte lovgivning. De nuværende eller nye restriktioner for datalokalisering skal være nøje begrundet i henhold til traktaten og relevant afledt ret, så det sikres, at de er nødvendige og rimelige for at nå et overordnet mål af almen interesse såsom den offentlige sikkerhed[19].

Princippet om fri udveksling af personoplysninger[20], der er nedfældet i primær og afledt ret, bør også finde anvendelse i tilfælde, hvor den generelle forordning om databeskyttelse giver medlemsstaterne ret til at regulere særlige spørgsmål. Medlemsstaterne bør tilskyndes til ikke at gøre brug af de indledende bestemmelser i den generelle forordning om databeskyttelse med henblik på at indføre yderligere restriktioner for frie datastrømme.

I sine konklusioner af 15. december 2016 opfordrede Det Europæiske Råd til, at de resterende hindringer på det indre marked, herunder hindringerne for frie datastrømme, fjernes[21].

Med henblik på at gennemføre princippet om fri udveksling af data vil Kommissionen tage følgende to skridt:

- Efter offentliggørelsen af denne meddelelse vil Kommissionen indlede strukturerede dialoger med medlemsstaterne og andre interessenter om begrundelsen for og proportionaliteten af datalokaliseringsforanstaltninger, med udgangspunkt i de begrænsninger, som Kommissionen hidtil har konstateret.

- På baggrund af resultaterne af dialogerne og efter yderligere indsamling af dokumentation om omfanget og arten af restriktioner for datalokalisering og konsekvenserne deraf, navnlig for SMV'er og nystartede virksomheder (bl.a. gennem den ledsagende offentlige høring), vil Kommissionen, hvis der er behov for det, indlede traktatbrudsprocedurer for at tage fat på problemet med uberettigede eller uforholdsmæssige datalokaliseringsforanstaltninger og, hvis det er nødvendigt, også tage yderligere initiativer vedrørende frie datastrømme. I den sammenhæng vil eventuelle opfølgninger blive foretaget i overensstemmelse med principperne om bedre regulering.

[19] Under hensyntagen til, at de traktatfæstede undtagelser skal fortolkes restriktivt. En sådan relevant afledt ret omfatter den generelle forordning om databeskyttelse, direktiv 2000/31/EF (direktivet om e-handel), direktiv 2006/123/EF (servicedirektivet), og, for så vidt angår udkast til tekniske forskrifter og regler om informationssamfundets tjenester, direktiv 2015/1535 (gennemsigtighedsdirektivet).

[20] Bestemmelserne om den frie udveksling af personoplysninger findes i artikel 16 i traktaten om Den Europæiske Unions funktionsmåde, og reglerne for den frie udveksling af personoplysninger er fastsat i EU's gældende og fremtidige lovgivning om databeskyttelse. Artikel 1, stk. 3, i den generelle forordning om databeskyttelse fastlægger: "Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger."

[21] http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/

3. DATAADGANG OG -OVERFØRSEL

Stadig større mængder data genereres af maskiner eller processer, der er baseret på nye teknologier såsom tingenes internet. Disse data bruges i stigende omfang som nøglekomponenter i nye, innovative tjenester for at forbedre produkter eller produktionsprocesser og til støtte for beslutningstagningen.

Mangfoldigheden af data, der genereres af disse maskiner eller processer, giver aktørerne på datamarkedet store muligheder for at innovere og anvende indsigten i disse data. F.eks. vil data indhentet af sensorer, der anvendes i moderne landbrug, kunne anvendes til at skabe en applikation til høstoptimering, eller data, der genereres via sensorer i trafiklys, kunne anvendes til at skabe en applikation til trafikstyring eller ruteoptimering.

For at opnå størst mulig værdi af denne type data skal markedsaktørerne have adgang til store og forskelligartede datasæt. Dette vil dog blive vanskeligere at opnå, hvis datageneratorerne holder dataene for sig selv, og dataene derfor analyseres i siloer. Spørgsmålene om adgang og overførsel i relation til rådata (dvs. data, som ikke er blevet behandlet eller ændret efter registrering), der genereres af disse maskiner eller processer, er derfor af central betydning for udviklingen af en dataøkonomi og kræver en omhyggelig vurdering.

Spørgsmålet om adgang til maskingenererede data er under overvejelse i flere sektorer som f.eks. transport, energimarkeder, intelligente levemiljøer og sundheds- og plejesektoren.

Før undersøgelsen af den nuværende situation med hensyn til dataadgang i EU er det vigtigt at præcisere, hvilke typer data der behandles i denne kontekst.

