EUROPEISKA
KOMMISSIONEN

Bryssel den 29.5.2019
COM(2019) 250 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Vägledning om förordningen om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen

Innehåll

Europeiska kommissionen tillhandahåller detta dokument endast i informationssyfte. Det innehåller inte någon auktoritativ tolkning av Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen och utgör inte ett beslut eller en ståndpunkt från Europeiska kommissionens sida. Det påverkar inte eventuella beslut eller ställningstaganden från Europeiska kommissionens sida eller EU-domstolens befogenhet att tolka förordningen i enlighet med EU-fördragen.

1 Inledning

I en alltmer datadriven ekonomi är dataflöden centrala inom affärsprocesser i företag av alla storlekar och i alla sektorer. Ny digital teknik skapar nya möjligheter för allmänheten, företag och offentliga förvaltningar i EU.

För att ytterligare öka det gränsöverskridande utbytet av data och stimulera den datadrivna ekonomin antog Europaparlamentet och rådet i november 2018 förordning (EU) 2018/1807 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen[1] (nedan kallad förordningen om det fria flödet av andra data än personuppgifter), baserat på ett förslag från Europeiska kommissionen. Förordningen är tillämplig från och med den 28 maj 2019. Principen om det fria flödet av personuppgifter har redan fastställts i förordning (EU) 2016/679 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 (nedan kallad den allmänna dataskyddsförordningen)[2]. Som en följd av detta finns nu en heltäckande ram för ett gemensamt europeiskt uppgiftsområde och fri rörlighet för all data inom Europeiska unionen[3].

Förordningen om det fria flödet av andra data än personuppgifter skapar rättslig säkerhet för företag, vilket innebär att de kan behandla sina data var som helst i EU, detta ökar i sin tur förtroende för databehandlingstjänster och motverkar metoder som innebär inlåsning hos en leverantör (*vendor lock-in*). Detta kommer att leda till ökade valmöjligheter för konsumenterna, förbättrad effektivitet och ökad stimulans vad gäller införandet av molnteknik, vilket medför stora besparingar för EU-företag. En undersökning visar att företagen i EU kan spara 20–50 % av sina it-kostnader genom att migrera till molnet[4].

Data kan tack vare de två förordningarna flöda fritt mellan medlemsstaterna, vilket gör att användare av databehandlingstjänster kan använda data som samlats in på olika EU-marknader för att förbättra sin produktivitet och konkurrenskraft. Användarna kan därmed fullt ut utnyttja de stordriftsfördelar som tillhandahålls av den stora EU-marknaden för att förbättra sin globala konkurrenskraft och sammanlänkningen av den europeiska datadrivna ekonomin.

Förordningen om det fria flödet av andra data än personuppgifter har följande tre utmärkande egenskaper:

---

[1] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen, EUT L 303, 28.11.2018, s. 59.

[2] Europaparlamentets och rådets förordning (EU) 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).

[3] Den allmänna dataskyddsförordningen omfattar även Europeiska ekonomiska samarbetsområdet (EES), vilket inbegriper Island, Liechtenstein och Norge. Förordningen om det fria flödet av andra data än personuppgifter är dessutom märkt som en text av betydelse för EES.

[4] Deloitte: Measuring the economic impact of cloud computing in Europe, SMART 2014/0031, 2016. Finns på: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Den förbjuder i regel medlemsstaterna från att införa krav på var data ska lokaliseras. Undantag från denna regel får endast göras om det är motiverat av hänsyn till den allmänna säkerheten enligt proportionalitetsprincipen.
- Genom förordningen inrättas en samarbetsmekanism för att se till att behöriga myndigheter fortsatt kan utöva eventuella rättigheter som de har för att få åtkomst till data som behandlas i en annan medlemsstat.
- Det ger näringslivet incitament att med kommissionens stöd ta fram självreglerande uppförandekoder för byte av tjänsteleverantörer och dataportering.

Vägledningens syfte

Denna vägledning uppfyller kraven i artikel 8.3 i förordningen om det fria flödet av andra data än personuppgifter, som föreskriver att kommissionen ska offentliggöra vägledning om samspelet mellan denna förordning och den allmänna dataskyddsförordningen, ”särskilt med avseende på datamängder som består av både personuppgifter och andra data än personuppgifter”.

Denna vägledning syftar till att hjälpa användarna – särskilt små och medelstora företag – att förstå samspelet mellan förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen[5]. Vägledningen behandlar därför särskilt i) begreppen andra data än personuppgifter och personuppgifter, ii) principerna om fri rörlighet för uppgifter och förbud mot krav på datalokalisering enligt båda förordningarna, och iii) begreppet dataportabilitet inom ramen för det fria flödet av uppgifter som inte är personuppgifter. Den omfattar även krav gällande självreglering som fastställs i de två förordningarna.

Förordningen om det fria flödet av andra data än personuppgifter omfattar endast andra data än personuppgifter enligt definitionen i den allmänna dataskyddsförordningen, Genom den allmänna dataskyddsförordningen regleras behandlingen av personuppgifter, som är en viktig del av EU:s ram för uppgiftsskydd[6]. Den allmänna dataskyddsförordningen trädde i kraft i medlemsstaterna den 25 maj 2018 och innehåller harmoniserade regler för att skydda

5 Skäl 37 i förordningen om det fria flödet av andra data än personuppgifter.

6
– Europaparlamentets och rådets förordning (EU) 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).
– Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).
– Direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).
– Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37) (för närvarande under omarbetning).

människor i EU/EES när det gäller behandlingen av deras personuppgifter samt om den fria rörligheten för sådana uppgifter. I den allmänna dataskyddsförordningen i) specificeras vilken information som utgör personuppgifter, ii) fastställas rättsliga grunder för behandlingen av dem, och iii) definieras bland andra bestämmelser de rättigheter och skyldigheter som ska iakttas vid behandling av personuppgifter[7]. När det gäller principen om fri rörlighet för personuppgifter anges följande i artikel 1.3 i den allmänna dataskyddsförordningen: ”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.”

I verkligheten består en datamängd sannolikt av både personuppgifter och andra data än personuppgifter. Detta brukar kallas blandad datamängd. I avsnitt 2.2 redogörs närmare för samspelet mellan förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen vad gäller blandade datamängder.

Noteras bör att det inte finns några motstridiga skyldigheter enligt den allmänna dataskyddsförordningen och förordningen om det fria flödet av andra data än personuppgifter.

2 Samspelet mellan förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen – blandade datamängder

2.1 Begreppet "andra data än personuppgifter” i förordningen om det fria flödet av andra data än personuppgifter i Europeiska unionen

Förordningen om det fria flödet av andra data än personuppgifter[8] syftar till att säkerställa det fria flödet av andra uppgifter än personuppgifter . Genom hela förordningen används termen ”data”, som bör förstås som ”andra data än personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679 [den allmänna dataskyddsförordningen]”[9]. Sådana data definieras som motsatsen till personuppgifter, som fastställs i den allmänna dataskyddsförordningen.

