



EUROPEISKA  
KOMMISSIONEN

Bryssel den 10.1.2017  
COM(2017) 9 final

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET,  
RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT  
REGIONKOMMITTÉN**

**"ATT SKAPA EN EUROPEISK DATAEKONOMI"**

{SWD(2017) 2 final}

## ”ATT SKAPA EN EUROPEISK DATAEKONOMI”

### 1. INLEDNING

Data har blivit en viktig resurs för ekonomisk tillväxt, sysselsättning och samhällsutveckling. Genom dataanalys underlättas optimeringen av processer och beslut, innovation och möjligheten att förutse framtida händelser. Potentialen för denna globala trend är enorm inom olika områden och omfattar allt från hälsa, miljö, livsmedelssäkerhet, klimat- och resurseffektivitet till energi, intelligenta transportsystem och smarta städer.

Den så kallade *dataekonomin*<sup>1</sup> kännetecknas av ett ekosystem bestående av olika typer av marknadsaktörer – såsom tillverkare, forskare och leverantörer av infrastruktur – som samarbetar för att säkerställa att data är tillgängliga och användbara. Detta gör det möjligt för marknadsaktörerna att dra nytta av uppgifterna genom att skapa en mängd olika tillämpningar som har stor potential att förbättra det dagliga livet (inom t.ex. trafikledning, optimering av skördar eller sjukvård på distans).

Värdet av EU:s dataekonomi uppskattades till 257 miljarder euro år 2014, eller 1,85 % av EU:s BNP.<sup>2</sup> Denna siffra ökade till 272 miljarder euro år 2015, eller 1,87 % av EU:s BNP (en årlig tillväxt på 5,6 %). Enligt samma beräkningar förutspås värdet öka till 643 miljarder euro fram till 2020, vilket motsvarar 3,17 % av EU:s BNP, om de politiska och rättsliga ramarna för dataekonomin fastställs i tid.

Den allmänna dataskyddsförordningen<sup>3</sup> innebär att det från och med maj 2018 kommer att finnas en enda heltäckande uppsättning regler för hela Europa istället för dagens 28 nationella lagar. Genom det nya systemet med en enda kontaktpunkt<sup>4</sup> säkerställs att en dataskyddsmyndighet ansvarar för tillsynen av databearbetning över nationsgränserna som utförs av företag i EU. En konsekvent tolkning av de nya reglerna kommer att garanteras, och framför allt kommer, i de fall där flera nationella dataskyddsmyndigheter är involverade, ett enda beslut att fattas för att säkerställa gemensamma lösningar på gemensamma problem. Den allmänna dataskyddsförordningen kommer dessutom att skapa lika villkor för företag inom och utanför EU, eftersom företag som är baserade utanför EU kommer att vara tvungna att tillämpa samma regler som europeiska företag,

---

<sup>1</sup> Dataekonomin mäter de totala effekterna av datamarknaden – dvs. marknaden för datatjänster där digital data utbyts som produkter eller tjänster som härrör från rådata – på ekonomin i sin helhet. Den omfattar den generering, insamling, lagring, bearbetning, distribution, analys, utveckling, leverans och det utnyttjande av data som möjliggjorts genom digital teknik (*European Data Market study*, SMART 2013/0063, IDC, 2016).

<sup>2</sup> *European Data Market study*, SMART 2013/0063, IDC, 2016.

<sup>3</sup> Europaparlamentets och rådets förordning (EU) nr 2016/679 av den 27 april 2016, om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), EUT L 119, 4.5.2016, s. 1.

<sup>4</sup> Artikel 56 i den allmänna dataskyddsförordningen.

om de erbjuder varor och tjänster eller övervakar individers beteende inom EU. En ökad tillit bland konsumenterna kommer att gynna både europeiska och externa kommersiella aktörer.

Direktivet om integritet och elektronisk kommunikation gäller elektroniska kommunikationstjänster i EU. Det reviderade direktivet om integritet och elektronisk kommunikation, framlagt parallellt med detta meddelande i form av en förordning<sup>5</sup>, syftar till att säkerställa en hög skyddsnivå som fullständigt överensstämmer med den allmänna dataskyddsförordningen. Starka dataskyddsbestämmelser skapar det förtroende som är nödvändigt för att den digitala ekonomin ska kunna utvecklas i hela den inre marknaden.

I sitt tal om tillståndet i Europeiska unionen den 14 september 2016 lyfte ordförande Juncker fram att innebörden av att vara europé innebär rätten att få sina personuppgifter skyddade av kraftfulla lagar som gäller hela EU. För européerna vill inte ha drönare som cirkulerar ovanför dem och som registrerar allt de gör eller företag som lagrar vartenda musklick. Därför enades parlamentet, rådet och kommissionen i maj i år om en gemensam EU-förordning om skydd av personuppgifter. Detta är stark EU-lagstiftning som gäller för företag oavsett var de är baserade och oavsett vid vilken tidpunkt de behandlar dina personuppgifter. För i EU har privatlivet betydelse. Det är fråga om den mänskliga värdigheten.

Kommissionen bekräftar i sitt meddelande *Skydd av den personliga integriteten i en uppkopplad värld - En europeisk ram för personuppgiftsskydd för tjugohundratalet från 2012*<sup>6</sup> och i meddelandet *Mot en blomstrande datadriven ekonomi från 2014*<sup>7</sup> behovet av moderna, enhetliga regler i hela EU för att data ska kunna flöda fritt mellan medlemsstaterna, samt att den digitala ekonomin i Europa varit långsam när det gäller att omfamna datarevolutionen jämfört med USA, och även saknade en jämförbar industriell kapacitet. Kommissionen drog slutsatsen att avsaknaden av en rättslig miljö anpassad till handeln med data inom EU kan bidra till en otillräcklig tillgång till stora datamängder, eventuella inträdeshinder för nya marknadsaktörer och ha hämmande effekter på innovationen.

Omotiverade **begränsningar av det fria flödet av data** utgör sannolikt ett hinder för utvecklingen av EU:s dataekonomi. Dessa begränsningar är knutna till myndigheternas krav på var data som används för lagring eller bearbetning är lokaliserade. Frågan om fri rörlighet för data gäller alla typer av uppgifter: företag och andra aktörer inom dataekonomin hanterar industridata och maskingenererade uppgifter, såväl personliga som opersonliga, samt uppgifter som skapats till följd av mänsklig verksamhet. I strategin för den digitala inre marknaden meddelade kommissionen att man skulle föreslå ett initiativ för att hantera begränsningar av den fria rörligheten för data av andra skäl än för att skydda personuppgifter inom EU, samt omotiverade begränsningar för uppgifternas lokalisering i lagrings- eller bearbetningssyfte. Sådana begränsningar omfattar rättsakter antagna av medlemsstaterna, administrativa regler och praxis som har samma verkan. I takt med att dataekonomin växer tenderar begränsningarna att bli allt

---

<sup>5</sup> COM(2017) 10.

<sup>6</sup> COM(2012) 9.