3.1. Datatyper under overvejelse

Generelt kan data være personoplysninger eller ikke-personoplysninger. F.eks. kan data, der genereres af temperaturfølere i hjemmene, være af personlig karakter, hvis de kan relateres til en levende person, mens data om jordens fugtighed ikke er personlige. Personoplysninger kan omdannes til ikke-personoplysninger via anonymisering. Hvis data betragtes som personoplysninger[22], finder databeskyttelsesreglerne, navnlig den generelle forordning om databeskyttelse, anvendelse.

Maskingenererede data skabes uden direkte intervention fra menneskers side af computere, applikationer eller tjenester eller af sensorer, der behandler oplysninger modtaget fra udstyr, software eller materiel, uanset om de er virtuelle eller reelle.

Maskingenererede data kan være af personlig eller ikke-personlig art. Hvis maskingenererede data gør det muligt at identificere en fysisk person, betragtes de som personoplysninger med den konsekvens, at alle bestemmelserne om personoplysninger skal gælde, indtil de er blevet fuldt ud anonymiserede (f.eks. lokaliseringsdata fra et mobile applikationer).

[22] Som defineret i artikel 4, stk. 1, i den generelle forordning om databeskyttelse.

Et fælles tema, som sammenkæder den frie datastrøm med de nye spørgsmål om adgang og transmission af data, er, at virksomheder og aktører i dataøkonomien vil skulle behandle både personoplysninger og ikke-personoplysninger, og at datastrømme og datasæt jævnligt indeholder begge typer. Der skal ved alle politiske foranstaltninger tages hensyn til denne økonomiske realitet og de retlige rammer for beskyttelse af personoplysninger, samtidig med at de enkelte personers grundlæggende rettigheder respekteres.

3.2. Begrænset adgang til data

For at man kan vurdere dette nye spørgsmål, er det først nødvendigt at analysere, hvordan virksomheder og andre markedsaktører kan få adgang til de store og forskelligartede datasæt, der er behov for i dataøkonomien.

Den foreliggende dokumentation[23] viser, at virksomheder, der ligger inde med store mængder data, generelt har tendens til mest at benytte intern dataanalysekapacitet. I de fleste tilfælde kan data genereres og analyseres af samme virksomhed, og selv hvis en dataanalyse gives i underentreprise, genanvendes dataene undertiden ikke yderligere. I visse tilfælde er det sådan, at producenter, virksomheder, der tilbyder tjenester, eller andre markedsaktører, som ligger inde med data, holder de data, der genereres af deres maskiner eller gennem deres produkter og tjenesteydelser, for sig selv og dermed potentielt begrænser genanvendelse på markederne i de efterfølgende led. Mange virksomheder høster ikke fordel af eller giver ikke mulighed for brugervenlige programmeringsgrænseflader for applikationer (API)[24] (med angivelse af, hvordan forskellige applikationer skal interagere med hinanden), der kan tjene som sikre indgangsdøre til nye og innovative anvendelser af de data, virksomhederne ligger inde med.

Samlet set er udvekslingen af data på nuværende tidspunkt derfor fortsat begrænset. Datamarkederne er langsomt ved at skyde op, men anvendes endnu ikke i udbredt grad. Virksomhederne er undertiden ikke udstyret med de rette værktøjer og færdigheder til at kvantificere den økonomiske værdi af deres data, og de kan frygte at miste eller kompromittere deres konkurrencemæssige fordel, når konkurrenterne får adgang til data.

3.3. Maskingenererede rådata: Retlig situation på EU-plan og nationalt plan

Maskingenererede rådata ikke er beskyttet af de gældende intellektuelle ejendomsrettigheder, da de ikke anses for at være resultatet af en intellektuel indsats og/eller har en grad af originalitet. Sui generis-retten i databasedirektivet (96/9/EF) – som giver fremstillere af databaser retten til at forbyde udtræk og/eller genanvendelse af hele basens indhold eller en væsentlig del deraf – kan kun yde beskyttelse på den betingelse, at oprettelsen af en sådan database indebærer en væsentlig investering i indsamling, kontrol eller præsentation af dens indhold. Det nyligt vedtagne direktiv om beskyttelse af forretningshemmeligheder (2016/943/EU), der skal være gennemført i national

23 IDC, European Data Market Study, First Interim Report, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, First interim report, 2016; GD CONNECT-konference på højt plan, den 17. oktober 2016.

