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

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Digitaliseringen av ekonomin går allt snabbare. Informations- och kommunikationstekniken är inte längre en avgränsad sektor, utan utgör grunden för alla moderna innovativa ekonomiska system och samhällen. Elektroniska data står i centrum för dessa system och kan skapa stort värde när de analyseras eller kombineras med tjänster och produkter. Samtidigt väcker den datadrivna ekonomins snabba utveckling och raskt framväxande teknik såsom artificiell intelligens, produkter och tjänster med anknytning till ”sakernas internet” (Internet of Things, IoT), autonoma system och 5G nya rättsliga frågor om tillgång till och återanvändning av data samt om ansvar, etik och solidaritet. Insatser bör övervägas vad gäller ansvarsfrågan, särskilt genom genomförande av självreglerande uppförandekoder och bästa praxis av andra slag, med hänsyn till rekommendationer, beslut och åtgärder som kommer till stånd utan mänsklig medverkan genom hela värdekedjan vid databehandling. Sådana insatser skulle också kunna inbegripa lämpliga mekanismer för fastställande av ansvar, för överföring av ansvar mellan samarbetande enheter, för försäkringar och för revision.

(2) Datavärdekedjor bygger på olika verksamheter som rör data: skapande och insamling av data, sammanställning och organiserande av data, databehandling, analys, marknadsföring och distribution av data samt användning och återanvändning av data. En ändamålsenlig och effektiv databehandling är en grundläggande byggsten i alla datavärdekedjor. Databehandlingens ändamålsenlighet och effektivitet samt utvecklingen av den datadrivna ekonomin i unionen hämmas dock framför allt av två typer av hinder för datarörlighet och för den inre marknaden: datalokaliseringskrav som ställs av myndigheter i medlemsstaterna samt praxis i den privata sektorn som innebär inlåsning till en leverantör.

(3) Etableringsfriheten och friheten att tillhandahålla tjänster enligt fördraget om Europeiska unionens funktionssätt (nedan kallat *EUF-fördraget*) tillämpas på databehandlingstjänster. Tillhandahållandet av dessa tjänster försvåras, eller hindras i en del fall, emellertid av vissa nationella, regionala eller lokala krav på att lokalisera data på ett visst territorium.

(4) Sådana hinder för den fria rörligheten för databehandlingstjänster och för tjänsteleverantörers etableringsrätt härrör från krav i medlemsstaternas nationella rätt att lokalisera data i ett visst geografiskt område eller territorium för databehandlingsändamål. Andra regler eller administrativ praxis har liknande verkan genom att de inför särskilda krav som gör det svårare att behandla data utanför ett visst geografiskt område eller territorium inom unionen, till exempel krav på användning av teknisk utrustning som är certifierad eller godkänd i en specifik medlemsstat. Rättslig osäkerhet när det gäller i vilken utsträckning det förekommer lagliga och olagliga datalokaliseringskrav begränsar marknadsaktörernas och den offentliga sektorns valmöjligheter ytterligare när det gäller lokalisering av databehandling. Denna förordning begränsar inte på något sätt friheten för företag att sluta avtal som anger var data ska lokaliseras. Denna förordning är enbart avsedd att skydda denna frihet genom att säkerställa att en avtalad plats kan vara belägen var som helst inom unionen.

([1]) EUT C 227, 28.6.2018, s. 78.
([2]) Europaparlamentets ståndpunkt av den 4 oktober 2018 (ännu ej offentliggjord i EUT) och rådets beslut av den 6 november 2018.

(5) Samtidigt begränsas datarörligheten i unionen också av begränsningar i den privata sektorn: rättsliga, avtalsmässiga och tekniska aspekter som hindrar eller stoppar användare av databehandlingstjänster från att portera sina data från en tjänsteleverantör till en annan eller tillbaka till sina egna it-system, inte minst vid uppsägning av avtal med en tjänsteleverantör.