Personuppgifter

I den allmänna dataskyddsförordningen ges följande definition: *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad den registrerade); varvid en identifierbar fysisk person är en person som direkt eller indirekt kan

---

[7] För ytterligare vägledning angående olika aspekter av den allmän dataskyddsförordning och EU:s uppgiftsskyddslagstiftning, se webbplatsen för Europeiska dataskyddsstyrelsen, som har utfärdat ett antal riktlinjer i enlighet med artikel 70 i den allmänna dataskyddsförordningen, som finns på: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_sv. På den relevanta webbplatsen finns även hänvisningar till riktlinjer, rekommendationer och andra dokument som utfärdats av Europeiska dataskyddsstyrelsens föregångare – artikel 29-gruppen. För att öka medborgarnas och företagens medvetenhet om den allmän dataskyddsförordning har kommissionen utfärdat ett medelande om dataskydd - riktlinjer om direkt tillämpning av den allmänna dataskyddsförordningen COM/2018/043 final, som finns tillgänglig på: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

[8] Artikel 1 i förordningen om det fria flödet av andra data än personuppgifter.

[9] Se artikel 3.1 i förordningen om det fria flödet av andra data än personuppgifter.

identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Den breda definitionen av personuppgifter är avsiktlig och har i stort sett förblivit oförändrad i den allmänna dataskyddsförordningen jämfört med den tidigare lagstiftningen[10]. Olika aspekter av definitionen av personuppgifter, såsom ”varje upplysning”, ”som avser”, ”identifierad eller identifierbar”, har redan tagits upp i artikel 29-arbetsgruppens[11] yttrande 4/2007 om begreppet personuppgifter av den 20 juni 2007, WP 136.

Inom områden som till exempel forskning är pseudonymisering av personuppgifter gängse praxis för att dölja personers identitet. Pseudonymisering innebär att personuppgifter behandlas på ett sätt som gör att de inte kan tillskrivas en specifik person utan att kompletterande uppgifter används. Denna ytterligare information hålls separat och säkras genom organisatoriska eller tekniska åtgärder (t.ex. kryptering)[12][13]. Uppgifter som har pseudonymiserats anses dock fortfarande vara uppgifter om en identifierbar person om de kan tillskrivas denna person med hjälp av ytterligare information[14]. Sådana data utgör personuppgifter i enlighet med den allmänna dataskyddsförordningen.

Andra data än personuppgifter

Om aktuell data inte betraktas som personuppgifter enligt definitionen i den allmänna dataskyddsförordningen betraktas de som andra data än personuppgifter. Dessa kan kategoriseras efter ursprung, enligt följande:

- För det första, data som ursprungligen inte gällde en identifierad eller identifierbar fysisk person, t.ex. data om väderförhållanden som genereras av sensorer installerade på vindturbiner eller data om underhåll av industrimaskiner.

[10] Se artikel 2 a i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (upphörde att gälla: den 24 maj 2018, upphävd genom den allmänna dataskyddsförordningen). Se även domstolens rättspraxis om definition av personuppgifter, som medger den breda tolkningen av ett sådant begrepp, till exempel domstolens dom av den 29 januari 2009, Productores de Música de España (Promusicae)/Telefónica de España SAU , C-275/06, ECLI:EU:C:2008:54, domstolens dom av den 24 november 2011, Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) , C-70/10, ECLI:EU:C:2011:771, domstolens dom av den 19 oktober 2016, Patrick Breyer/Förbundsrepubliken Tyskland, C-582/14, ECLI:EU:C:2016:779.

[11] Artikel 29-gruppen var ett rådgivande organ som tillhandahöll kommissionen råd om uppgiftsskydd och som bidrog till utvecklingen av en harmoniserad uppgiftsskyddspolicy i EU. I och ed den allmänna dataskyddsförordningens ikraftträdande den 25 maj 2018 efterträddes artikel 29-gruppen av Europeiska dataskyddsstyrelsen.

[12] Se artikel 4.5 i den allmänna dataskyddsförordningen för definitionen av pseudonymisering.

[13] Till exempel skulle en forskningsstudie om effekterna av ett nytt läkemedel räknas som pseudonymisering, om deltagarnas personuppgifter ersattes med en unik beteckning (t.ex. en siffra eller kod) i forskningsdokumenten och deras personuppgifter förvarades separat med den tilldelade unika beteckningen i ett säkrat dokument (t.ex. i en lösenordsskyddad databas).

[14] Se skäl 26 i den allmänna dataskyddsförordningen.

- För det andra, uppgifter som ursprungligen var personuppgifter men som senare **anonymiserats**[15]. ”Anonymiseringen” av personuppgifter skiljer sig från pseudonymisering (se ovan), eftersom korrekt anonymiserade uppgifter inte kan tillskrivas en viss person, inte ens genom användning av ytterligare uppgifter[16] och därför är andra data än personuppgifter.

Bedömningen av huruvida data är korrekt anonymiserade beror på specifika och unika omständigheter i varje enskilt fall[17]. Flera exempel på återidentifiering av datamängder som påstås ha anonymiserats har visat att en sådan utvärdering kan vara krävande[18]. För att fastställa om en person är identifierbar måste man beakta alla hjälpmedel som, antingen av en personuppgiftsansvarig eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera en person[19].

Exempel på andra data ön personuppgifter:

- Data som samlas in i sådan utsträckning att enskilda händelser (t.ex. en persons enskilda utlandsresor eller resemönster som skulle kunna utgöra personuppgifter) inte längre är identifierbara kan anses vara anonyma data[20].. Anonyma data används exempelvis inom statistik eller i försäljningsrapporter (t.ex. för att bedöma hur populär en produkt eller dess egenskaper är).
- Data om högfrekvenshandel i finanssektorn eller data om precisionsjordbruk som hjälper till att övervaka och optimera användningen av bekämpningsmedel, näringsämnen och vatten.

---

15 Se skäl 26 i den allmänna dataskyddsförordningen, i vilket följande anges: ”Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar.”

16 Se domstolens dom av den 19 oktober 2016, Patrick Breyer/Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779. Domstolen ansåg att dynamiska IP-adresser kan utgöra personuppgifter även om en tredje part (t.ex. en internetleverantör) innehar kompletterande data som skulle göra det möjligt att identifiera personen. För att avgöra om en person är identifierbar måste man beakta hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera personen.

17 Vid anonymisering av data bör alltid den senaste anonymiseringstekniken användas.

18 För exempel på återidentifiering av förmodat anonymiserade data, se undersökningen om framtida dataflöden som utförts av Europaparlamentets utskott för industrifrågor, forskning och energi genom Blackman, C., Forge, S.: *Data Flows – Future Scenarios:* In-Depth Analysis for the ITRE Committee, 2017, s. 22, ruta 2. Finns på: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

19 Se skäl 26 i den allmänna dataskyddsförordningen, där följande anges: ”För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen.”

20 Se artikel 29-arbetsgruppens yttrande 05/2014 om avidentifieringsmetoder, som antogs den 10 april 2014, WP216, s. 9: ”Endast om den registeransvarige aggregerar uppgifterna till en nivå där de enskilda händelserna inte längre kan identifieras kan det dataset som blir följden anses vara anonymt. Exempel: Om en organisation samlar in uppgifter om enskilda personers resor utgör de individuella resemönstren på händelsenivå fortfarande personuppgifter för varje part, så länge som den registeransvarige (eller någon annan part) fortfarande har tillgång till ursprungliga rådata, även om direkta identifierare har avlägsnats från det dataset som tillhandahålls till tredje parter. Men om den registeransvarige utplånar rådata och endast tillhandahåller statistik som aggregerats på hög nivå till tredje parter, såsom ’på måndagar är det 160 % fler passagerare på reseträcka X än på tisdagar’, kan detta räknas som anonyma uppgifter.”