24 F.eks. https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

lovgivning senest i juni 2018, vil beskytte forretningshemmeligheder mod ulovlig erhvervelse, brug og videregivelse. For at data kan betragtes som en "forretningshemmelighed", skal der træffes foranstaltninger til at beskytte den fortrolige karakter af information, der udgør "virksomhedens intellektuelle kapital".

I henhold til lovgivningen i forskellige medlemsstater anvendes retskravene kun på data, hvis disse data opfylder specifikke betingelser for at kunne komme i betragtning som f.eks. en intellektuel ejendomsret, en databaserettighed eller en forretningshemmelighed. På EU-plan vil maskingenererede rådata som sådan dog ikke generelt opfylde de relevante betingelser.

Derfor findes der i øjeblikket ingen omfattende politikrammer på nationalt plan eller EU-plan i forbindelse med maskingenererede rådata, som ikke kan betragtes som personoplysninger, eller vedrørende betingelserne for økonomisk udnyttelse af og handel med sådanne data. Spørgsmålet er i høj grad overladt til kontraktbaserede løsninger. Anvendelsen af de eksisterende generelle aftale- og konkurrenceretlige instrumenter, man har i EU, er måske en tilstrækkelig løsning. Derudover kunne man forestille sig frivillige aftaler eller paraplyaftaler, der dækker visse sektorer. Hvis de forskellige markedsdeltagere ikke har samme forhandlingsstyrke, vil det dog muligvis ikke være tilstrækkeligt alene med markedsbaserede løsninger til at sikre retfærdige og innovationsvenlige resultater, lette adgangen for nye markedsdeltagere og undgå situationer med fastlåsning.

3.4. Situationen i praksis

I visse tilfælde kan producenter eller tjenesteydere *de facto* blive "ejere" af data, som deres maskiner eller processer genererer, også selv om de pågældende maskiner ejes af brugeren. En *de facto*-kontrol over disse data kan være en differentieringsfaktor og en konkurrencemæssig fordel for producenterne. Dette kan dog være problematisk, fordi producenten ofte forhindrer brugeren i at tillade, at en anden part kan anvende dataene.

De forskellige markedsaktører, som har kontrol over dataene, kan afhængigt af markedernes specificiteter således udnytte huller i lovgivningen eller de retlige usikkerhedsmomenter, der er beskrevet ovenfor, ved at påtvinge brugerne urimelige standardkontraktvilkår eller ved at benytte tekniske midler som f.eks. beskyttede formater eller kryptering. Selv om flere medlemsstater har udvidet anvendelsesområdet for forbrugerbeskyttelsesdirektivet om urimelige kontraktvilkår til også at omfatte B2B-transaktioner, er det ikke alle, som har gjort det. Dette vil f.eks. kunne resultere i, at brugere og virksomheder bliver fastlåst i eksklusive dataudnyttelsesordninger. Der vil eventuelt kunne opnås frivillig udveksling af data, men forhandlingerne om sådanne kontrakter kan indebære store transaktionsomkostninger for de svagere parter, når der er tale om en ulige forhandlingsposition, eller der skal afholdes betydelige omkostninger til juridisk ekspertise.

3.5. En fremtidig EU-ramme for dataadgang

Visse medlemsstater i færd med at undersøge mulighederne for at sikre adgang til maskingenererede data og vil muligvis beslutte selv at regulere dette spørgsmål. En ukoordineret tilgang risikerer at skabe fragmentering og vil skade udviklingen af EU's

dataøkonomi og anvendelsen af datatjenester og -teknologier på tværs af grænserne i det indre marked.

Derfor agter Kommissionen at indlede en dialog med medlemsstaterne og andre interessenter for at undersøge mulighederne for en eventuel fremtidig EU-ramme for dataadgang. Kommissionen mener, at denne dialog bør omhandle de mest effektive måder til at nå følgende mål:

- **Forbedre adgangen til anonyme maskingenererede data**: Gennem udveksling, genanvendelse og aggregering bliver maskingenererede data en kilde til værditilvækst, innovation og mangfoldighed af forretningsmodeller[25].

- **Lette og fremme udvekslingen af sådanne data**: Enhver fremtidig løsning bør fremme en effektiv adgang til data, idet der f.eks. tages hensyn til eventuelle forskelle i forhandlingsstyrke mellem markedsaktørerne.

- **Beskytte investeringer og aktiver**: Ved enhver fremtidig løsning bør der også tages hensyn til de legitime interesser hos markedsdeltagere, der investerer i produktudvikling, således at de sikres et rimeligt afkast på deres investeringer og dermed bidrager til innovation. Samtidig bør enhver fremtidig løsning sikre en retfærdig deling af fordele mellem dataindehavere[26], databehandlere og applikationsudbydere inden for værdikæder.