<sup>7</sup> COM(2014) 442.

fler, vilket skapar osäkerhet kring var uppgifterna kan lagras eller bearbetas. Detta kan påverka alla sektorer inom ekonomin, och både privata och offentliga organisationer, som kan ha svårt att få tillgång till mer innovativa eller billigare datatjänster. Omotiverade begränsningar för lokalisering av uppgifter kan försämra friheten att tillhandahålla tjänster och etableringsfriheten som fastställs i fördraget, och även strida mot den relevanta sekundärlagstiftningen. De medför en risk för fragmentering av marknaden och minskar kvaliteten på tjänsterna för användare och konkurrenskraften för leverantörer av datatjänster, särskilt mindre företag.

Omotiverad lokalisering av data är också något som diskuteras mellan EU och dess handelspartner, med tanke på den ökade betydelsen av data och datatjänster i världsekonomin och tredjeländers potentiella inställning i frågan. EU:s regler för skydd av personuppgifter kan inte bli föremål för förhandlingar i ett frihandelsavtal. Såsom anges i meddelandet om utbyte och skydd av personuppgifter i en globaliserad värld<sup>8</sup> måste dialoger om uppgiftsskydd och handelsförhandlingar med tredjeländer följa separata spår. Utöver detta kommer kommissionen, vilket framgår i meddelandet om handel för alla, *Trade for All*<sup>9</sup>, att sträva efter att använda EU:s handelsbestämmelser för att reglera e-handel och gränsöverskridande dataflöden och bekämpa nya former av digital protektionism i full överensstämmelse med, och utan att det påverkar tillämpningen av, EU:s regler om uppgiftsskydd.

I takt med att den datadrivna omvandlingen når in i ekonomin och samhället, genereras ständigt ökande mängder data av maskiner eller processer som bygger på ny teknik, till exempel sakernas internet, framtidens fabriker och autonoma uppkopplade system. Uppkopplingen i sig själv förändrar uppgifternas tillgänglighet: i allt högre utsträckning kan man i dag få tillgång på distans till uppgifter som tidigare enbart var tillgängliga genom fysiska förbindelser. Den enorma mångfalden av datakällor och typer av data, och de stora möjligheter som finns att utvinna kunskap ur dessa data för olika områden, däribland utveckling av offentlig politik, har bara börjat växa fram. För att utnyttja dessa möjligheter måste såväl offentliga som privata aktörer på datamarknaden ha tillgång till stora och diversifierade datamängder. Frågorna om tillgång och överföring av de uppgifter som genereras av dessa maskiner eller processer är därför centrala för utvecklingen av dataekonomin och kräver en noggrann bedömning.

Andra nya frågor gäller tillämpningen av bestämmelserna om ansvar för skador som sker till följd av ett fel i en uppkopplad enhet eller robot, och uppgifternas portabilitet och interoperabilitet. När det gäller ny teknik, till exempel sakernas internet eller robotteknik, är de inbördes beroendena ofta komplexa och sofistikerade både inom produkterna (baserat på hårdvara och mjukvara) och mellan sammankopplade enheter. Dessutom kan nya frågor uppstå i fråga om autonoma maskiner, vars oförutsedda och oavsiktliga agerande skulle kunna orsaka skador på personer och föremål. Sådana händelser skulle kunna leda till rättsosäkerhet när det gäller tillämpningen av det befintliga ramverket om ansvarighet och säkerhet.

Såsom angivits i strategin för den digitala inre marknaden är kommissionens mål att skapa en tydlig och anpassad politisk och rättslig ram för dataekonomin genom att

---

<sup>8</sup> COM(2017) 7.

<sup>9</sup> COM(2015) 497.

avlägsna kvarvarande hinder för datarörlighet och åtgärda den rättsliga osäkerhet som skapats av nya datatekniker. Andra mål som ligger till grund för detta meddelande syftar till att öka uppgifternas tillgänglighet och användning, främja nya affärsmodeller för data och förbättra villkoren för tillgång till data och utvecklingen av dataanalys i EU. I detta syfte ska kommissionen presentera fokuserade frågor för diskussion med målet att ”skapa en europeisk dataekonomi”.

I detta meddelande undersöks därför följande frågor: fritt flöde av data, tillgång och överföring av maskingenererad data, ansvar och säkerhet när det gäller nya tekniker, samt portabilitet för icke-personliga uppgifter, interoperabilitet och standarder. I meddelandet ges också förslag på hur man kan experimentera med gemensamma lagstiftningslösningar i en verklig miljö.

Kommissionen ska inleda en omfattande dialog med berörda parter om de frågor som undersöks i detta meddelande. Det första steget i denna dialog är ett offentligt samråd, som inleddes parallellt med paketet om dataekonomi<sup>10</sup>.

## **2. FRITT INFORMATIONSFLÖDE**

I en väl fungerande och dynamisk dataekonomi måste flödet av data på den inre marknaden möjliggöras och skyddas. I ett sammanhang av snabb teknisk utveckling bidrar ett säkert och pålitligt fritt flöde av data till skyddet av de fyra grundläggande friheterna på den inre marknaden som garanteras i fördragen (varor, personer, tjänster och kapital). Datatjänsterna ökar snabbt i EU och globalt. En effektiv inre marknad fri från hinder inom denna sektor skulle kunna skapa betydande möjligheter till ytterligare tillväxt och sysselsättning.

Denna tillväxt och innovation i dataekonomin, liksom införandet av gränsöverskridande offentliga tjänster, kan äventyras av hinder för uppgifternas fria rörlighet inom EU. Det kan till exempel röra sig om oskäliga krav på datalokalisering från myndigheternas sida. Sådana åtgärder är ett effektivt sätt att återinföra digitala ”gränskontroller”<sup>11</sup>. Det kan handla om allt från tillsynsmyndigheters krav på dem som tillhandahåller finansiella tjänster att de måste lagra sina uppgifter lokalt, till sekretessregler som innebär att uppgifter måste lagras och bearbetas lokalt, och övergripande bestämmelser med krav på lokal lagring av arkiverad information som genereras av den offentliga sektorn, oavsett hur känslig informationen är.

Farhågor kring skyddet av personuppgifter är berättigade, men de bör inte användas av myndigheterna som skäl för att begränsa det fria flödet av uppgifter på ett omotiverat sätt. Som anges ovan är den allmänna dataskyddsförordningen en enda uppsättning regler som ger ett starkt skydd av personuppgifter i hela EU. Den stärker konsumenternas förtroende för onlinetjänster och säkerställer en enhetlig tillämpning av bestämmelserna i alla medlemsstater genom starkare nationella dataskyddsmyndigheter. Den allmänna dataskyddsförordningen främjar det förtroende som är nödvändigt för databehandling och utgör grunden för det fria flödet av personuppgifter inom EU. I den allmänna

---

<sup>10</sup> <https://ec.europa.eu/digital-single-market/news-redirect/52039>.