(6) Kombinationen av dessa hinder har lett till bristande konkurrens mellan molntjänsteleverantörer i unionen, till olika inlåsningseffekter och till en allvarlig brist på datarörlighet. På samma sätt har datalokaliseringspolitik undergrävt möjligheten för företag inom forskning och utveckling att underlätta samarbeten mellan företag, universitet och andra forskningsorganisationer i syfte att driva innovation.

(7) Av rättssäkerhetsskäl och till följd av behovet av lika villkor inom unionen är en enda uppsättning regler för alla marknadsaktörer en avgörande förutsättning för att den inre marknaden ska fungera väl. För att avlägsna handelshinder och snedvridningar av konkurrens till följd av olikheter mellan nationell rätt i olika medlemsstater, samt för att förhindra uppkomsten av fler sannolika handelshinder och betydande snedvridningar av konkurrensen, är det nödvändigt att anta enhetliga regler tillämpliga i alla medlemsstater.

(8) Den rättsliga ramen om skydd för fysiska personer med avseende på behandling av personuppgifter och om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation, särskilt Europaparlamentets och rådets förordning (EU) 2016/679 ([1]) och Europaparlamentets och rådets direktiv (EU) 2016/680 ([2]) och 2002/58/EG ([3]), påverkas inte av denna förordning.

(9) Det växande sakernas internet (IoT), artificiell intelligens och maskininlärning utgör viktiga källor till andra data än personuppgifter, till exempel som ett resultat av deras användning inom automatiserade industriella produktionsprocesser. Konkreta exempel på andra data än personuppgifter inkluderar aggregerade och anonymiserade datamängder som används för stora dataanalyser, data om precisionsjordbruk som kan bidra till övervakning och optimering av användningen av bekämpningsmedel och vatten, eller data om underhållsbehov för industriella maskiner. Om teknisk utveckling gör det möjligt att omvandla anonymiserade data till personuppgifter ska sådana data behandlas som personuppgifter, och förordning (EU) 2016/679 ska tillämpas i enlighet med detta.

(10) Enligt förordning (EU) 2016/679 får medlemsstaterna varken begränsa eller förbjuda den fria rörligheten för personuppgifter inom unionen av skäl som rör skyddet för fysiska personer med avseende på behandling av personuppgifter. Den här förordningen fastställer samma princip om fri rörlighet inom unionen för andra data än personuppgifter, utom när det av hänsyn till den allmänna säkerheten är motiverat med en begränsning eller ett förbud. Förordning (EU) 2016/679 och den här förordningen tillhandahåller ett enhetligt regelverk som möjliggör fri rörlighet för olika typer av data. Vidare föreskriver den här förordningen inte någon skyldighet att lagra de olika typerna av data separat.

(11) För att skapa en ram för det fria flödet av andra data än personuppgifter i unionen och för att lägga grunden för att utveckla den datadrivna ekonomin och stärka unionsindustrins konkurrenskraft är det nödvändigt att fastställa en tydlig, heltäckande och förutsebar rättslig ram för behandling av andra data än personuppgifter på den inre marknaden. En principbaserad ansats som tillhandahåller möjlighet till både samarbete mellan medlemsstaterna och självreglering bör säkerställa att ramen är tillräckligt flexibel för att ta hänsyn till de ständigt föränderliga behoven hos användare, tjänsteleverantörer och nationella myndigheter i unionen. För att undvika risk för överlappning med befintliga mekanismer och därigenom undvika ökade bördor för både medlemsstater och företag bör detaljerade tekniska regler inte fastställas.

(12) Denna förordning bör inte påverka databehandling i den mån den utförs som en del av en verksamhet som inte omfattas av unionsrättens tillämpningsområde. Det bör särskilt erinras om att det framgår av artikel 4 i fördraget om Europeiska unionen (nedan kallat *EU-fördraget*) att den nationella säkerheten är varje medlemsstats eget ansvar.

([1]) 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).