- **Undgå videregivelse af fortrolige data**: I forbindelse med enhver fremtidig løsning bør man mindske risikoen for at videregive fortrolige data, navnlig til eksisterende eller potentielle konkurrenter. I den sammenhæng bør det også være muligt at gennemføre en egentlig dataklassificering forud for vurderingen af, hvorvidt et bestemt dataelement kan udveksles.

- **I videst muligt omfang undgå fastlåsning**: Der bør tages hensyn til virksomhedernes og privatpersonernes ulige forhandlingsstyrke. Der bør undgås situationer med fastlåsning, navnlig for SMV'er og nystartede virksomheder og privatpersoner.

I dialogerne med interessenterne agter Kommissionen at drøfte følgende muligheder for at løse spørgsmålet om adgang til maskingenererede data, der er forskellige mht. interventionsgrad:

- **Retningslinjer for tilskyndelse af virksomheder til at udveksle data**: For at afbøde virkningerne af divergerende nationale regler og give virksomhederne større retssikkerhed vil Kommissionen kunne udstede retningslinjer for, hvordan kontrolrettighederne for ikke-personoplysninger bør behandles i kontrakter. Disse retningslinjer vil blive baseret på gældende lovgivning, navnlig kravene om gennemsigtighed og rimelighed i EU's markedsførings- og forbrugerlovgivning, direktivet om forretningshemmeligheder og lovgivningen om ophavsret, navnlig databasedirektivet. Kommissionen har til hensigt at iværksætte en evaluering af databasedirektivet i 2017.

[25] Hvis der er tale om personoplysninger, finder den generelle forordning om databeskyttelse anvendelse.

[26] Den enhed, der i praksis forvalter og opbevarer de maskingenererede data.

- **Fremme af udviklingen af tekniske løsninger for pålidelig identifikation og udveksling af data**: Sporbarhed og klar identifikation af datakilder er en forudsætning for en reel kontrol af data på markedet. Det kan være nødvendigt at definere pålidelige og eventuelt standardiserede protokoller for varig identifikation af datakilder for at skabe tillid til systemet. Programmeringsgrænseflader for applikationer (API) kan også fremme oprettelsen af et økosystem af applikations- og algoritmeudviklere, der er interesserede i de data, som virksomhederne har. API'er kan hjælpe virksomhederne og de offentlige myndigheder med at identificere og udnytte forskellige former for genanvendelse af de data, de ligger inde med. På dette grundlag kan der overvejes en bredere anvendelse af åbne, standardiserede og veldokumenterede API ved hjælp af teknisk vejledning, herunder identifikation og udbredelse af bedste praksis for virksomheder og offentlige organer. Dette vil også kunne omfatte, at der stilles data til rådighed i maskinlæsbart format og tilvejebringes tilknyttede metadata.

- **Standardkontraktregler**: Via standardregler vil man kunne fastlægge en afbalanceret benchmarkløsning for kontrakter vedrørende data, idet der også tages behørigt hensyn til den igangværende kvalitetskontrol af, hvordan direktivet om urimelige kontraktvilkår generelt fungerer. Sådanne regler vil kunne kombineres med indførelsen af en kontrol af urimelige betingelser i B2B-kontraktforhold[27], som ville føre til ugyldiggørelse af kontraktbestemmelser, som afviger væsentligt fra standardreglerne. De kan også suppleres af et sæt anbefalede standardkontraktvilkår, der er udarbejdet af interessenterne. Denne tilgang kan reducere de juridiske hindringer for små virksomheder og mindske uligevægten i forhandlingspositioner, samtidig med at den giver mulighed for en høj grad af aftalefrihed.

- **Adgang af hensyn til samfundets interesse og videnskabelige formål**: Offentlige myndigheder vil kunne få adgang til data, hvis det er i "almenhedens interesse" og i høj grad vil forbedre den offentlige sektors funktion, f.eks. hvis statistiske kontorer har adgang til forretningsoplysninger, eller trafikstyringssystemer optimeres på grundlag af realtids-data fra private køretøjer. Statistikmyndighedernes adgang til forretningsoplysninger vil typisk bidrage til at lette det statistiske indberetningsarbejde for de erhvervsdrivende. På samme måde er det for den videnskabelige forskning afgørende at have adgang til og mulighed for at kombinere data fra forskellige kilder på områder som f.eks. læge-, samfunds- og miljøvidenskab.