<sup>11</sup> OECD, *Emerging Policy Issues: Localisation Barriers to Trade*, 2015 och pågående arbete.

dataskyddsförordningen förbjuds begränsningar av det fria flödet av personuppgifter inom unionen om skälen till begränsningarna rör skydd av personuppgifter<sup>12</sup>. Begränsningar av andra skäl än skydd av personuppgifter, till exempel beskattnings- eller redovisningslagar, omfattas dock inte av den allmänna dataskyddsförordningen. Dessutom omfattas inte icke-personliga uppgifter, dvs. uppgifter som inte är avser en identifierad eller identifierbar fysisk person<sup>13</sup>, av den allmänna dataskyddsförordningen. Det kan röra sig om exempelvis icke-personliga maskingenererade uppgifter.

Restriktioner för datalokalisering kan ha sitt ursprung i rättsliga bestämmelser eller administrativa riktlinjer eller rutiner som kräver att lagringen eller bearbetningen av uppgifter<sup>14</sup> i elektronisk form<sup>15</sup> måste begränsas till ett visst geografiskt område eller en viss jurisdiktion. Ibland inför medlemsstaterna restriktioner i tron att tillsynsmyndigheterna lättare kan granska data som lagras lokalt. Lokalisering används också som ett substitut för garantier när det gäller personlig integritet, granskning och brottsbekämpning, såväl som för datasäkerhet. I praktiken bidrar emellertid dessa åtgärder sällan till att de avsedda målen uppnås.

Informationssäkerheten är beroende av en rad faktorer utöver var uppgifterna fysiskt lagras, såsom bibehållen konfidentialitet och integritet när uppgifterna är tillgängliga utanför den plats där de lagras. Istället för restriktioner för datalokalisering, är det i detta avseende snarare genom toppmodern IKT-förvaltning och bästa praxis i en betydligt större omfattning än enskilda system som en säker lagring och bearbetning av uppgifter kan tillhandahållas. För att till exempel hålla uppgifterna säkra vid lokala naturkatastrofer eller IT-angrepp kan lagringsutrymmen beläggas i olika medlemsstater utgöra säkerhetskopior, där de tekniska och organisatoriska åtgärder som föreskrivs i direktivet om säkerhet i nätverks- och informationssystem<sup>16</sup> (it-säkerhetsdirektivet) utnyttjas. Dessutom skulle tillgången till uppgifter för reglering och tillsyn, som inte på något sätt ifrågasätts, säkerställas bättre genom ett ökat samarbete mellan nationella myndigheter, eller mellan sådana myndigheter och den privata sektorn, i stället för genom begränsningar i fråga om lokalisering. På områden som präglas av nära samarbete mellan tillsynsmyndigheter, exempelvis finansiella tjänster, kan datalokaliseringskrav också visa sig vara kontraproduktiva.<sup>17</sup>

---

<sup>12</sup> Artikel 1.3. En dynamisk IP-adress registrerad av en medieleverantör på nätet när en person besöker en webbplats som leverantören gör tillgänglig för allmänheten betraktas exempelvis som en personuppgift som hanteras av leverantören, om denne har juridiska möjligheter att identifiera den registrerade med hjälp av ytterligare uppgifter som internetleverantören har om personen i fråga. Se dom i mål C-582/14, Breyer, ECLI:EU:C:2016:779, punkt 49.

<sup>13</sup> I enlighet med artikel 4.1 i den allmänna dataskyddsförordningen.

<sup>14</sup> Både privata och offentliga uppgifter.

<sup>15</sup> Inklusive kopior av datamängderna.

<sup>16</sup> Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

<sup>17</sup> Ett antal EU-bestämmelser om finansiella tjänster och det europeiska systemet för finansiell tillsyn kräver att tillsynsmyndigheterna har tillgång till uppgifter om finansiella institut och transaktioner överallt i gemenskapen. Krav på att uppgifter lagras i en viss medlemsstats territorium, eller som villkorar tillsynsmyndigheternas tillgång

Krav på datalokalisering kan dock vara motiverade och proportionerliga i särskilda situationer eller när det gäller specifika data, särskilt innan ett effektivt gränsöverskridande samarbete har inrättats, för att till exempel garantera en säker behandling av vissa uppgifter om kritisk energiinfrastruktur, eller tillgången till elektroniska bevis (t.ex. lokala kopior av datamängder) för brottsbekämpande myndigheter, eller lokal lagring av uppgifter i vissa offentliga register.

Tyvärr går trenden, både globalt och i Europa, mot lokalisering av data i allt högre utsträckning, en metod som ofta baseras på missuppfattningen att lokaliserade tjänster per automatik är säkrare än gränsöverskridande tjänster. Dessutom påverkas marknaden för datatjänster väsentligt av bristen på transparenta regler och en stark uppfattning om att data ska vara lokaliserade. Detta kan begränsa företags och offentliga organisationers tillgång till billigare eller mer innovativa datatjänster, eller tvinga företag som bedriver gränsöverskridande verksamheter att skapa överkapacitet för lagring och bearbetning av data. Det kan även hindra databaserade företag, i synnerhet uppstarts företag och små och medelstora företag, från att trappa upp sin verksamhet och komma in på nya marknader (om de t.ex. måste investera i datacenter i 28 medlemsstater) eller centralisera data- och analyskapaciteten i syfte att utveckla nya produkter och tjänster.

För närvarande levereras 84 % av den slutliga efterfrågan av IKT-relaterade tjänster (konsulttjänster, hantering och utveckling) från EU. Om dessa tjänster enklare kunde korsa nationsgränserna inom EU genom att begränsningar för datalokalisering avskaffas skulle det kunna leda till BNP-vinster på upp till 8 miljarder euro per år i kostnadsbesparingar och effektivitetsvinster<sup>18</sup>.

Datalokalisering hämmar också en mer utbredd användning av molntjänster för lagring och databehandling, vilket också skulle ha mer omfattande effekter för samhället. En mer effektiv användning av IT-resurser skulle också kunna bidra till att minska energiförbrukningen och koldioxidutsläppen med 30 % netto, eller mer. Ett litet företag som övergår till molntjänster skulle kunna minska sin energianvändning och sina koldioxidutsläpp med mer än 90 % genom att bedriva sin verksamhet i molnet i stället för att köra samma applikationer i en egen infrastruktur. Den globala marknaden för energieffektiva datacenter förväntas växa till nästan 90 miljarder euro i slutet av 2020. En fragmenterad datatjänstmarknad skulle förhindra att dessa mer energieffektiva tjänster utvecklas fullt ut inom EU, och även sätta viljan att investera på spel.

För att åtgärda de problem och begränsningar som anges ovan och utnyttja den europeiska dataekonomins fulla potential, bör alla åtgärder i medlemsstaterna som påverkar lagring eller bearbetning av data styras av **principen om fri rörlighet för data inom EU**, som en följd av deras skyldigheter inom ramen för den fria rörligheten för tjänster och den fria etableringsrätten som fastställs i fördraget och relevant sekundärlagstiftning. Eventuella befintliga eller nya begränsningar för datalokalisering måste motiveras noggrant i enlighet med fördraget och relevant sekundärrätt, för att

---

till de administrativa förfarandena, kan minska tillsynsmyndigheternas tillgång till uppgifter som är av avgörande betydelse för att de ska kunna genomföra sitt uppdrag.