([2]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 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).

([3]) 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).

(13) Det fria flödet av data inom unionen kommer att ha en viktig roll när det gäller att uppnå datadriven tillväxt och innovation. Medlemsstaternas myndigheter och offentligrättsliga organ gynnas precis som företag och konsumenter av ökad valfrihet när det gäller leverantörer av datadrivna tjänster, av konkurrenskraftigare priser och av ett effektivare tillhandahållande av tjänster till medborgarna. I och med de stora mängder data som myndigheter och offentligrättsliga organ hanterar är det av största vikt att de föregår med gott exempel genom att utnyttja databehandlingstjänster och avstår från att införa datalokaliseringsbegränsningar när de använder sig av databehandlingstjänster. Därför bör medlemsstaternas myndigheter och offentligrättsliga organ omfattas av denna förordning. I detta avseende bör den princip om det fria flödet av andra data än personuppgifter som föreskrivs i denna förordning tillämpas även på allmän och konsekvent administrativ praxis samt på andra datalokaliseringskrav på området för offentlig upphandling, utan att det påverkar tillämpningen av Europaparlamentets och rådets direktiv 2014/24/EU ([1]).

(14) I likhet med direktiv 2014/24/EU påverkar denna förordning inte lagar och andra författningar som rör medlemsstaternas interna organisation och som fördelar, bland myndigheter och offentligrättsliga organ, befogenheter och ansvarsområden för databehandling utan avtalsenlig ersättning till privata parter, och inte heller medlemsstaters lagar och andra författningar som föreskriver genomförandet av dessa befogenheter och ansvar. Samtidigt som myndigheter och offentligrättsliga organ uppmuntras att överväga ekonomiska fördelar och andra fördelar med utkontraktering till externa tjänsteleverantörer kan de ha legitima skäl att välja att själva tillhandahålla tjänsterna eller att anlita interna resurser. Följaktligen finns det inget i denna förordning som ålägger medlemsstaterna att utkontraktera eller anlita externa leverantörer för tillhandahållande av tjänster som de skulle vilja tillhandahålla själva, eller att organisera arbetet på annat sätt än genom offentliga upphandlingskontrakt.

(15) Denna förordning bör tillämpas på fysiska eller juridiska personer som tillhandahåller databehandlingstjänster till användare som är bosatta eller har ett verksamhetsställe i unionen, inbegripet de som tillhandahåller databehandlingstjänster i unionen utan att ha något verksamhetsställe i unionen. Förordningen bör därför inte vara tillämplig på vare sig databehandlingstjänster som äger rum utanför unionen eller datalokaliseringskrav rörande sådana data.

(16) I den här förordningen föreskrivs inte regler för fastställande av tillämplig lag på privaträttens område och den påverkar därmed inte tillämpningen av Europaparlamentets och rådets förordning (EG) nr 593/2008 ([2]). Ett avtal för tillhandahållande av tjänster är i princip underkastat lagen i det land där tjänsteleverantören har sin vanliga vistelseort, i den utsträckning tillämplig lag för avtalet inte har valts i enlighet med den förordningen.

(17) Denna förordning bör gälla för databehandling i dess vidaste bemärkelse, och omfatta användning av alla typer av it-system, oavsett om de finns i en användares lokaler eller är utkontrakterade till en tjänsteleverantör. Den bör omfatta databehandling på olika nivåer, från datalagring (infrastruktur som tjänst, Infrastructure-as-a-Service (IaaS)) till databehandling på plattformar (plattform som nättjänst, Platform-as-a-Service (PaaS)) eller i tillämpningar (program som nättjänst, Software-as-a-Service (SaaS)).