Om andra data än personuppgifter på något sätt kan kopplas till en person, så att personen blir direkt eller indirekt identifierbar, ska de dock anses vara personuppgifter.

Om exempelvis en rapport om kvalitetskontroll av en produktionslinje gör det möjligt att koppla data till specifika fabriksarbetare (t.ex. de som fastställer produktionsparametrarna) skulle dessa data betraktas som personuppgifter och den allmänna dataskyddsförordningen måste då tillämpas. Samma regler gäller när utvecklingen inom teknisk analys och dataanalys gör det möjligt att konvertera anonymiserade data till personuppgifter[21].

Eftersom definitionen av personuppgifter avser ”fysiska personer” utgör datamängder som innehåller juridiska personers namn och kontaktuppgifter i princip andra data än personuppgifter[22]. I vissa situationer kan de dock utgöra personuppgifter[23]. Det kan till exempel röra sig om att en juridisk person har samma namn som den fysiska person som äger enheten eller att uppgifterna avser en identifierad eller identifierbar fysisk person[24].

2.2 Blandade datamängder

Förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen har två olika förhållningssätt till den fria rörligheten för data i EU.

I förordningen om det fria flödet av andra data än personuppgifter fastställs ett allmänt förbud mot datalokaliseringskrav för andra data än personuppgifter. Enligt artikel 4.1 i förordningen är datalokaliseringskrav förbjudna såvida de inte är motiverade med hänsyn till allmän säkerhet, i överensstämmelse med proportionalitetsprincipen.

Förutom att den allmänna dataskyddsförordningen säkerställer en hög skyddsnivå för personuppgifter säkrar den även det fria flödet av desamma. I enlighet med artikel 1.3 i den allmänna dataskyddsförordningen får den fria rörligheten för personuppgifter ”varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter”. Tillsammans möjliggör de två förordningarna fri rörlighet för alla data inom EU. De specifika bestämmelserna behandlas ytterligare i avsnitt 3.1 och 3.2.

---

[21] Om personuppgifter behandlas på ett olagligt sätt, eller om de på annat sätt strider mot den allmänna dataskyddsförordningen, har registrerade (fysiska personer) enligt den allmänna dataskyddsförordningen rätt att inge klagomål till en nationell tillsynsmyndighet (dataskyddsmyndighet) i EU och rätt till ett effektivt rättsmedel vid en nationell domstol. De nationella tillsynsmyndigheternas uppgifter, behörighet och befogenheter styrs av avsnitt 2 i kapitel VI i den allmänna dataskyddsförordningen.

[22] I skäl 14 i den allmänna dataskyddsförordningen anges följande: ”Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.” Detta måste dock tolkas mot bakgrund av definitionen av personuppgifter i artikel 4.1 i den allmänna dataskyddsförordningen.

[23] Se domstolens dom av den 9 november 2010 i förenade målen Volker und Markus Schecke GbR, C- 92/09 och Hartmut Eifert, C- 93/09/Land Hessen, ECLI:EU:C:2010:662, punkt 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

En blandad datamängd består av både personuppgifter och andra data än personuppgifter. Blandade datamängder utgör majoriteten av de datamängder som används i den datadrivna ekonomin och är vanliga i och med den tekniska utvecklingen, som innefattar sakernas internet (dvs. digitalt sammanbundna objekt), artificiell intelligens och teknik som möjliggör analys av stordata.

Exempel på blandade datamängder:

- Ett företags skatteuppgifter, inklusive den verkställande direktörens namn och telefonnummer.
- Datamängder i en bank, särskilt data med kundinformation och transaktionsuppgifter, såsom betaltjänster (kredit- och bankkort), låneavtal och tillämpningar för förvaltning av partsrelationer samt dokument med data som rör både fysiska och juridiska personer.
- Anonymiserad statistik från forskningsinstitutioner och rådata som ursprungligen samlats in av institutionerna, såsom svar på statistiska frågeformulär från enskilda uppgiftslämnare.
- Ett företags kunskapsdatabas över it-problem och lösningar baserade på enskilda rapporter om it-incidenter.
- Data kopplade till sakernas internet, där vissa data gör att antaganden kan göras om identifierbara personer (t.ex. att personen befunnit sig på en viss adress eller personens användningsmönster).
- Analys av operativa loggdata för tillverkningsutrustning inom tillverkningsindustrin.

Exempel: kundvårdstjänster

Vissa banker använder kundvårdstjänster (CRM, customer relationship management) från tredje parter som kräver att en kunds data görs tillgängliga inom CRM-miljön. Data som innehas inom denna tjänst innefattar alla uppgifter som behövs för att på ett effektivt sätt hantera samspelet med kunder, såsom deras post- och e-postadresser, telefonnummer, vilka produkter och tjänster de köper samt försäljningsrapporter, inklusive aggregerade data. Det kan därmed röra sig om både personuppgifter och andra data än personuppgifter.

Beträffande blandade datamängder anges i förordningen[25] om det fria flödet av andra data än personuppgifter:

”I fall då en datamängd består av både personuppgifter och andra data än personuppgifter är denna förordning tillämplig på den del av datamängden som utgörs av andra data än personuppgifter. I fall då personuppgifter och andra data än personuppgifter i en datamängd är oupplösligt sammanlänkade ska denna förordning inte påverka tillämpningen av förordning (EU) 2016/679.”

[25] Artikel 2.2 i förordningen.

Detta innebär följande (i fall då en datamängd består av både personuppgifter och andra data än personuppgifter):

- Förordningen om det fria flödet av andra data än personuppgifter är tillämplig på den del av datamängden som utgörs av andra data än personuppgifter.
- Bestämmelserna om det fria flödet i den allmänna dataskyddsförordningen[26] är tillämplig på den del av datamängden som utgörs av personuppgifter.
- Om delarna med andra data än personuppgifter och delarna med personuppgifter är ”oupplösligt sammanlänkade” är de rättigheter och skyldigheter som avser uppgiftsskydd som följer av den allmänna dataskyddsförordningen till fullo tillämpliga på hela den blandade datamängden, även när personuppgifter endast utgör en liten del av datamängden[27].

Denna tolkning överensstämmer med rätten till skydd av personuppgifter, som garanteras genom Europeiska unionens stadga om de grundläggande rättigheterna[28], och med skäl 8 i förordningen om det fria flödet av andra data än personuppgifter[29]. I skäl 8 anges följande: ”Den rättsliga ramen om skydd för fysiska personer med avseende på behandling av personuppgifter [...], särskilt [den allmänna dataskyddsförordningen] [...] och [...] direktiv (EU) 2016/680 och 2002/58/EG [...], påverkas inte av denna förordning.”

Praktiskt exempel:

Ett företag med verksamhet i EU erbjuder sina tjänster via en plattform. Företag (kunder) laddar upp sina dokument som innehåller blandade datamängder på plattformen. Som personuppgiftsansvarig måste det företag som laddar upp dokumenten se till att behandlingen uppfyller kraven i den allmänna dataskyddsförordningen. Genom att behandla datamängden för den personuppgiftsansvariges räkning måste det företag som erbjuder tjänsterna (nedan kallat personuppgiftsbiträdet) lagra och behandla data i enlighet med den allmänna dataskyddsförordningen, för att exempelvis se till att en lämplig säkerhetsnivå beträffande datan kan garanteras, bland annat genom kryptering.