<sup>18</sup> *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, ECIPE, 2016, beräkning baserad på ett ökat konkurrenstryck på en fullständigt pristransparent ”industriell” digital inre marknad.

säkerställa att de är nödvändiga och proportionerliga för att uppnå ett övergripande mål av allmänt intresse, såsom den allmänna säkerheten<sup>19</sup>.

Principen om fri rörlighet för personuppgifter,<sup>20</sup> som fastställs i primär- och sekundärlagstiftning, bör också tillämpas i de fall där den allmänna dataskyddsförordningen överlåter åt medlemsstaterna att reglera i specifika frågor. Medlemsstaterna bör också uppmuntras att inte utnyttja undantagsklausulerna i den allmänna dataskyddsförordningen för att ytterligare begränsa det fria flödet av data.

I sina slutsatser av den 15 december 2016 uppmanade Europeiska rådet till insatser för att avlägsna kvarvarande hinder på den inre marknaden, inklusive sådana som hindrar den fria rörligheten för data<sup>21</sup>.

För att genomföra principen om fri rörlighet för data kommer kommissionen att vidta följande åtgärder:

- Efter offentliggörandet av detta meddelande kommer kommissionen att inleda en strukturerad dialog med medlemsstaterna och andra aktörer om skäl för och proportionalitet i fråga om åtgärder kring datalokalisering, med utgångspunkt i de begränsningar som hittills identifierats av kommissionen.
- Med utgångspunkt i resultatet av dialogerna och en fortsatt bevisinhämtning om omfattningen av och typerna av begränsningar för datalokalisering och deras effekter, i synnerhet på små och medelstora företag och uppstartsföretag, kommer kommissionen att vid behov inleda överträdelseförfaranden för att ta itu med omotiverade eller orimliga datalokaliseringsåtgärder. Om det är nödvändigt kommer kommissionen även att ta ytterligare initiativ som rör det fria flödet av uppgifter. I detta sammanhang kommer eventuella uppföljningsåtgärder att genomföras i enlighet med principerna för bättre lagstiftning.

### 3. TILLGÅNG TILL OCH ÖVERFÖRING AV DATA

Ständigt ökande mängder data genereras av maskiner eller processer som bygger på ny teknik, som till exempel sakernas internet. Sådana data används allt oftare som en viktig komponent för nya, innovativa tjänster, i syfte att förbättra produkter eller produktionsprocesser och för att stödja beslutsfattande.

Den mångfald av data som genereras av dessa maskiner eller processer ger stora möjligheter för datamarknadens aktörer till innovation och att utvinna kunskaper ur

<sup>19</sup> Med beaktande av att fördragets undantag ska tolkas restriktivt. Sådan relevant sekundär lagstiftning innefattar den allmänna dataskyddsförordningen, direktiv 2000/31/EG (e-handelsdirektivet), direktiv 2006/123/EG (tjänstedirektivet) och, när det gäller utkast till tekniska föreskrifter och bestämmelser om informationssamhällets tjänster, direktiv 2015/1535 (insynsdirektivet).

<sup>20</sup> Det fria flödet av personuppgifter omfattas av artikel 16 i fördraget om Europeiska unionens funktionssätt, och reglerna för den fria rörligheten för personuppgifter fastställs i nuvarande och framtida EU-lagstiftning om uppgiftsskydd. I artikel 1.3 i den allmänna dataskyddsförordningen anges följande: "Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter."

<sup>21</sup> <http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/>.

uppgifterna. De data som samlas in med hjälp av sensorer i moderna jordbruk skulle till exempel kunna användas för att skapa en tillämpning för optimerad skörd, och de data som genereras av trafikljussensorer skulle kunna utnyttjas för att skapa en tillämpning för trafikledning eller ruttoptimering.

För att utnyttja värdet av denna typ av data fullt ut behöver marknadens aktörer ha tillgång till stora och varierade datamängder. Det blir dock svårt att förverkliga om de som genererar uppgifterna behåller dem för sig själva, och uppgifterna följaktligen analyseras i separata informationssiloer. Frågorna om tillgång och överföring av rådata (dvs. de data som inte bearbetats eller ändrats sedan de registrerats) som genererats av dessa maskiner eller processer är därför centrala för utvecklingen av dataekonomin och kräver en noggrann bedömning.

Frågan om tillgång till maskingenererad data är under övervägande inom flera områden, däribland sektorerna för transport, energi, smarta livsmiljöer samt hälso- och sjukvård.

Innan den aktuella situationen prövas när det gäller tillgången till data i EU är det viktigt att precisera vilken typ av data som beaktas i detta sammanhang.

### **3.1. Typer av data under övervägande**

Data kan som regel vara personliga eller icke-personliga. Exempelvis kan data som genereras av temperatursensorer i hemmet vara av personlig karaktär om uppgifterna kan kopplas till en levande person, samtidigt som uppgifter om markfuktigheten inte är personliga. Personliga data kan omvandlas till icke-personliga genom en anonymiseringsprocess. När uppgifterna kan anses vara personliga<sup>22</sup> tillämpas ramen för skydd av personuppgifter, och i synnerhet den allmänna dataskyddsförordningen.

Maskingenererade data skapas utan direkta mänskliga ingripanden genom datorprocesser, -tillämpningar eller -tjänster, eller genom sensorer som bearbetar information från utrustning, programvara eller maskinvara; virtuell eller icke-virtuell.

Maskingenererade data kan som regel vara personliga eller icke-personliga till sin natur. I fall där maskingenererade data gör det möjligt att identifiera en fysisk person, betraktas uppgifterna som personuppgifter, med följden att alla bestämmelser om personuppgifter är tillämpliga tills uppgifterna anonymiserats helt och hållet (t.ex. lokaliseringssuppgifter i mobilapplikationer).

Något det fria flödet av data har gemensamt med nya frågor om tillgång till och överföring av data är att företag och aktörer i dataekonomin kommer att hantera både personliga och icke-personliga uppgifter, och att dataflöden och datamängder regelbundet kommer att omfatta båda dessa typer. Denna ekonomiska verklighet måste beaktas i alla politiska åtgärder och i den rättsliga ramen för skydd av personuppgifter, samtidigt som enskilda människors grundläggande rättigheter respekteras.

---

<sup>22</sup> I enlighet med artikel 4.1 i den allmänna dataskyddsförordningen.

### 3.2. Begränsad tillgång till data

För att bedöma denna nya fråga måste analyser utföras av hur företag och andra marknadsaktörer kan få tillgång till de stora och varierade datamängder som behövs i dataekonomin.

Tillgängliga uppgifter<sup>23</sup> visar att företag som innehar stora mängder data i allmänhet tenderar att främst använda intern dataanalyskapacitet. I de flesta fall genereras och analyseras uppgifterna av samma företag, och även när dataanalysen sker på entreprenad är det inte säkert att uppgifterna återutnyttjas. Producenter, tjänsteföretag eller andra marknadsaktörer som innehar data behåller i vissa fall de data som genereras av deras maskiner eller via deras produkter och tjänster för sig själva, vilket eventuellt kan begränsa återutnyttjandet i efterföljande marknadsled. Många företag drar inte nytta av eller möjliggör användning av användarvänliga gränssnitt för tillämpningsprogram (API)<sup>24</sup> (som anger hur olika applikationer bör samverka med varandra) som kan fungera som säkra ingångar för nya och innovativa sätt att använda de data som innehas av företag.