(18) Datalokaliseringskrav utgör ett tydligt hinder för det fria tillhandahållandet av databehandlingstjänster i unionen och för den inre marknaden. Sådana krav bör därför förbjudas såvida de inte är motiverade med hänsyn till allmän säkerhet, enligt definitionen i unionsrätten, särskilt i den mening som avses i artikel 52 i EUF-fördraget, och är förenliga med proportionalitetsprincipen i artikel 5 i EU-fördraget. I syfte att ge verkan åt principen om det fria flödet av andra data än personuppgifter över gränserna, för att säkerställa ett snabbt undanröjande av befintliga datalokaliseringskrav och för att av operativa skäl möjliggöra databehandling på flera platser i unionen, och eftersom det i denna förordning föreskrivs åtgärder för att säkerställa tillgång till data för kontrolländamål, bör medlemsstaterna endast kunna åberopa hänsyn till allmän säkerhet som motivering för datalokaliseringskrav.

(19) Begreppet *allmän säkerhet*, i den mening som avses i artikel 52 i EUF-fördraget och i enlighet med domstolens tolkning, omfattar både den inre och den yttre säkerheten i en medlemsstat 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, 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. I överensstämmelse med proportionalitetsprincipen bör datalokaliseringskrav som är motiverade med hänsyn till allmän säkerhet vara anpassade för att uppnå det mål som eftersträvas och bör inte gå utöver vad som är nödvändigt för att uppnå detta mål.

([1]) 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).

([2]) Europaparlamentets och rådets förordning (EG) nr 593/2008 av den 17 juni 2008 om tillämplig lag för avtalsförpliktelser (Rom I) (EUT L 177, 4.7.2008, s. 6).

(20) För att säkerställa en effektiv tillämpning av principen om det fria flödet av andra data än personuppgifter över gränserna och förhindra att det uppstår nya hinder för en väl fungerande inre marknad, bör medlemsstaterna till kommissionen omedelbart överlämna varje utkast till akt som inför ett nytt datalokaliseringskrav eller ändrar ett befintligt datalokaliseringskrav. Dessa utkast till akter bör överlämnas och bedömas i enlighet med Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]).

(21) För att undanröja eventuella befintliga hinder bör medlemsstaterna dessutom, under en övergångsperiod på 24 månader från och med denna förordnings tillämpningsdatum, göra en översyn av sådana befintliga lagar och andra författningar av allmän karaktär som innehåller datalokaliseringskrav och till kommissionen överlämna eventuella sådana datalokaliseringskrav som de anser överensstämma med denna förordning, tillsammans med en motivering. Detta bör göra det möjligt för kommissionen att granska efterlevnaden av kvarvarande datalokaliseringskrav. Kommissionen bör, när så är lämpligt, kunna lämna synpunkter till medlemsstaten i fråga. Sådana synpunkter kan inbegripa en rekommendation att ändra eller upphäva datalokaliseringskravet.

(22) De skyldigheter att överlämna befintliga datalokaliseringskrav och utkast till akter till kommissionen som fastställs i denna förordning bör vara tillämpliga på lagreglerade datalokaliseringskrav och utkast till akter av allmän karaktär, men inte på beslut som riktar sig till en specifik fysisk eller juridisk person.

(23) För att säkerställa transparensen för fysiska och juridiska personer, såsom tjänsteleverantörer och användare av databehandlingstjänster, när det gäller datalokaliseringskrav i medlemsstaterna som fastlagts i en lag eller annan författning av allmän karaktär bör medlemsstaterna offentliggöra information om sådana krav via en nationell informationspunkt online och regelbundet uppdatera den informationen. Alternativt bör medlemsstaterna lämna uppdaterad information om sådana krav till en central informationspunkt som inrättats enligt en annan unionsakt. För att på lämpligt sätt informera fysiska och juridiska personer om datalokaliseringskrav i hela unionen bör medlemsstaterna meddela kommissionen webbadresserna till sådana informationspunkter. Kommissionen bör offentliggöra denna information på sin webbplats, tillsammans med en konsoliderad och regelbundet uppdaterad förteckning över alla datalokaliseringskrav som är i kraft i medlemsstaterna, inbegripet sammanfattande information om dessa krav.