Begreppet ”oupplösligt förbunden” definieras inte i någon av de två förordningarna[30]. Det kan i praktiken avse en situation där en datamängd innehåller både personuppgifter och andra data än personuppgifter och det skulle vara antingen omöjligt eller enligt den personuppgiftsansvariges mening olönsamt eller tekniskt omöjligt att separera dessa data. Till exempel skulle ett företag som köper CRM-system och system för försäljningsrapportering

[26] Artikel 1.3 i den allmänna dataskyddsförordningen. Se även avsnitt 3.2 i förordningen.

[27] I kommissionens arbetsdokument Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (SWD(2017) 304 final), del 1/2, s. 3, anges att oberoende av hur många personuppgifter som ingår i de blandade datamängderna måste den allmänna dataskyddsförordningen iakttas fullt ut när det gäller den del av datamängden som utgörs av personuppgifter.

[28] Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 362, 26.10.2012, s. 391).

[29] Skäl 8 i förordningen om det fria flödet av andra data än personuppgifter.

[30] Förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen.

tvingas fördubbla sina kostnader för programvaran genom att köpa separat programvara för CRM-systemet (personuppgifter) och systemet för försäljningsrapportering (aggregerade data/andra data än personuppgifter) baserat på CRM-data.

Dessutom skulle en separation av datamängden troligtvis leda till att datamängdens värde minskade betydligt. Eftersom data även har en tendens att ändras (se avsnitt 2.1) blir det svårare att tydligt särskilja och därefter separera olika datakategorier.

Det är värt att notera att ingen av de två förordningarna innehåller krav på att företag ska separera de datamängder som de kontrollerar eller behandlar.

Följaktligen omfattas en blandad datamängd i allmänhet av personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med hänsyn till de registrerades rättigheter enligt den allmänna dataskyddsförordningen.

Behandling av hälsodata

Hälsodata kan vara en del av en blandad datamängd. Exempel på dessa är elektroniska patientjournaler, kliniska prövningar eller data som samlas in genom olika mobila applikationer för hälsa och välbefinnande (t.ex. applikationer för att mäta vårt hälsotillstånd, för att påminna oss om att ta våra mediciner eller för att kontrollera våra förbättingar av konditionen)[31]. Den exakta avgränsningen mellan personuppgifter och andra data än personuppgifter i sådana datamängder blir alltmer otydlig i takt med den tekniska utvecklingen. Behandlingen av dessa data måste därför uppfylla kraven i den allmänna dataskyddsförordningen, särskilt artikel 9 (med tanke på att hälsodata är en särskild datakategori enligt förordningen), i vilken ett allmänt förbud mot behandling av särskilda datakategorier och undantag från detta förbud fastställs.

Data i blandade datamängder som innehåller hälsodata kan vara en värdefull informationskälla, t.ex. för ytterligare medicinsk forskning, för att mäta ett förskrivet läkemedels bieffekter, för ändamål som rör sjukdomsstatistik eller för att ta fram nya hälso- och sjukvårdstjänster eller behandlingar. Den allmänna dataskyddsförordningen måste dock följas både vid inledande och ytterligare databehandling. All sådan behandling av hälsodata måste därför ha en giltig rättslig grund[32] och en lämplig motivering, vara säker och ge tillräckliga garantier.

Slutligen är det viktigt för privatpersoner och företag att få rättslig säkerhet och förtroende för behandlingen av data. Detta är även avgörande för den datadrivna ekonomin. De två förordningarna bidrar till att säkerställa detta, och de har båda som mål att inte påverka den fria rörligheten för data.

[31] Utvecklingen och driften av mobila hälsoapplikationer måste ske helt i enlighet med reglerna i den allmänna dataskyddsförordningen. Dessa krav kommer att klargöras ytterligare i uppförandekoden för integritet avseende mobila hälsoapplikationer, som för närvarande håller på att utarbetas. För mer information om utarbetandet av uppförandekoden, se https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Se artikel 6.1 i den allmänna dataskyddsförordningen.

3 Det fria flödet av data och undanröjande av datalokaliseringskrav

Detta avsnitt innehåller en mer utförlig förklaring av begreppet datalokaliseringskrav enligt förordningen om det fria flödet av andra data än personuppgifter, samt begreppet principen om fri rörlighet i den allmänna dataskyddsförordningen. Även om dessa bestämmelser inriktas på medlemsstaterna kan det vara bra för företag att få en bättre bild av hur de två förordningarna bidrar till den fria rörligheten för alla data inom EU.

3.1 Det fria flödet av icke-personuppgifter

I förordningen om det fria flödet av andra data än personuppgifter[33] anges följande: ”Datalokaliseringskrav ska vara förbjudna såvida de inte är motiverade med hänsyn till allmän säkerhet, i överensstämmelse med proportionalitetsprincipen.”

Datalokaliseringskrav definieras[34] som ”varje skyldighet, förbud, villkor, begränsning eller annat krav som föreskrivs i en medlemsstats lagar eller andra författningar eller som är ett resultat av en medlemsstats och dess offentligrättsliga organs allmänna och konsekventa administrativa praxis, inbegripet på området för offentlig upphandling, utan att tillämpningen av direktiv 2014/24/EU påverkas, enligt vilket databehandling ska äga rum på en viss medlemsstats territorium eller hindrar behandling av data i någon annan medlemsstat”[35].

Definitionen visar att de åtgärder som begränsar den fria rörligheten för data i EU kan anta olika former. De kan fastställas i lagar, andra författningar eller till och med följa av allmän och konsekvent administrativ praxis. Förbudet mot datalokaliseringskrav omfattar dessutom både direkta och indirekta åtgärder som skulle begränsa den fria rörligheten för andra data än personuppgifter.

Direkta datalokaliseringskrav kan till exempel bestå av en skyldighet att lagra data på en särskild geografisk plats (t.ex. att servrar måste vara belägna i en viss medlemsstat) eller en skyldighet att uppfylla unika nationella tekniska krav (t.ex. att datan måste ha särskilda nationella format).

Indirekta datalokaliseringskrav, som syftar till att förhindra behandling av andra data än personuppgifter i en annan medlemsstat, kan förekomma i många olika former. De kan innefatta krav på användning av teknisk utrustning som är certifierad eller godkänd i en specifik medlemsstat eller andra krav som får till följd att det blir svårare att behandla data utanför ett visst geografiskt område eller territorium inom EU[36] [37].

---

[33] Artikel 4.1 i förordningen.

[34] Artikel 3.5 i förordningen om det fria flödet av andra data än personuppgifter.

[35] Observera att rättslig osäkerhet när det gäller i vilken utsträckning det förekommer lagliga och olagliga datalokaliseringskrav ytterligare begränsar marknadsaktörernas och den offentliga sektorns valmöjligheter vad gäller lokalisering av databehandling (se skäl 4 i förordningen om det fria flödet av andra data än personuppgifter).

[36] Skäl 4 i förordningen om det fria flödet av andra data än personuppgifter.

[37] Se två undersökningar om datalokaliseringskrav som genomfördes före antagandet av förordningen om det fria flödet av andra data än personuppgifter: 1) Godel, M., m.fl.: Facilitating cross border data flows in the Digital Single Market, SMART number 2015/2016, som finns på

Vid bedömningen av huruvida en specifik åtgärd utgör ett indirekt datalokaliseringskrav måste hänsyn tas till de särskilda omständigheterna i varje enskilt fall.