- **Dataproducenters rettigheder**: "Dataproducenten", dvs. ejeren eller langtidsbrugeren (dvs. leasingtageren) af udstyret, kan eventuelt gives en ret til at anvende og tillade anvendelsen af ikke-personoplysninger. Denne tilgang tager sigte på at afklare den retlige situation og give dataproducenten flere valgmuligheder ved at åbne mulighed for, at brugerne kan anvende deres data og dermed bidrage til at frigøre maskingenererede data. Imidlertid vil de relevante undtagelser skulle angives klart, især hvad angår producentens eller de offentlige myndigheders ikke-eksklusive adgang til dataene, f.eks. til trafikstyring eller af

[27]. Naturligvis skal benchmarket for urimelige betingelser for B2B være forskelligt fra B2C-aftaler for at afspejle den højere grad af aftalefrihed i B2B-forbindelser.

miljømæssige årsager. Hvis der er tale om personoplysninger, vil enkeltpersoner bevare deres ret til at trække deres samtykke tilbage på et hvilket som helst tidspunkt, efter at de har tilladt anvendelsen. Personoplysningerne vil skulle anonymiseres på en sådan måde, at den enkelte ikke eller ikke længere kan identificeres, inden den anden part kan tillade den videre anvendelse. Den generelle forordning om databeskyttelse gælder således fortsat for alle personoplysninger (uanset om de er maskingenererede eller ej), indtil disse data er blevet anonymiseret.

- **Adgang mod betaling**: En ramme, der potentielt er baseret på visse nøgleprincipper som f.eks. fair, rimelige og ikkediskriminerende (FRAND) vilkår, vil kunne udvikles for dataindehavere såsom producenter, tjenesteydere eller andre parter for at give adgang til de data, de ligger inde med, mod betaling efter anonymisering. Det vil være nødvendigt at tage hensyn til relevante legitime interesser samt behovet for at beskytte forretningshemmeligheder. Der kan også overvejes forskellige adgangsordninger for forskellige sektorer og/eller forretningsmodeller for at tage hensyn til specificiteterne i hver enkelt sektor. F.eks. kan der i visse tilfælde foretrækkes (fuldstændig eller delvis) fri adgang til data for både virksomhederne og samfundet.

Kommissionen vil høre interessenterne om de spørgsmål, der er skitseret ovenfor, med henblik på at indsamle flere oplysninger om, hvordan datamarkederne fungerer i de enkelte sektorer, og undersøge løsningsmuligheder. I den sammenhæng er det væsentligt med en bred debat på makroniveau for at drøfte løsningsmuligheder og undgå utilsigtede bivirkninger, som kan hæmme innovation eller forhindre konkurrence. Desuden vil der blive afholdt sektorspecifikke drøftelser med relevante interessenter i dataværdikæden.

4. ANSVAR

Et andet nyt spørgsmål vedrører anvendelsen af de nuværende regler om ansvar i dataøkonomien i forbindelse med produkter og tjenesteydelser baseret på nye teknologier som f.eks. tingenes internet, fremtidens fabrikker og autonome netforbundne systemer. Tingenes internet er et hastigt voksende netværk af hverdagsgenstande såsom ure, køretøjer og termostater, som er tilsluttet internettet. Autonome netforbundne systemer, f.eks. selvkørende køretøjer, fungerer uafhængigt af mennesker og er i stand til at forstå og fortolke de omgivende miljøer. Disse nye teknologier benytter sensorer til at levere de mange typer data, der ofte kræves, for at produktet eller tjenesten kan fungere.

Alle disse innovationer vil sandsynligvis bidrage til større sikkerhed og livskvalitet, men det kan ikke undgås, at der fortsat er risiko for udformningsfejl, fejlfunktion eller konstruktionsfejl i hvert stykke udstyr. Dette kan skyldes transmission af ukorrekte data fra en sensor, f.eks. på grund af softwarefejl, problemer med netforbindelsen eller ukorrekt drift. Disse systemer er af en sådan art, at det kan være vanskeligt at fastslå den nøjagtige årsag til et problem, der forårsager skader, hvilket rejser spørgsmålet om, hvordan man sikrer, at disse systemer er sikre for brugerne med henblik på at mindske problemet med skader, og hvem der skal holdes ansvarlig for en skade, hvis den alligevel opstår.

Spørgsmålet om, hvordan man kan skabe større sikkerhed for både brugere og producenter af sådant udstyr, for så vidt angår deres potentielle ansvar, er derfor af central betydning i udviklingen af en dataøkonomi.