(24) Datalokaliseringskrav grundar sig ofta i bristande förtroende för gränsöverskridande databehandling, som i sin tur beror på antagandet att data inte kommer att vara tillgängliga för de behöriga myndigheterna i medlemsstaterna, till exempel för inspektioner och revisioner i samband med tillsyn eller övervakning. Ett sådant bristande förtroende kan inte överbryggas uteslutande genom en ogiltigförklaring av avtalsvillkor som förhindrar lagenlig tillgång till data för behöriga myndigheter när de utför sitt uppdrag. Denna förordning bör därför klart och tydligt ange att den inte påverkar de behöriga myndigheternas befogenhet att begära eller få tillgång till data i enlighet med unionsrätt eller nationell rätt och att behöriga myndigheter inte får nekas tillgång till data på grundval av att data behandlas i en annan medlemsstat. Behöriga myndigheter skulle kunna uppställa funktionella krav för att stödja tillgången till data, till exempel kräva att systembeskrivningar ska förvaras i den berörda medlemsstaten.

(25) Fysiska eller juridiska personer som omfattas av skyldigheter att lämna data till behöriga myndigheter kan uppfylla dessa skyldigheter genom att tillhandahålla och garantera behöriga myndigheter faktisk och snabb elektronisk tillgång, oberoende av på vilken medlemsstats territorium datan behandlas. Sådan tillgång kan säkerställas genom konkreta villkor i avtal mellan å ena sidan den fysiska eller juridiska person som omfattas av skyldigheten att ge tillgång till data och å andra sidan tjänsteleverantören.

(26) Om en fysisk eller juridisk person som omfattas av en skyldighet att tillhandahålla data inte uppfyller den skyldigheten bör den behöriga myndigheten ha möjlighet att begära assistans från behöriga myndigheter i andra medlemsstater. I sådana fall bör behöriga myndigheter använda specifika samarbetsinstrument i unionsrätten eller enligt internationella avtal, beroende på vilken fråga som berörs i det aktuella fallet, exempelvis, på området för

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

polissamarbete, straffrättsliga eller civilrättsliga fall respektive administrativa ärenden, rådets rambeslut 2006/960/RIF ([1]), Europaparlamentets och rådets direktiv 2014/41/EU ([2]), Europarådets konvention om it-brottslighet ([3]), rådets förordning (EG) nr 1206/2001 ([4]), rådets direktiv 2006/112/EG ([5]) respektive rådets förordning (EU) nr 904/2010 ([6]). I avsaknad av sådana specifika samarbetsmekanismer bör de behöriga myndigheterna samarbeta med varandra genom utsedda kontaktpunkter i syfte att ge tillgång till efterfrågade data.

(27) Om en begäran om assistans innefattar tillträde till en fysisk eller juridisk persons lokaler, inbegripet utrustning och medel för databehandling, måste sådant tillträde vara förenligt med unionsrätten eller nationell processrätt, inklusive eventuella krav på rättsliga tillstånd.

(28) Denna förordning bör inte göra det möjligt för användare att försöka undandra sig tillämpningen av nationell rätt. Den bör därför föreskriva att medlemsstaterna ska tillämpa effektiva, proportionella och avskräckande sanktioner på användare som hindrar behöriga myndigheter från att få tillgång till data som de behöver för att utföra sitt uppdrag enligt unionsrätten och nationell rätt. I brådskande fall, där en användare missbrukar sina rättigheter, bör medlemsstaterna kunna vidta strikt proportionella interimistiska åtgärder. Interimistiska åtgärder som innefattar krav på omlokalisering av data i mer än 180 dagar räknat från själva omlokaliseringen skulle innebära en avvikelse från principen om fri rörlighet för data under en betydande period, och kommissionen bör därför underrättas om sådana åtgärder så att deras förenlighet med unionsrätten kan granskas.