I förordningen om det fria flödet av andra data än personuppgifter[38] hänvisas till begreppet **allmän säkerhet** enligt vad som anges i domstolens rättspraxis. Begreppet *allmän säkerhet* ”omfattar både den inre och den yttre säkerheten i en medlemsstat[39] samt andra frågor med bäring på allmän säkerhet, särskilt för att underlätta utredning, upptäckt och lagföring av brott. Det förutsätter att det föreligger ett verkligt och tillräckligt allvarligt hot som påverkar ett av samhällets grundläggande intressen[40], såsom ett hot mot institutioners och väsentliga offentliga tjänsters funktion samt befolkningens överlevnad, liksom en risk för en allvarlig störning i yttre förbindelser eller av den fredliga samexistensen mellan folken, eller en risk för militära intressen”.

Dessutom måste eventuella datalokaliseringskrav som är motiverade med hänsyn till den allmänna säkerheten vara proportionerliga. I enlighet med domstolens rättspraxis kräver proportionalitetsprincipen att de åtgärder som vidtas är lämpliga för att se till att de eftersträvade målen uppfylls och inte går utöver vad som är nödvändigt för det syftet[41].

Notera att förbudet mot datalokaliseringskrav inte påverkar tillämpningen av befintliga begränsningar som fastställts i unionsrätten[42].

Förordningen om det fria flödet av andra data än personuppgifter innehåller dessutom inte några skyldigheter för företag och begränsar inte deras avtalsfrihet vad gäller beslutet om var deras data ska behandlas.

---

http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 and (2) Time.lex, Spark Legal Network and Tech4i2:*Cross-border data flow in the digital single market: study on data localisation restrictions*. SMART number 2015/0054, Som finns på http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

[38] Skäl 19 i förordningen om det fria flödet av andra data än personuppgifter.

[39] Se t.ex. domstolens dom av den 23 november 2010, Land Baden-Württemberg/Tsakouridis, C-145/09, ECLI:EU:C:2010:708, punkt 43, samt domstolens dom av den 4 april 2017, Sahar Fahimian/Bundesrepublik Deutschland, C-544/15, ECLI:EU:C:2017:225, punkt 39.

[40] Se t.ex. domstolens dom av den 22 december 2008, Europeiska gemenskapernas kommission/Republiken Österrike, C-161/07, ECLI:EU:C:2008:759, punkt 35 och där angiven rättspraxis, samt domstolens dom av den 26 mars 2009, Europeiska gemenskapernas kommission/Republiken Italien, C-326/07, ECLI:EU:C:2009:193, punkt 70 och där angiven rättspraxis.

[41] Se t.ex. domstolens dom av den 8 juli 2010, Afton Chemical Limited/Secretary of State for Transport, C-343/09, ECLI:EU:C:2010:419, punkt 45 och där angiven rättspraxis.

[42] Se exempelvis artikel 245.2 i rådets direktiv 2006/112/EG av den 28 november 2006 om ett gemensamt system för mervärdesskatt, där följande anges: ”Medlemsstaterna får ålägga beskattningsbara personer som är etablerade inom deras territorium att meddela dem lagringsplatsen, när denna är belägen utanför deras territorium.” Detta krav måste dock läsas med beaktande av artikel 249, i vilken följande föreskrivs: ”När en beskattningsbar person lagrar de fakturor han utfärdar eller mottar på sådan elektronisk väg som säkerställer åtkomst online av uppgifterna och lagringsplatsen är belägen i en annan medlemsstat än den där han är etablerad, skall de behöriga myndigheterna i den medlemsstat där den beskattningsbara personen är etablerad ha rätt, för tillämpningen av detta direktiv, till åtkomst av dessa fakturor på elektronisk väg och till nedladdning och användning av sådana fakturor, med de begränsningar som fastställs i gällande föreskrifter i den medlemsstat där den beskattningsbara personen är etablerad och i den mån detta är nödvändigt för de behöriga myndigheternas kontrolländamål.”

Medlemsstaterna måste offentliggöra information om eventuella datalokaliseringskrav som är tillämpliga på deras territorium via en nationell informationspunkt online (nationella webbplatser). Medlemsstaterna måste uppdatera denna information eller tillhandahålla uppdaterade uppgifter till en central informationspunkt som inrättats enligt en annan EU-rättsakt[43]. För att göra det smidigt för företag och ge dem enkel tillgång till relevant information i hela EU kommer kommissionen att offentliggöra länkar till dessa informationspunkter på portalen Ditt Europa[44].

3.2 Det fria flödet av andra data än personuppgifter

I den allmänna dataskyddsförordningen[45] 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.”

Om en medlemsstat inför lokaliseringskrav gällande personuppgifter av andra skäl än skydd av personuppgifter måste medlemsstaten bedömas mot bakgrund av bestämmelserna om de grundläggande friheterna och de tillåtna grunderna för att göra undantag från dessa friheter i fördraget om Europeiska unionens funktionssätt[4647] och relevant EU-lagstiftning, såsom tjänstedirektivet[48] och direktivet om elektronisk handel[49].

Exempel:

Enligt nationell lagstiftning krävs att löneredovisningen hålls i en viss medlemsstat för kontrolländamål, t.ex. för kontroller av nationella skattemyndigheter. En sådan nationell bestämmelse skulle inte omfattas av artikel 1.3 i den allmänna dataskyddsförordningen, eftersom skälen inte avser skydd av personuppgifter. Detta krav skulle i stället behöva bedömas mot bakgrund av bestämmelserna om de grundläggande friheterna och de tillåtna grunderna för att göra undantag från dessa friheter i fördraget om Europeiska unionens funktionssätt.

I den allmänna dataskyddsförordningen[50] medges att medlemsstaterna får införa villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om

43 Artikel 4.4 i förordningen om det fria flödet av andra data än personuppgifter.

44 https://europa.eu/youreurope/index.htm

45 Artikel 1.3 i den allmänna dataskyddsförordningen.

46 Konsoliderad version av fördraget om Europeiska unionens funktionssätt (EUT C 326, 26.10.2012, s. 47).

47 Se även domstolens dom av den 19 juni 2008, Europeiska gemenskapernas kommission/Storhertigdömet Luxemburg, C-319/06, ECLI:EU:C:2008:350, punkterna 90–91. Domstolen konstaterade här att skyldigheten att förvara och hålla vissa handlingar tillgängliga i en viss medlemsstat utgör en inskränkning i friheten att tillhandahålla tjänster; att det rent allmänt blir lättare för myndigheterna att utöva sin tillsyn är inte ett tillräckligt skäl.

48 Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden, EUT L 376, 27.12.2006, s. 36.

49 Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”), EGT L 178, 17.7.2000, s. 1.

50 Artikel 9.4 i den allmänna dataskyddsförordningen.

hälsa. Enligt skäl 53 bör sådana nationella begränsningar emellertid inte hindra det fria flödet av personuppgifter inom EU, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter. Detta överensstämmer med artikel 16 i fördraget om Europeiska unionens funktionssätt, som ger en rättslig grund för att anta bestämmelser om rätten till skydd av personuppgifter samt om den fria rörligheten för sådana uppgifter.