4.1. EU-regler om ansvar

I civilretlig sammenhæng sondres der generelt mellem to former for retligt ansvar: ansvar i kontraktforhold, hvor ansvaret for skaden udløses af kontraktforholdet mellem parterne; og ansvar uden for kontraktforhold[28], hvor ansvarsforpligtelserne er fastlagt uden for en kontrakt. En vigtig form for ansvar uden for kontraktforhold er den, der vedrører produktansvar. På EU-plan er der i direktivet om produktansvar (85/374/EØF) ("produktansvarsdirektivet") fastlagt et princip om objektivt ansvar, dvs. ansvar uden culpa: Hvis et defekt produkt påfører en forbruger en skade, kan producenterne pålægges ansvaret, også selv om de ikke har gjort sig skyldige i nogen forsømmelse eller fejl. Det kan dog være vanskeligt eller uklart, hvordan bestemmelserne i dette direktiv[29] skal anvendes i forbindelse med tingenes internet og autonome netforbundne systemer (f.eks. robotteknologi) af følgende årsager: Disse systemer har visse særlige kendetegn, f.eks. en kompliceret produkt- eller tjenesteværdikæde, med indbyrdes afhængighedsforhold mellem leverandører, producenter og andre tredjeparter; der består en vis usikkerhed med hensyn til den retlige karakter af tingenes internet, dvs. om der er tale om produkter, tjenester eller produkter i tilknytning til salget af en tjeneste; og det forhold, at disse teknologier er kendetegnet ved autonomi.

Kommissionen har lanceret en omfattende evaluering af produktansvarsdirektivet for at vurdere, hvordan det generelt fungerer, og hvorvidt reglerne, som blev udformet til meget anderledes forhold, stadig er hensigtsmæssige for nye teknologier som f.eks. tingenes internet og autonome netforbundne systemer.

4.2. Mulige veje frem

Det er Kommissionens mål at øge retssikkerheden med hensyn til ansvar i forbindelse med nye teknologier og dermed skabe gunstige betingelser for innovation. Ud over status quo[30] kan der kigges på forskellige tilgange, bl.a.:

- **Tilgange vedrørende risikoskabelse eller risikoforvaltning**: Inden for rammerne af disse tilgange kan man f.eks. lægge ansvaret på de markedsaktører, der skaber en større risiko for andre, eller på de markedsaktører, der er bedst stillede til at begrænse eller undgå, at sådanne risici bliver til virkelighed.

- **Frivillige eller obligatoriske forsikringsordninger**: Ovennævnte tilgange for ansvar kan eventuelt kobles sammen med sådanne ordninger. De skal sikre

[28] EU-reglerne om ansvar vedrører kun ansvarsforpligtelser uden for kontraktforhold.

[29] Der henvises til producenters objektive ansvar i tilfælde af defekte produkter i andre dele af lovgivningen om produktsikkerhed, f.eks. direktivet om radioudstyr (2014/53/EU), reglerne om medicinsk udstyr, maskindirektivet (2006/42/EF) og direktivet om produktsikkerhed i almindelighed (2001/95/EF).

[30] Kommissionen kan udstede retningslinjer for anvendelsen af EU-reglerne om ansvar, hvad angår tingenes internet og robotteknologi.

kompensation til de parter, som har lidt skade (f.eks. forbrugeren). Der skal i forbindelse med denne tilgang sikres retssikkerhed for de investeringer, der foretages af virksomheder, samtidig med at ofre får en vis sikkerhed for en rimelig kompensation eller passende forsikring i tilfælde af skader.

Der skal i forbindelse med alle tilgange tages hensyn til de aktiviteter, der udføres af den enkeltperson, som benytter teknologien, og nærmere bestemt skal det klart fastlægges, hvilken rolle brugerne af den pågældende teknologi skal have.

Kommissionen vil høre interessenternes mening om, hvorvidt de nuværende EU-regler for ansvar i forbindelse med tingenes internet og autonome netforbundne systemer er hensigtsmæssige, og hvilke metoder der eventuelt kan benyttes til at overvinde de nuværende vanskeligheder med at tildele ansvar. Sideløbende hermed gennemføres der også en offentlig høring om den generelle vurdering af anvendelsen af produktansvarsdirektivet. Kommissionen vil vurdere resultaterne og overveje mulighederne for fremtidige tiltag.