Överlag är därför utbytet av data för närvarande fortfarande begränsat. Nya marknadsplatser för data har börjat framträda, men de används i liten utsträckning. Företagen har kanske inte de verktyg och kunskaper som krävs för att beräkna det ekonomiska värdet av sina data, och de kan vara rädda för att förlora eller äventyra sin konkurrensfördel om uppgifterna görs tillgängliga för konkurrenter.

### 3.3. Maskingenererade rådata: rättsläget på EU-nivå och nationell nivå

Maskingenererade rådata skyddas inte av befintliga immateriella rättigheter eftersom de inte anses vara resultatet av en intellektuell insats eller ha en viss originalitet. Den rätt av sitt eget slag som föreskrivs i databasdirektivet (96/9/EG) – som ger dem som framställer databaser rätt att förbjuda utdrag eller återanvändning av hela eller en väsentlig del av innehållet i en databas – kan ge skydd endast på villkor att inrättandet av en sådan databas innebär betydande investeringar i anskaffning, kontroll eller presentation av innehållet. Genom det nyligen antagna direktivet om skydd av företagshemligheter (2016/943/EU), som ska omvandlas till nationell lag senast i juni 2018, kommer affärshemligheter att skyddas mot olagligt förvärv, användning och utlämnande. För att data ska räknas som företagshemligheter måste åtgärder vidtas för att skydda sekretessen i informationen, som motsvarar företagets ”intellektuella kapital”.

Enligt olika medlemsstaters lagstiftning kan rättsliga anspråk tillämpas på data endast om uppgifterna uppfyller särskilda villkor för att kunna betraktas exempelvis som en immateriell rättighet, en databasrättighet eller en företagshemlighet. Maskingenererad rådata som sådan skulle dock i allmänhet inte uppfylla de relevanta villkoren på EU-nivå.

---

23 IDC, *European Data Market Study*, första interimrapporten, 2016; *Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability*, första interimrapporten, 2016; GD Kommunikationsnät, innehåll och teknik, högnivåkonferens 17 oktober 2016.

24 Till exempel <https://developer.lufthansa.com/>, <https://data.sncf.com/api>, <https://api.tfl.gov.uk/>, <https://dev.blablacar.com/>

Några omfattande politiska ramverk finns för närvarande därför inte på nationell nivå eller unionsnivå när det gäller maskinellt framtagen rådata som inte utgör personuppgifter, eller vad gäller villkoren för hur de utnyttjas eller överläts i kommersiellt syfte. Frågan är i stor utsträckning lämnad åt avtalsenliga lösningar. Användningen av befintliga allmänna avtalsrättsliga och konkurrensrättsliga instrument som finns tillgängliga i unionen skulle kunna vara en tillräcklig lösning. Dessutom skulle frivilliga avtal eller paraplyavtal som omfattar vissa sektorer kunna komma i fråga. I de fall där olika marknadsaktörerna har olika förhandlingsstyrka kan emellertid enbart marknadsbaserade lösningar vara otillräckliga för att garantera rättvisa och innovationsinriktade resultat, och underlätta ett enkelt tillträde för nya marknadsaktörer och undvika inlåsningsituationer.

### **3.4. Situationen i praktiken**

I vissa fall kan producenter eller tjänsteleverantörer i praktiken bli de som "äger" de uppgifter som deras maskiner eller processer genererar, även om själva maskinerna ägs av användarna. En faktisk kontroll av dessa data kan vara en källa till differentiering och konkurrensfördelar för tillverkare. Detta kan vara problematiskt, eftersom användarna ofta förhindras av tillverkarna att ge någon annan part rätt att använda uppgifterna.

De olika marknadsaktörerna som kontrollerar uppgifterna kan, beroende på särdragen hos marknaderna, därmed dra fördel av skillnaderna i regelverk eller av den rättsliga osäkerhet som beskrivs ovan, genom orättvisa standardavtalsvillkor för användarna eller teknik, till exempel skyddade format eller kryptering. Även om flera medlemsstater har utökat tillämpningsområdet för direktivet om konsumentskydd mot oskäligen avtalsvillkor även till transaktioner mellan företag, har dock inte alla gjort det. Det kan till exempel leda till att användare och företag blir låsta i exklusivitetsarrangemang för utnyttjande av data. Ett frivilligt utbyte av uppgifter kan komma att uppstå, men att förhandla om sådana avtal skulle kunna medföra betydande transaktionskostnader för den svagare parten i fall där förhandlingsställningarna är ojämlika, eller på grund av att kostnaderna för att anlita juridiska experter är betydande.

### **3.5. En framtida EU-ram för dataåtkomst**

Hur tillgången till maskingenererade data kan säkerställas undersöks av vissa medlemsstater, som kan komma att bestämma sig för att själva reglera frågan. En icke samordnad strategi riskerar att skapa fragmentering och skulle vara till nackdel för utvecklingen av EU:s dataekonomi och för gränsöverskridande tjänster och teknik på den inre marknaden.

Kommissionen har för avsikt att inleda en dialog med medlemsstaterna och andra intressenter för att undersöka en eventuell framtida EU-ram för tillgång till data. Kommissionen anser att denna dialog bör vara centrerad kring det effektivaste sättet att uppnå följande mål:

- **Förbättra tillgången till anonym maskingenererad data:** Genom utbyte, återutnyttjande och sammanställning av maskingenererade data blir de en källa till värdeskapande, innovation och olika affärsmodeller<sup>25</sup>.
- **Underlätta och uppmuntra utbytet av sådana data:** En framtida lösning bör främja en effektiv tillgång till data som tar hänsyn till exempelvis eventuella skillnader i förhandlingsstyrka mellan marknadsaktörer.
- **Skydda investeringar och tillgångar:** En framtida lösning bör ta hänsyn till de berättigade intressena hos marknadsaktörer som investerar i produktutveckling och säkerställa en rimlig avkastning på deras investeringar, och därmed bidra till innovation. Samtidigt bör en framtida lösning säkerställa en rättvis fördelning av vinster mellan innehavare av data<sup>26</sup>, bearbetningsföretag och leverantörer av tillämpningar inom värdekedjorna.
- **Undvika utlämnande av konfidentiella uppgifter:** En framtida lösning bör minska riskerna för att röja konfidentiella uppgifter, särskilt för befintliga eller potentiella konkurrenter. Den bör också möjliggöra att en korrekt klassificering av data kan utföras innan bedömningen av huruvida en viss informationskomponent kan delas.
- **Minimera inlåsnings effekter:** De ojämlika förhandlingspositionerna för företag och privatpersoner bör beaktas. Inlåsnings situationer, särskilt för små och medelstora företag, nystartade företag och privatpersoner, bör undvikas.