(29) Möjligheten att portera data utan hinder är en avgörande faktor när det gäller att underlätta användarnas val och främja effektiv konkurrens på marknaderna för databehandlingstjänster. De faktiska eller upplevda svårigheterna i fråga om att portera data över gränser undergräver också professionella användares förtroende när det gäller att acceptera gränsöverskridande anbud, och därigenom deras förtroende för den inre marknaden. Medan enskilda konsumenter kan dra nytta av befintlig unionsrätt underlättas inte möjligheten att byta tjänsteleverantör för användare som agerar inom ramen för sin närings- eller yrkesverksamhet. Enhetliga tekniska krav i hela unionen avseende teknisk harmonisering, ömsesidigt erkännande eller frivillig harmonisering bidrar också till utvecklingen av en konkurrenskraftig inre marknad för databehandlingstjänster.

(30) För att dra nytta av den konkurrensutsatta miljön fullt ut bör professionella användare kunna göra välinformerade val och på ett enkelt sätt jämföra enskilda delar av olika erbjudanden om databehandlingstjänster på den inre marknaden, bland annat när det gäller avtalsvillkoren för dataportering vid uppsägning av avtal. Den detaljerade informationen och de operativa kraven för dataportering bör, i syfte att anpassa dem till marknadens innovationspotential och med beaktande av den erfarenhet och sakkunskap som finns hos tjänsteleverantörer och professionella användare av databehandlingstjänster, fastställas av marknadsaktörerna genom självreglering i form av uppförandekoder på unionsnivå som skulle kunna inbegripa standardavtalsvillkor, vilket bör uppmuntras, underlättas och övervakas av kommissionen.

(31) För att uppnå ändamålsenlighet och underlätta byte av tjänsteleverantör och dataportering bör uppförandekoderna vara heltäckande och inbegripa åtminstone de huvudaspekter som är viktiga under dataporteringsprocessen, såsom de processer som används för, och platsen för, backup av data, tillgängliga dataformat och support, erforderlig it-konfiguration och minsta nätverksbandbredd, den tid som krävs innan porteringsprocessen inleds och den tid under vilken data kommer att förbli tillgängliga för portering samt garantier för tillgång till data om tjänsteleverantören går i konkurs. Uppförandekoderna bör även klargöra att inlåsning till en leverantör inte är en godtagbar affärspraxis samt föreskriva tillitsfrämjande teknik, och de bör uppdateras regelbundet för att hålla jämna steg med den tekniska utvecklingen. Kommissionen bör säkerställa att samråd sker med alla berörda parter, inbegripet sammanslutningar av små och medelstora företag och uppstartsföretag, användare och molntjänsteleverantörer, under hela processen. Kommissionen bör utvärdera utarbetandet av sådana uppförandekoder, och effektiviteten i genomförandet av dem.

([1]) Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (EUT L 386, 29.12.2006, s. 89).
([2]) Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området (EUT L 130, 1.5.2014, s. 1).
([3]) Europarådets konvention om it-brottslighet, CETS nr 185.
([4]) Rådets förordning (EG) nr 1206/2001 av den 28 maj 2001 om samarbete mellan medlemsstaternas domstolar i fråga om bevisupptagning i mål och ärenden av civil eller kommersiell natur (EGT L 174, 27.6.2001, s. 1).
([5]) Rådets direktiv 2006/112/EG av den 28 november 2006 om ett gemensamt system för mervärdesskatt (EUT L 347, 11.12.2006, s. 1).
([6]) Rådets förordning (EU) nr 904/2010 av den 7 oktober 2010 om administrativt samarbete och kampen mot mervärdesskattebedrägeri (EUT L 268, 12.10.2010, s. 1).