5. PORTABILITET, INTEROPERABILITET OG STANDARDER

Andre nye spørgsmål i dataøkonomien er portabilitet af ikke-personoplysninger, interoperabilitet mellem tjenester for at muliggøre dataudveksling samt hensigtsmæssige tekniske standarder for gennemførelse af meningsfuld portabilitet.

5.1. Portabilitet af ikke-personoplysninger

Dataportabilitet betyder, at forbrugere og virksomheder let kan tage deres data fra et system til et andet. I dataøkonomien er det at skifte system generelt forbundet med lave omkostninger og dermed med lave adgangsbarrierer. Den generelle forordning om databeskyttelse vil give enkeltpersoner ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger, der gives udbyderen, samt ret til at transmittere dem til en anden udbyder[31].

Hvad angår ikke-personoplysninger er der i øjeblikket ingen forpligtelser til at sikre blot et minimumsniveau af dataportabilitet, selv for bredt anvendte onlinetjenester såsom cloudhosting. Dette skyldes delvis, at kravene for gennemførelse af dataportabilitet kan være teknisk krævende og dyre, da forskellige udbydere af samme tjenester kan lagre data forskelligt.

Hvis portabiliteten af ikke-personoplysninger skal være meningsfuld, vil der også skulle tages hensyn til mere generelle overvejelser om datastyring, herunder gennemsigtighed for brugere, styret adgang samt interoperabilitet for at sammenkæde forskellige platforme på en måde, der stimulerer innovation.

[31] Artikel 20.

5.2. Interoperabilitet

Ofte er overvejelserne om dataportabilitet knyttet nøje sammen med spørgsmål om interoperabilitet mellem data, der gør det muligt for flere digitale tjenester at udveksle data uden problemer og ved hjælp af passende tekniske specifikationer. Direktivet om den offentlige sektors informationer og dertil hørende retningslinjer (herunder den europæiske interoperabilitetsramme) understreger betydningen af rige, standardiserede metadata, der følger etablerede vokabularer med henblik på at lette søgning og interoperabilitet. Direktivet om infrastrukturen for geografisk information i Det Europæiske Fællesskab (Inspire) og dets bestemmelser om interoperabilitet og retningslinjer for geodatatjenester og geodata, herunder sensorobservationsdata, gælder i øjeblikket for den offentlige sektors geodata[32].

Hvad angår onlineplatforme, letter en sådan datainteroperabilitet ikke blot skift, men også en samtidig anvendelse af flere platforme (såkaldt "multihoming") samt omfattende dataudveksling mellem platforme, hvilket indebærer et potentiale til at fremme innovation i den digitale økonomi.

5.3. Standarder

Hvis politikkerne for dataportabilitet skal være effektive, skal de understøttes af passende tekniske standarder for at gennemføre en meningsfuld portabilitet på en teknologisk neutral måde. Kommissionen har forpligtet sig[33] til at støtte passende standarder for at forbedre interoperabiliteten, portabiliteten og sikkerheden i forbindelse med cloud-tjenester ved bedre at integrere det arbejde, der gøres i open sourcesamfund, i standardiseringsprocessen på europæisk plan. Som eksempler på en sådan tilgang kan nævnes TOSCA-specifikationen for cloud-applikationer, som tager sigte på at øge portabiliteten og den operationelle forvaltning af cloud-applikationer og -tjenester[34], og de tekniske specifikationer og retningslinjer i gennemførelsesbestemmelserne for Inspire[35].

5.4. Mulige veje frem

Blandt de mulige veje frem for at løse ovennævnte spørgsmål kan nævnes:

- **Udvikling af anbefalede kontraktvilkår for at gøre det lettere at skifte udbydere**: Eftersom dataportabilitet og skift mellem datatjenesteudbydere er indbyrdes afhængige, kan man eventuelt overveje at udvikle standardkontraktvilkår, der forpligter udbyderen til at sikre, at en kundes data kan overføres.

[32] Maskingenererede data er "geodata", idet sensorer normalt også transmitterer deres direkte eller indirekte position (placering) sammen med deres måling.

[33] COM(2016) 176 final: IKT-standardiseringsprioriteter for det digitale indre marked.

[34] https://www.oasis-open.org/committees/tosca

[35] Inspire-lovgivningen: http://inspire.ec.europa.eu/inspire-legislation/26

- **Udbygning af retten til dataportabilitet**: På grundlag af retten til dataportabilitet i henhold til den generelle forordning om databeskyttelse og de foreslåede aftaleregler om levering af digitalt indhold kan der indføres yderligere rettigheder med hensyn til portabilitet af ikke-personoplysninger, især så de omfatter B2B-forhold, samtidig med at der tages behørigt hensyn til resultatet af den igangværende kvalitetskontrol af centrale elementer af EU's markedsførings- og forbrugerlovgivning[36].