För att ta itu med frågan om tillgång till maskingenererade data avser kommissionen att i dialogerna med de berörda parterna diskutera följande möjligheter, som skiljer sig åt vad gäller graden av ingripande:

- **Vägledning för att motivera företagen att dela med sig av data:** För att mildra effekterna av olika nationella regler och skapa större rättssäkerhet för företag kan kommissionen komma att utfärda riktlinjer för hur rättigheter till kontroll av icke-personliga uppgifter bör hanteras i kontrakt. Denna vägledning skulle bygga på befintlig lagstiftning, särskilt de krav på öppenhet och rättvisa som fastställs genom EU:s lagstiftning om marknadsföring och konsumentskydd, direktivet om företagshemligheter samt upphovsrättslagstiftning, i synnerhet databasdirektivet. Kommissionen har för avsikt att inleda en utvärdering av databasdirektivet under 2017.
- **Främja utvecklingen av tekniska lösningar för tillförlitlig identifiering och utbyte av uppgifter:** Spårbarhet och tydlig identifiering av datakällor är en förutsättning för verklig kontroll av data på marknaden. Att definiera tillförlitliga och eventuellt standardiserade protokoll för permanent identifiering av datakällor kan vara nödvändigt för att skapa förtroende för systemet. Gränssnitt för tillämpningsprogram (API) kan också främja skapandet av ett ekosystem för utvecklare av applikationer och algoritmer som är intresserade av de data som

<sup>25</sup> Vid behandling av personuppgifter är den allmänna dataskyddsförordningen tillämplig.

<sup>26</sup> Det företag som i praktiken förvaltar och lagrar de maskingenererade uppgifterna.

innehålls av företag. Med hjälp av gränssnitt för tillämpningsprogram kan företag och myndigheter identifiera och utnyttja olika typer av återutnyttjande av de data som de har. Utifrån detta kan en bredare användning av öppna, standardiserade och väldokumenterade gränssnitt för tillämpningsprogram övervägas med hjälp av teknisk vägledning, bland annat identifiering och spridning av bästa praxis för företag och offentliga organ. Det skulle kunna innebära att göra data tillgängliga i maskinläsbart format och tillhandahållande av tillhörande metadata.

- **Standardavtalsregler:** Med standardregler skulle ett riktmärke för en väl avvägd lösning kunna anges för avtal som gäller data och som även beaktar den pågående kontrollen av ändamålsenligheten hos direktivet om oskäligen avtalsvillkor och hur direktivet fungerar i allmänhet. Reglerna skulle kunna kopplas samman med införandet av ett kontrollsystem för oskäligen villkor i avtal mellan företag,<sup>27</sup> som skulle ogiltigförklara avtalsklausuler som avviker alltför mycket från standardreglerna. De skulle också kunna kompletteras med en rad rekommenderade standardavtalsvillkor som utformas av berörda parter. Denna metod skulle kunna minska de rättsliga hindren för små företag och minska ojämlikheten i förhandlingspositioner, och samtidigt möjliggöra en hög grad av avtalsfrihet.
- **Tillgång för allmänna intressen och vetenskapliga ändamål:** Myndigheterna skulle kunna få tillgång till data om det skulle ligga i det ”allmänna intresset” och avsevärt förbättra den offentliga sektorns funktion, till exempel tillgång för statistikmyndigheters till affärsdata eller optimering av trafikstyrningssystem genom tillgång till data i realtid från privata fordon. Statistikmyndigheters tillgång till affärsdata skulle i normala fall bidra till att lätta bördan vad gäller statistikrapportering om ekonomiska aktörer. På samma sätt är tillgången till och förmågan att kombinera data från olika källor av avgörande betydelse för den vetenskapliga forskningen inom områden som till exempel medicin, samhällsvetenskap och miljövetenskap.
- **Dataproducenternas rättigheter:** Rätten att använda och tillåta användning av icke-personliga uppgifter skulle kunna beviljas för ”dataproducenter”, dvs. en enhets ägare eller användare på lång sikt (dvs. leasetagaren). Denna metod skulle syfta till att klargöra rättsläget och ge dataproducenterna ytterligare valmöjligheter genom att öppna upp möjligheten för användarna att använda sina uppgifter och därigenom bidra till att frigöra maskingenererad data. De relevanta undantagen måste emellertid vara klart definierade, särskilt när det gäller tillhandahållandet av icke-exklusiv tillgång till data för producenter eller myndigheter, för exempelvis trafikförvaltning eller av miljömässiga skäl. Vid behandling av personuppgifter ska enskilda individer behålla rätten att dra tillbaka sitt samtycke när som helst efter att användningen godkänts. Personuppgifter måste anonymiseras på ett sådant sätt att enskilda individer inte längre kan identifieras innan uppgifternas vidare användning kan tillåtas av den andra parten. Den allmänna dataskyddsförordningen fortsätter också att gälla alla personuppgifter (oavsett om de genererats av maskiner eller ej) tills uppgifterna har anonymiserats.

---

<sup>27</sup>. Riktmärket för oskäligen avtalsvillkor måste givetvis vara olika för avtal mellan företag och för avtal mellan företag och kunder för att återspegla den högre graden av avtalsfrihet i relationer mellan företag.

- **Tillgång mot ersättning:** En ram potentiellt baserad på vissa viktiga principer, såsom rättvisa, rimliga och icke-diskriminerande villkor, skulle kunna tas fram för datainnehavare, såsom producenter, tjänsteleverantörer eller andra parter, för att ge tillgång till uppgifter som de innehar mot ersättning efter avidentifiering. Relevanta legitima intressen, liksom behovet av att skydda företagshemligheter, måste beaktas. Olika system för tillgång för olika sektorer eller affärsmodeller kan också övervägas för att ta hänsyn till särdragen i olika branscher. Exempelvis kan öppen tillgång till data (partiell eller fullständig) i vissa fall vara att föredra både för företag och för allmänheten.

Kommissionen ska samråda med berörda parter om de frågor som beskrivits ovan, i syfte att samla in mer information om hur datamarknaderna fungerar i olika sektorer och utforska möjliga lösningar. I detta sammanhang är en bred diskussion på makronivå avgörande för att diskutera möjliga lösningar och undvika icke avsedda sidoeffekter som kan hämma innovationen eller förhindra konkurrens. Dessutom kommer sektorsspecifika diskussioner att hållas med berörda aktörer i datavärdekedjan.

#### 4. ANSVAR

En annan ny fråga avser tillämpningen av de befintliga bestämmelserna om ansvar i dataekonomin när det gäller produkter och tjänster som bygger på ny teknik, exempelvis sakernas internet, fabriker för framtiden och autonoma uppkopplade system. Sakernas internet är ett snabbt växande nätverk av vardagliga föremål, exempelvis klockor, fordon och termostater, som är anslutna till internet. Autonoma uppkopplade system, exempelvis självkörande fordon, agerar oberoende av människor och är kapabla att förstå och tolka sin omgivning. I dessa nya tekniker används sensorer för att tillhandahålla de många typer av data som ofta krävs för att produkten eller tjänsten ska fungera.