3.3 Tillämpningsområde för förordningen om det fria flödet av andra data än personuppgifter

Som redan omnämnts syftar förordningen om det fria flödet av andra data än personuppgifter till att säkerställa det fria flödet av andra data än personuppgifter'inom unionen'[51]. Förordningen är därför inte tillämplig på behandling som äger rum utanför EU eller på datalokaliseringskrav rörande sådan behandling[52] [53].

Förordningens tillämpningsområde är därför, i enlighet med artikel 2.1, begränsat till behandling av andra elektroniska data än personuppgifter i EU som

(a) tillhandahålls som en tjänst till användare som är bosatta eller har ett verksamhetsställe i EU, oavsett om tjänsteleverantören är etablerad i EU eller inte, eller
(b) utförs av en fysisk eller juridisk person som är bosatt eller har ett verksamhetsställe i EU, för eget behov.

Exempel:

Artikel 2.1 a i förordningen om det fria flödet av andra data än personuppgifter:

- En molntjänsteleverantör som är etablerad i USA tillhandahåller behandlingstjänster till kunder som är bosatta eller etablerade i EU. Leverantören administrerar sin verksamhet via servrar som är belägna i EU, där datan från de europeiska kunderna lagras eller behandlas på annat sätt. Leverantören behöver inte äga EU-baserad infrastruktur, men kan till exempel även hyra serverutrymme i EU. Förordningen om det fria flödet av andra data än personuppgifter gäller för den här typen av databehandling.
- En molntjänsteleverantör som är etablerad i Japan erbjuder sina tjänster åt europeiska kunder. Leverantörens behandlingskapacitet är belägen i Japan och all behandling sker där. I detta fall, dvs. när all behandling äger rum utanför EU, är förordningen om det fria flödet av andra data än personuppgifter[54] inte tillämplig.

[51] Se artikel 1 i förordningen om det fria flödet av andra data än personuppgifter.

[52] Se skäl 15 i förordningen om det fria flödet av andra data än personuppgifter.

[53] Begreppet behandling har getts en bred definition (artikel 3.2 i förordningen om det fria flödet av andra data än personuppgifter), och förordningen ska, såsom anges i skäl 17, gälla för behandling i dess vidaste bemärkelse, och omfatta användning av alla typer av it-system.

[54] Observera att förordningen om det fria flödet av andra data än personuppgifter inte avser datalokaliseringskrav som införs av medlemsstaterna för lagring av andra data än personuppgifter i tredjeländer, och dessa kan förekomma i nationella rättsordningar. Den allmänna dataskyddsförordningen gäller alltså för behandling av personuppgifter som avser registrerade som befinner sig i EU och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerat i EU, om behandlingen har

Artikel 2.1 b i förordningen om det fria flödet av andra data än personuppgifter:

- Ett litet europeiskt uppstartsföretag från medlemsstat A beslutar att utöka sin verksamhet genom att öppna ett verksamhetsställe i medlemsstat B. För att minimera kostnaderna bestämmer sig företaget för att centralisera lagringen och behandlingen av data för det nya verksamhetsstället på sin server i medlemsstat A. Medlemsstaterna får inte förbjuda sådan it-centralisering, såvida det inte är motiverat med hänsyn till allmän säkerhet i enlighet med proportionalitetsprincipen.

Trots att förordningen om det fria flödet av andra data än personuppgifter inte är tillämplig när all behandling av andra data än personuppgifter äger rum utanför EU, måste den allmänna dataskyddsförordningen iakttas om datamängden omfattar personuppgifter. Särskilt reglerna för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt den allmänna dataskyddsförordningen måste följas[55].

3.4 Verksamhet kopplad till medlemsstaternas interna organisation

Det finns ingenting i förordningen om det fria flödet av andra data än personuppgifter som ålägger medlemsstaterna att utkontraktera tillhandahållande av tjänster i fråga om andra data än personuppgifter som de skulle vilja tillhandahålla själva, eller att organisera dem på annat sätt än genom offentliga upphandlingskontrakt[56].

I artikel 2.3 andra stycket i förordningen om det fria flödet av andra data än personuppgifter anges följande:

”Denna förordning påverkar inte lagar och andra författningar som rör medlemsstaternas **interna organisation** och som fördelar, bland myndigheter och offentligrättsliga organ enligt definitionen i artikel 2.1.4 i direktiv 2014/24/EU[57], befogenheter och ansvar för **databehandling utan avtalsenlig ersättning till privata parter**, och inte heller lagar och

---

anknytning till a) utbjudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller b) övervakning av deras beteende så länge beteendet sker inom unionen (se artikel 3.2 i den allmänna dataskyddsförordningen).

[55] När det gäller överföringar av personuppgifter till tredjeländer, se kommissionens webbplats: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_sv och kommissionens meddelande till Europaparlamentet och rådet, Utbyte och skydd av personuppgifter i en globaliserad värld, COM(2017) 7 final. Meddelandet finns på: https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=COM:2017:7:FIN. När det gäller Japan antog kommissionen den 23 januari 2019 ett beslut om adekvat skyddsnivå, vilket betyder att personuppgifter kan flöda fritt mellan de båda ekonomierna på grundval av starka skyddsgarantier.

[56] Skäl 14 i förordningen om det fria flödet av andra data än personuppgifter.

[57] Enligt artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65) är ”offentligrättsliga organ: varje organ som har samtliga följande egenskaper”: a) De har särskilt inrättats för att tillgodose behov i det allmännas intresse, utan industriell eller kommersiell karaktär. b) De är juridiska personer. och c) De finansieras till största delen av statliga, regionala eller lokala myndigheter, eller av andra offentligrättsliga organ, eller står under administrativ tillsyn av sådana myndigheter eller organ; eller de har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala eller lokala myndigheter, eller av andra offentligrättsliga organ.”

andra författningar i medlemsstaterna som föreskriver genomförandet av dessa befogenheter och ansvar."[58]

Det kan finnas berättigade intressen som motiv till valet att själv tillhandahålla databehandlingstjänster, såsom interna resurser eller gemensamma överenskommelser mellan offentliga förvaltningar. Typiska exempel är bland annat användningen av så kallade "statliga moln" eller när en regering ger en centraliserad it-byrå i uppdrag att tillhandahålla databehandlingstjänster för offentliga institutioner och organ.

Förordningen om det fria flödet av andra data än personuppgifter uppmuntrar emellertid medlemsstaterna att beakta den ekonomiska effektiviteten och andra fördelar med att använda externa tjänsteleverantörer[59] [60]. När nationella myndigheter utkontrakterar databehandling med avtalsenlig ersättning till privata parter, och behandlingen äger rum i EU, omfattas den av förordningen om det fria flödet av andra data än personuppgifter. Detta betyder att principen om det fria flödet av andra data än personuppgifter gäller för de nationella myndigheternas allmänna och administrativa praxis. De måste bl.a. avstå från att införa begränsningar för datalokalisering, t.ex. i anbudsförfaranden för offentliga upphandlingar[61]..

4 Självregleringsmetoder som understöder för det fria flödet av uppgifter

Självreglering bidrar till innovation och förtroende mellan marknadsaktörerna och är potentiellt en mer lyhörd metod i förhållande till förändringarna på marknaden. I detta avsnitt ges en överblick över självreglerande initiativ för behandling av både personuppgifter och andra data än personuppgifter.