- **Sektorspecifikke forsøg med standarder**: For at udvikle en solid tilgang til portabilitetsregler, der styres gennem standarder, kan der eventuelt iværksættes sektorspecifikke eksperimenter. Dette vil typisk omfatte samarbejde mellem mange forskellige interessenter, herunder standardiseringsorganer, industrien, tekniske kredse og offentlige myndigheder.

Kommissionen vil høre de interesserede parter om disse spørgsmål og på grundlag deraf afgøre, om der kræves yderligere tiltag, eventuelt i form af ovennævnte foranstaltninger, enten individuelt eller i kombination.

6. EKSPERIMENTERING OG TEST

Eksperimentering er en vigtig del af udforskningen af de nye spørgsmål i dataøkonomien. Det vil blive undersøgt, om der er mulighed for at anvende Horisont 2020 til at støtte denne form for test og eksperimenter.

Før der drages konklusioner om, hvorvidt de eventuelle løsninger for dataadgang og ansvar er egnede, bør der organiseres en specifik afprøvning for at teste de pågældende spørgsmål i praksis, i partnerskab med interesserede parter. Der er behov for en europæisk løsning, som bygger på samarbejde og eksperimentering mellem medlemsstaterne.

Man kunne f.eks. overveje at benytte en sådan afprøvning for samarbejdende, netforbundet og automatiseret mobilitet[37] i betragtning af denne sektors grænseoverskridende dimension.

I flere medlemsstater er man allerede ved at iværksætte projekter for at udvikle samarbejdende systemer og højere automatiseringsgrad[38]. Disse projekter gør det muligt via net for køretøjer at være forbundet med hinanden og med vejinfrastruktur som f.eks. trafiklys eller vejskilte. Desuden har Kommissionen til hensigt at arbejde sammen med en gruppe af interesserede medlemsstater om at skabe en retlig testningsramme til udførelse af forsøgene på grundlag af harmoniserede regler om dataadgang og ansvar. For at skabe adgang til en tilstrækkelig stor mængde data, bør afprøvningerne baseres på

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

[37] Se COM (2016) 766 af 30.11.2016.

[38] Se COM (2016) 766: En europæisk strategi for samarbejdende intelligente transportsystemer.

5G, der fungerer gnidningsløst sammen med teknologier, som allerede er i anvendelse, og under iagttagelse af princippet om komplementaritet[39].

En andet interessant eksperimenteringsform vil komme fra den geospatiale sektor, med fremkomsten af et nyt økosystem for data, der er bygget op omkring Copernicus - EU's jordobservationsprogram og den tredjestørste dataleverandør i verden. Kommissionen er i færd med at udvikle innovative løsninger for at fremme udviklingen af applikationer, som bygger på Copernicus og andre geodata og navnlig tager fat om spørgsmål om dataadgang, interoperabilitet og forudsigelighed.

7. KONKLUSION

For at opbygge dataøkonomien har EU brug for en politisk ramme, der gør det muligt at bruge data i hele værdikæden for videnskabelige, samfundsmæssige og industrielle formål. Med henblik herpå lancerer Kommissionen en omfattende dialog med interessenterne om de emner, som belyses i denne meddelelse. Det første skridt i denne dialog vil være en offentlig høring. Spørgsmålene om dataadgang og ansvar vil også blive testet i praksis inden for samarbejdende, netforbundet og automatiseret mobilitet.

Hvad angår fri udveksling af data, vil Kommissionen videreføre arbejdet på dette område i overensstemmelse med den tilgang, der er skitseret ovenfor, for i fuldt omfang at implementere princippet om frie datastrømme inden for EU, også ved hjælp af prioriterede håndhævelsesforanstaltninger, hvis det er nødvendigt og hensigtsmæssigt. Kommissionen vil også fortsætte med at overvåge og indsamle dokumentation og, hvis det er nødvendigt, overveje at tage yderligere initiativer om frie datastrømme.

På grundlag af resultaterne af dialogen med interessenterne vil Kommissionen også tage stilling til, om der kræves yderligere tiltag vedrørende de nye spørgsmål, og foreslå løsninger i overensstemmelse hermed. I den sammenhæng vil eksperimenter under reelle forhold kunne komme på tale.

[39] Se COM (2016) 588: 5G til Europa: En handlingsplan.