Alla dessa innovationer kommer sannolikt att bidra till ökad säkerhet och livskvalitet, men det är omöjligt att undvika designfel, funktionsfel eller manipulering i varje enskild enhet. Orsakerna kan vara en sensor som överför felaktiga data på grund av till exempel defekter i programvaran, anslutningsproblem eller felaktig drift av maskinen. Utformningen av dessa system innebär att det kan vara svårt att fastställa den exakta orsaken till problem som leder till skador, vilket väcker frågor om hur dessa system ska garanteras vara säkra för användarna och skaderiskerna minimeras, och vem som ska hållas ansvarig för skadorna om de inträffar.

Frågan om hur man kan skapa säkerhet för både användare och tillverkare av sådana produkter i förhållande till deras eventuella ansvar är därför av central betydelse för utvecklingen av dataekonomin.

##### 4.1. EU-bestämmelser om ansvar

Inom civilrätt skiljer man i allmänhet mellan två typer av skadeståndsansvar: avtalsrättsligt, där ansvaret för skadorna har sin grund i avtalsförhållandet mellan parterna, och utomobligatoriskt<sup>28</sup>, om skadorna inträffar utanför ett avtal. En viktig typ av

<sup>28</sup> EU:s regler om skadeståndsansvar avser endast utomobligatoriska förpliktelser.

utomobligatoriskt ansvar är det som rör skadeståndsansvaret för defekta produkter. På EU-nivå fastställs genom direktivet om skadeståndsansvar för produkter med säkerhetsbrister (85/374/EEG) (nedan kallat *direktivet om produktansvar*) principen om strikt ansvar, dvs. ansvar utan skuld: om en defekt produkt skadar en konsument kan tillverkaren ställas till svars även om ingen försumlighet skett eller något fel har begåtts. Det kan dock bli svårt eller oklart hur detta direktivs bestämmelser<sup>29</sup> ska tillämpas i fråga om sakernas internet och autonoma uppkopplade system (t.ex. robotteknik) på grund av bland annat egenskaperna hos dessa system, exempelvis komplicerade värdekedjor för produkterna eller tjänsterna med ömsesidiga beroenden mellan leverantörer, tillverkare och andra tredje parter, osäkerhet när det gäller den rättsliga karaktären hos anordningar inom sakernas internet, dvs. om det är fråga produkter, tjänster eller produkter som medföljer vid försäljningen av en tjänst, och dessa teknikers autonoma natur.

Kommissionen har inlett en omfattande utvärdering av direktivet om produktansvar för att bedöma dess övergripande funktion och huruvida dess regler, som utvecklats för en helt annan miljö, fortfarande är relevanta för nya tekniker som sakernas internet och autonoma uppkopplade system.

#### 4.2. Möjligheter framåt

Kommissionens mål är att stärka rättssäkerheten när det gäller skadeståndsansvar i samband med ny teknik och därigenom skapa gynnsamma villkor för innovation. Utöver status quo<sup>30</sup> kan olika metoder undersökas, inklusive följande:

- **Modeller baserade på riskskapande eller riskhantering:** Enligt dessa modeller skulle ansvar kunna tilldelas de marknadsaktörer som skapar stora risker för andra eller de marknadsaktörer som har bäst förutsättningar att minimera eller undvika att sådana risker förverkligas.
- **Frivilliga eller obligatoriska försäkringssystem:** Sådana system skulle kunna kopplas till ovannämnda ansvarsmodeller och kompensera de parter som lidit skada (t.ex. konsumenter). Denna modell skulle behöva tillhandahålla ett rättsligt skydd för företags investeringar och samtidigt säkerställa rättvis kompensation och lämplig försäkring till skadelidande i händelse av skada.

I varje modell måste man ta hänsyn till agerandet hos de enskilda individer som använder tekniken och mer specifikt fastställa vilken rollen bör vara för teknikens användare.

Kommissionen kommer att samråda med berörda parter om huruvida nuvarande EU-bestämmelser om ansvar är tillräckliga i förhållande till sakernas internet och autonoma uppkopplade system, samt om möjliga metoder för att lösa nuvarande svårigheter när det gäller att fördela ansvar. Ett parallellt offentligt samråd om den övergripande utvärderingen av tillämpningen av direktivet om produktansvar sker också. Kommissionen kommer att utvärdera resultaten och överväga möjligheter till framtida

<sup>29</sup> Hänvisningar till producenters strikta skadeståndsansvar för defekta produkter görs i andra delar av lagstiftningen om produkters säkerhet, till exempel direktivet om radioutrustning (2014/53/EU), förordningarna om medicinsk utrustning, maskindirektivet (2006/42/EG) och direktivet om allmän produktsäkerhet (2001/95/EG).

<sup>30</sup> Kommissionen kan utfärda riktlinjer om tillämpningen av EU:s regler om skadeståndsansvar för sakernas internet och robotteknik.

åtgärder.

## 5. PORTABILITET, INTEROPERABILITET OCH STANDARDER

Andra nya frågor inom dataekonomin rör portabiliteten för icke-personliga uppgifter, interoperabiliteten mellan tjänster för att möjliggöra informationsutbyte, och lämpliga tekniska standarder för genomförande av en ändamålsenlig portabilitet.

### 5.1. Portabilitet för icke-personliga uppgifter

Uppgiftsportabilitet innebär att konsumenter och företag enkelt kan föra med sig sina uppgifter från ett system till ett annat. Den är i allmänhet förknippad med låga omställningskostnader, och därmed låga inträdeshinder, i dataekonomin. Den allmänna dataskyddsförordningen ger enskilda individer rätt att få ut de personuppgifter som lämnats till tjänsteleverantören i ett strukturerat, allmänt använt maskinläsbart format och rätt att överföra informationen till en annan leverantör<sup>31</sup>.

När det gäller icke-personliga uppgifter finns dock för närvarande inga skyldigheter att garantera någon miniminivå för dataportabilitet, inte ens för allmänt utnyttjade online-tjänster som lagring i molnet. Detta beror delvis på att det kan vara tekniskt krävande och kostsamt att genomföra dataportabilitet, eftersom olika leverantörer av samma tjänster kan lagra data på olika sätt.

För att portabiliteten för icke-personliga uppgifter ska vara meningsfull måste hänsyn även tas till större styrningsöverväganden som berör användarnas insyn, reglerad tillgång och interoperabilitet för att koppla samman olika plattformar i syfte att stimulera innovation.

### 5.2. Interoperabilitet

Överväganden som rör dataportabilitet har ofta nära anknytning till frågor om datainteroperabilitet, som gör det möjligt för flera digitala tjänster att utbyta data utan avbrott, något som underlättas genom lämpliga tekniska specifikationer. I direktivet om information från den offentliga sektorn och tillhörande vägledning (inklusive den europeiska interoperabilitetsramen) understryks vikten av utförlig, standardiserad metadata uttryckt enligt en fastställd vokabulär för att underlätta sökning och interoperabilitet. Direktivet om infrastruktur för rumslig information i gemenskapen (Inspire) och dess interoperabilitetsbestämmelser och riktlinjer för rumsliga datatjänster och data, inklusive observationsdata från sensorer, tillämpas för närvarande på rumsliga data i den offentliga sektorn<sup>32</sup>.