4.1 Dataportering och byte mellan molntjänsteleverantörer

Ett av syftena med förordningen om det fria flödet av andra data än personuppgifter är att undvika praxis som innebär inlåsning hos en leverantör. Sådan praxis uppstår när användare inte kan byta molntjänsteleverantör eftersom data är inlåst i leverantörens system, t.ex. på grund av specifika dataformat eller avtalsvillkor, och inte kan överföras utanför leverantörens it-system. Att data kan porteras utan hinder är viktigt för att användarna ska kunna välja fritt mellan leverantörer av databehandlingstjänster, så att effektiv konkurrens kan säkerställas på marknaden.

Dataportabilitet mellan företag blir allt viktigare inom en rad olika digitala branscher, däribland molntjänster.

Enligt artikel 6 i förordningen om det fria flödet av andra data än personuppgifter ska kommissionen uppmuntra och underlätta utarbetandet av självreglerande uppförandekoder på

[58] I skäl 13 i förordningen om det fria flödet av andra data än personuppgifter påpekas att förordningen påverkar inte tillämpningen av direktiv 2014/24/EU.

[59] Skäl 14 i förordningen om det fria flödet av andra data än personuppgifter.

[60] En extern tjänsteleverantör kan vara vilken enhet som helst som inte är ett offentligrättsligt organ, enligt definitionen i artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG, EUT L 94, 28.3.2014, s. 65.

[61] Skäl 13 i förordningen om det fria flödet av andra data än personuppgifter.

EU-nivå (nedan kallade uppförandekoder), i syfte att bidra till en konkurrenskraftig datadriven ekonomi. Förordningen utgör en grund för att branschen ska utarbeta självreglerande uppförandekoder för byte av tjänsteleverantör och dataportering mellan olika it-system.

Vid utarbetandet av sådana uppförandekoder för dataportering bör ett antal aspekter beaktas, särskilt följande:

- Bästa praxisför att underlätta såväl byte av tjänsteleverantör som dataportering i ett strukturerat , allmänt förekommande och maskinläsbart format.
- **Minimikrav i fråga om information** för att säkerställa att professionella användare får tillräckligt detaljerad och tydlig information innan ett avtal ingås vad gäller de processer, tekniska krav, tidsramar och avgifter som gäller om en professionell användare vill byta till en annan tjänsteleverantör eller portera data tillbaka till sina egna it-system.
- **Ansatser i fråga om certifieringssystem** för att göra det lättare att jämföra molntjänster.
- Kommunikationsfärdplaner för att öka medvetenheten om uppförandekoderna.

På marknaden för molntjänster har kommissionen börjat underlätta arbetet i arbetsgrupperna för intressenter inom molntjänster på den digitala inre marknaden, vilka innefattar experter på molnområdet och professionella användare, inklusive små och medelstora företag. I detta skede håller en undergrupp på att ta fram självreglerande uppförandekoder för dataportering och byte mellan molntjänstleverantörer (Swipo-arbetsgruppen)[62] och en annan undergrupp som arbetar med att utveckla säkerhetscertifieringen i moln (CSPERT-arbetsgruppen)[63]..

Swipo-arbetsgruppen håller på att ta fram uppförandekoder som täcker hela spektrumet av molntjänster: infrastruktur som en tjänst (IaaS), plattform som en tjänst (PaaS) och programvara som en tjänst (SaaS).

Kommissionen förväntar sig att de olika uppförandekoderna ska kompletteras av standardavtalsklausuler[64]. Dessa kommer att möjliggöra tillräcklig teknisk och rättslig specificering i det praktiska genomförandet och tillämpningen av uppförandekoderna, vilket kommer att vara särskilt viktigt för små och medelstora företag. Utformningen av standardavtalsklausulerna planeras efter utarbetandet av uppförandekoderna (som bör vara klart senast den 29 november 2019).

I enlighet med artikel 8 i förordningen om det fria flödet av andra data än personuppgifter kommer kommissionen att utvärdera genomförandet av förordningen senast den 29 november 2022. Detta innebär att en bedömning kommer att kunna göras av i) effekterna på det fria flödet av data i Europa, ii) tillämpningen av förordningen, särskilt vad gäller blandade datamängder, iii) i vilken utsträckning medlemsstaterna reellt har upphävt befintliga oberättigade begränsningar för datalokalisering, och iv) uppförandekodernas marknadseffektivitet vad gäller att portera data och byta molntjänstleverantörer.

62 Cloud Switching and Porting Data Working Group.
63 European Cloud Service Provider Certification Working Group. Se även avsnitt 4.3.
64 Se skäl 30 i förordningen om det fria flödet av andra data än personuppgifter.

Begreppet ”portabilitet” och samspelet med den allmänna dataskyddsförordningen

I båda förordningarna[65] hänvisas till dataportabilitet och målet att göra det enklare att portera data från en it-miljö till en annan, dvs. antingen till en annan leverantörs system eller till system på plats. Detta förhindrar inlåsning hos en leverantör och främjar konkurrens mellan tjänsteleverantörer. Förordningarna skiljer sig dock i fråga om inställningen till portabilitet när det gäller förhållandet mellan de berörda intressegrupperna och bestämmelsernas rättsliga art.

Rätten till personuppgiftsportabilitet enligt artikel 20 i den allmänna dataskyddsförordningen inriktas på förhållandet mellan den registrerade och den personuppgiftsansvarige. Det handlar om den registrerades rätt att få ut personuppgifter som den registrerade har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade ska även ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig eller till sin egen lagringskapacitet utan hinder från den personuppgiftsansvarige som tillhandahållits personuppgifterna[66]. Den registrerade i det här förhållandet är i regel en konsument av olika typer av nättjänster som vill byta tjänsteleverantör.

I artikel 6 i förordningen om det fria flödet av andra data än personuppgifter föreskrivs ingen rättighet för professionella användare att portera data. Den innehåller dock en ansats i fråga om självreglering, med frivilliga uppförandekoder för branschen. Samtidigt avses i förordningen en situation där en professionell användare har utkontrakterat behandlingen av sina data till en tredje part som erbjuder databehandlingstjänster[67].I enlighet med artikel 3.8 i förordningen om det fria flödet av andra data än personuppgifter kan en ”professionell användare” omfatta både fysiska och juridiska personer, däribland offentliga myndigheter eller offentligrättsliga organ, som använder eller begär databehandlingstjänster för ändamål relaterade till deras näringsverksamhet, affärsverksamhet, hantverk, yrke eller verksamhet.

I praktiken avser portabiliteten enligt artikel 6 i förordningen om det fria flödet av andra data än personuppgifter samspelet mellan olika företag, dvs. mellan en professionell användare (som i fall som inbegriper behandling av personuppgifter betraktas som personuppgiftsansvarig i enlighet med den allmänna dataskyddsförordningen) och en tjänsteleverantör (som på liknande sätt betraktas som personuppgiftsbiträde i vissa fall).

Trots dessa skillnader kan situationer uppstå där dataporteringen skulle kunna omfattas av både förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen vad gäller blandade datamängder.

---

[65] Artikel 6 i förordningen om det fria flödet av andra data än personuppgifter och artikel 20 i den allmänna dataskyddsförordningen.

[66] Se artikel 29-arbetsgruppens Riktlinjer om rätten till dataportabilitet, WP 242 rev.01, antagna den 13 december 2016, senast reviderade och antagna den 5 april 2017.

[67] I skäl 29 i förordningen om det fria flödet av andra data än personuppgifter anges följande: ”Medan enskilda konsumenter kan dra nytta av befintlig unionsrätt [dvs. den allmänna dataskyddsförordningen] underlättas inte möjligheten att byta tjänsteleverantör för användare som agerar inom ramen för sin närings- eller yrkesverksamhet.”