När det gäller nätplattformar gör en sådan datainteroperabilitet det inte bara lättare att byta, utan också att samtidigt använda flera olika plattformar (så kallad ”multi-homing”),

---

<sup>31</sup> Artikel 20.

<sup>32</sup> Maskingenererade data är ”rumsliga data”, eftersom sensorer i regel också överför sina egna direkta eller indirekta positioner (lokaliseringar) tillsammans med sina mätningar.

samt i stor utsträckning utbyta data över plattformsgränserna, vilket potentiellt kan leda till ökad innovation i den digitala ekonomin.

### 5.3. Standarder

Effektiva portabilitetsåtgärder måste stödjas av relevanta tekniska standarder för genomförande av ändamålsenlig portabilitet på ett teknikneutralt sätt. Kommissionen har åtagit sig<sup>33</sup> att stödja lämpliga standarder för att förbättra interoperabiliteten, portabiliteten och säkerheten i molntjänster genom att bättre integrera det arbete som utförs av grupper som använder öppen källkod i arbetet med att fastställa standarder på europeisk nivå. Exempel på detta är TOSCA-specifikationen för molnapplikationer, vars syfte är att förbättra portabiliteten och den operativa förvaltningen av molnapplikationer och molntjänster<sup>34</sup>, och de tekniska specifikationerna och riktlinjerna i Inspires genomförandeförordningar<sup>35</sup>.

### 5.4. Möjligheter framåt

Framtida möjligheter för att ta itu med dessa frågor omfattar följande:

- **Utveckla rekommenderade avtalsvillkor för att underlätta byte av tjänsteleverantörer:** Eftersom dataportabilitet och byte av leverantör av datatjänster är beroende av varandra skulle utveckling av standardavtalsvillkor som kräver att tjänsteleverantören genomför portabilitet för kundens uppgifter kunna undersökas.
- **Utveckla ytterligare rättigheter till dataportabilitet:** Med utgångspunkt i de rättigheter som föreskrivs för dataportabilitet i den allmänna dataskyddsförordningen och i de föreslagna reglerna om avtal för leverantörer av digitalt innehåll, skulle ytterligare rättigheter till portabilitet för icke-personliga uppgifter kunna införas, i synnerhet mellan företag, samtidigt som vederbörlig hänsyn tas till resultatet av den pågående kontrollen av ändamålsenligheten i viktiga delar av EU:s marknadsförings- och konsumentlagstiftning<sup>36</sup>.
- **Sektorsspecifika försök med standarder:** För att skapa ett stabilt förhållningssätt till portabilitetsregler kodade med hjälp av standarder skulle sektorsspecifika försök kunna inledas. Dessa skulle normalt inbegripa ett samarbete med flera aktörer, såsom standardiseringsansvariga, industrin, det tekniska samfundet och myndigheterna.

---

<sup>33</sup> COM(2016) 176 final: Prioriteringar för informations- och kommunikationsteknisk standardisering på den digitala inre marknaden.

<sup>34</sup> <https://www.oasis-open.org/committees/tosca>.

<sup>35</sup> Inspire-lagstiftning: <http://inspire.ec.europa.eu/inspire-legislation/26>.

<sup>36</sup> [http://ec.europa.eu/consumers/consumer\\_rights/review/index\\_en.htm](http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm).

Kommissionen ska samråda med berörda parter om dessa frågor och utifrån detta fastställa om ytterligare åtgärder krävs, eventuellt i form av genomförande av ovannämnda åtgärder enskilt eller tillsammans.

## 6. FÖRSÖK OCH TESTER

Försök utgör en viktig del av undersökningen av nya möjligheter i dataekonomin. Möjligheten att använda finansiering inom ramen för Horisont 2020 för att stödja försök och experiment av detta slag kommer att undersökas.

Innan slutsatser dras om hur lämpliga de möjliga lösningarna för tillgång och ansvarsfördelning är bör en särskild prövning organiseras där problemen testas i en realistisk miljö, i partnerskap med berörda parter. En europeisk lösning som bygger på samarbete och försök som bedrivs mellan medlemsstaterna är nödvändig.

Samverkande, uppkopplad och automatiserad rörlighet<sup>37</sup> kan övervägas i en sådan prövning, med tanke på denna sektors gränsöverskridande dimension.

Projekt pågår redan i flera medlemsstater för att utveckla samverkande system och högre grader av automatisering<sup>38</sup>. Dessa projekt gör det möjligt att koppla samman fordon med varandra och med väginfrastruktur som vägmärken och trafiksinaler. Dessutom avser kommissionen att arbeta tillsammans med en grupp intresserade medlemsstater för att skapa en rättslig ram för att utföra försök baserade på harmoniserade regler om tillgång till data och ansvar. För att möjliggöra tillgång till tillräckligt stora datavolymer bör prövningarna grundas på 5G och ske i sömlös samexistens med teknik som redan finns på plats och enligt principen om komplementaritet<sup>39</sup>.

Ett annat intressant experiment kommer från den geospatiala sektorn, där ett nytt ekosystem för data vuxit fram kring Copernicus, EU:s jordobservationsprogram och världens största leverantör av data. Innovativa lösningar utvecklas av kommissionen för att främja utvecklingen av applikationer baserade på Copernicus och annan rumslig data, i synnerhet för att ta itu med frågor om tillgång till data, interoperabilitet och förutsägbarhet.

## 7. SLUTSATS

För att bygga en dataekonomi behöver EU en politisk ram som gör det möjligt att använda data genom hela värdekedjan för vetenskapliga, samhällsliga och industriella ändamål. I detta syfte ska kommissionen inleda en omfattande dialog med berörda parter om de frågor som undersökts i detta meddelande. Det första steget i denna dialog kommer att vara ett offentligt samråd. De frågor som rör tillgång till data och ansvar ska också provas i en verklig miljö inom området för samverkande, uppkopplad och automatiserad rörlighet.

<sup>37</sup> Se COM (2016) 766 av den 30 november 2016.

<sup>38</sup> Se COM (2016) 766: *En europeisk strategi för samverkande intelligenta transportsystem*.

<sup>39</sup> Se COM (2016) 588: *5G för Europa: en handlingsplan*.

När det gäller det fria flödet av uppgifter kommer kommissionen att fortsätta att verka i enlighet med den metod som beskrivs ovan för att fullt ut genomföra principen om det fria flödet av uppgifter inom EU, bland annat genom prioriterade verkställighetsåtgärder där det behövs och är lämpligt. Kommissionen kommer även att fortsätta att övervaka och samla in bevis och kan vid behov överväga ytterligare initiativ gällande det fria flödet av uppgifter.

Baserat på resultaten i dialogen med berörda parter kommer kommissionen också att besluta om ytterligare åtgärder krävs för nya problem, och föreslå lösningar därefter. I detta sammanhang kan försök under verkliga förhållanden komma att spela en roll.