Exempel:

Ett företag som använder en molntjänst bestämmer sig för att byta molntjänsteleverantör och portera alla data till en ny leverantör. Bytet av tjänsteleverantör och dataporteringen omfattas av avtalet mellan kunden och molntjänsteleverantören. Om den tidigare molntjänsteleverantören följer de uppförandekoder som utarbetats enligt förordningen om det fria flödet av andra data än personuppgifter måste dataporteringen ske i enlighet med kraven i dessa uppförandekoder.

Om en del av de porterade datamängderna även utgörs av personuppgifter måste porteringen överensstämma med alla relevanta bestämmelser i den allmänna dataskyddsförordningen, särskilt när det gäller att säkerställa att den nya molntjänsteleverantören följer de tillämpliga kraven, t.ex. i fråga om säkerhet[68].

Exempel:

Om en bank beslutar att byta CRM-leverantör kan vissa data (personuppgifter och andra data än personuppgifter) behöva migreras från den gamla leverantören till den nya. Dessa data kommer då att omfattas av olika lagkrav, där vissa härrör från den allmänna dataskyddsförordningen och andra från förordningen om det fria flödet av andra data än personuppgifter.

4.2 Uppförandekoder och certifieringssystem för skydd av personuppgifter

Uppförandekoder och certifieringssystem kan användas för att visa överensstämmelse med skyldigheterna enligt den allmänna dataskyddsförordningen (se artiklarna 24.3 och 28.5).

I enlighet med artiklarna 40.1 och 42.1 i den allmänna dataskyddsförordningen ska medlemsstaterna, tillsynsmyndigheterna, Europeiska dataskyddsstyrelsen och kommissionen uppmuntra branschen att utarbeta uppförandekoder och upprätta certifieringsmekanismer för dataskydd.

Sammanslutningar eller andra organ som företräder en särskild kategori av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder för den specifika sektorn. Utkastet till uppförandekod ska inges till respektive behörig tillsynsmyndighet för godkännande[69]. Om utkastet till uppförandekod avser behandling i flera medlemsstater måste tillsynsmyndigheten inge utkastet till Europeiska dataskyddsstyrelsen före godkännandet. Styrelsen kommer att avge ett yttrande om huruvida utkastet till uppförandekod överensstämmer med den allmänna dataskyddsförordningen.

[68] Se artikel 29-arbetsgruppens yttrande 05/2012 om datormoln (cloud computing), antaget den 1 juli 2012, WP 196, för mer information om molnanvändarnas och molntjänsteleverantörernas ställning och skyldigheter gällande behandlingen av personuppgifter.

[69] Se artiklarna 40.5 och 55 i den allmänna dataskyddsförordningen.

Europeiska dataskyddsstyrelsen har offentliggjort sina riktlinjer 1/2019 om uppförandekoder och övervakningsorgan inom ramen för den allmänna dataskyddsförordningen[70]. Riktlinjerna innehåller information om att utforma uppförandekoder och kriterier för deras godkännande samt annan användbar information. På liknande sätt ger Europeiska dataskyddsstyrelsens riktlinjer 1/2018 om certifiering och identifiering av certifieringskriterier i enlighet med artiklarna 42 och 43 i den allmänna dataskyddsförordningen information om certifiering enligt denna förordning samt utarbetande och godkännande av certifieringskriterier[71].

Exempel på uppförandekoder som utarbetats av molnbranschen:

EU:s uppförandekod för molntjänster togs fram med stöd av kommissionen och i samarbete med Cloud Select Industry Group på grundval av dataskyddsdirektivet[72], och därmed den allmänna dataskyddsförordningen. EU:s uppförandekod för molntjänster omfattar alla typer av molntjänster: programvara som en tjänst (SaaS), plattform som en tjänst (PaaS) och infrastruktur som en tjänst (IaaS)[73].

Uppförandekoden för leverantörer av molninfrastrukturtjänster i Europa[74] (Cloud Infrastructure Services Providers in Europe, CISPE) inriktas på leverantörer av infrastruktur som en tjänst. CISPE-uppförandekoden består av krav avseende IaaS-leverantörer som agerar som personuppgiftsbiträden enligt den allmänna dataskyddsförordningen. Den innehåller även bestämmelser för ledningsstrukturen för genomförande och tillämpning av koden.

Cloud Security Alliances uppförandekod för efterlevnad av den allmänna dataskyddsförordningen inriktas på alla berörda parter inom molntjänster och den europeiska personuppgiftslagstiftningen, såsom molntjänsteleverantörer, molnkunder och potentiella kunder, molnrevisorer och molnmäklare. Uppförandekoden omfattar alla typer av molntjänsteleverantörer[75].

4.3 Stärka tilltron till gränsöverskridande databehandling – säkerhetscertifiering

Såsom anges i skäl 33 i förordningen om det fria flödet av andra data än personuppgifter bör en stärkt tilltro till säkerheten i gränsöverskridande databehandling kunna minska marknadsaktörers och den offentliga sektorns benägenhet att använda datalokalisering som ett

[70] Europeiska dataskyddsstyrelsen: Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (ej översatta till svenska), antagna den 12 februari 2019, version för offentligt samråd. Finns på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

[71] Europeiska dataskyddsstyrelsen: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 (ej översatta till svenska), antagna den 23 januari 2019. Finns på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[72] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (upphörde att gälla den 24 maj 2018).

[73] För mer information om EU:s uppförandekoder för molntjänster, se https://eucoc.cloud/en/home.html

[74] För mer information om CISPE-uppförandekoden, se https://cispe.cloud/code-of-conduct/

[75] För mer information om Cloud Security Alliances uppförandekod, se https://gdpr.cloudsecurityalliance.org/

medel för datasäkerhet. Utöver det cybersäkerhetspaket som kommissionen föreslog 2017[76] arbetar CSPCERT-arbetsgruppen med att ta fram rekommendationer för att inrätta ett europeiskt certifieringssystem för molntjänster som kommer att läggas fram för kommissionen. Ett sådant system har potential att främja den fria rörligheten för data, göra det enklare att jämföra olika molntjänster samt stimulera spridningen av molntjänster. Kommissionen får begära att Europeiska unionens cybersäkerhetsbyrå (Enisa) utarbetar ett förslag till system i enlighet med relevanta bestämmelser i cybersäkerhetsakten[77]. Ett sådant system kan omfatta både personuppgifter och andra data än personuppgifter. Utöver cybersäkerhetsakten, och såsom anges i avsnitt 4.2, kan även den allmänna dataskyddsförordningen användas för att visa att det finns lämpliga garantier för datasäkerhet[78].

Slutliga anmärkningar

Att ha rättslig säkerhet och förtroende för behandlingen av data är grundläggande för EU:s förmåga att använda data till deras fulla potential, där värdekedjor kan utvecklas i olika sektorer och över gränserna. De båda förordningarna säkerställer detta och båda syftar till att uppnå ett fritt flöde av uppgifter. Tillsammans lägger förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen grunden för ett fritt flöde av alla data inom EU och en mycket konkurrenskraftig europeisk datadriven ekonomi.

[76] Läs mer på https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Europaparlamentets och rådets förordning av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

[78] Se skäl 74 i cybersäkerhetsakten.