(32) Om en behörig myndighet i en medlemsstat begär assistans från en annan medlemsstat för att få tillgång till data enligt denna förordning bör den, genom en utsedd kontaktpunkt, lämna in en vederbörligen motiverad begäran till den sistnämnda medlemsstatens utsedda kontaktpunkt, vilken bör inbegripa en skriftlig förklaring av skälen och de rättsliga grunderna för begäran om tillgång till data. Den kontaktpunkt som utsetts av den medlemsstat vars assistans begärs bör underlätta överföringen av begäran till den relevanta behöriga myndigheten i den tillfrågade medlemsstaten. I syfte att säkerställa ett verkningsfullt samarbete bör den myndighet till vilken begäran överförts utan onödigt dröjsmål tillhandahålla assistans som svar på en viss begäran eller informera om svårigheter med att tillmötesgå en sådan begäran eller om skälen för att avslå den.

(33) Att stärka tilltron till säkerheten i gränsöverskridande databehandling bör kunna minska marknadsaktörers och den offentliga sektorns benägenhet att använda datalokalisering som ett medel för datasäkerhet. Det bör också kunna förbättra företags rättsliga säkerhet vad gäller efterlevnad av tillämpliga säkerhetskrav när de utkontrakterar sina databehandlingsaktiviteter till tjänsteleverantörer, inbegripet tjänsteleverantörer i andra medlemsstater.

(34) Alla databehandlingsrelaterade säkerhetskrav som tillämpas på ett motiverat och proportionellt sätt med stöd av unionsrätten eller med stöd av nationell rätt i överensstämmelse med unionsrätten, i den medlemsstat där de fysiska eller juridiska personer vars data berörs är bosatta eller etablerade, bör vara tillämpliga på databehandlingen även när den sker i en annan medlemsstat. Dessa fysiska eller juridiska personer bör kunna uppfylla dessa krav, antingen själva eller genom klausuler i avtal med tjänsteleverantören.

(35) Säkerhetskrav som fastställs på nationell nivå bör vara nödvändiga och stå i proportion till riskerna relaterade till säkerheten vid databehandling inom tillämpningsområdet för den nationella rätt där kraven fastställts.

(36) Europaparlamentets och rådets direktiv (EU) 2016/1148 ([1]) föreskriver rättsliga åtgärder för att förbättra den generella cybersäkerhetsnivån i unionen. Databehandlingstjänster utgör en av de digitala tjänster som omfattas av det direktivet. Enligt det direktivet ska medlemsstaterna säkerställa att leverantörer av digitala tjänster utarbetar och vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder. Sådana åtgärder bör garantera en säkerhetsnivå som är lämplig i förhållande till den föreliggande risken, och bör ta hänsyn till systemens och anläggningarnas säkerhet, incidenthantering, driftskontinuitetshantering, övervakning, revision och testning samt efterlevnad av internationella standarder. Dessa element ska specificeras närmare av kommissionen i genomförandeakter enligt det direktivet.

(37) Kommissionen bör lägga fram en rapport om genomförandet av denna förordning, särskilt i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska eller marknadsmässiga utvecklingen. Rapporten bör särskilt utvärdera denna förordning, särskilt dess tillämpning på datamängder som består av både personuppgifter och andra data än personuppgifter, samt genomförandet av undantaget avseende allmän säkerhet. Innan denna förordning blir tillämplig bör kommissionen även offentliggöra informativ vägledning om hur datamängder som består av både personuppgifter och andra data än personuppgifter bör hanteras, för att företag, inbegripet små och medelstora sådana, bättre ska förstå samspelet mellan denna förordning och förordning (EU) 2016/679 och för att säkerställa att båda förordningarna efterlevs.

(38) Denna förordning respekterar de grundläggande rättigheterna och följer de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna, och bör tolkas och tillämpas i enlighet med dessa rättigheter och principer, inbegripet rätten till skydd av personuppgifter, yttrande- och informationsfriheten samt näringsfriheten.

(39) Eftersom målet för denna förordning, nämligen att säkerställa det fria flödet för andra data än personuppgifter i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål,

([1]) 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).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

Denna förordning syftar till att säkerställa det fria flödet av andra data än personuppgifter inom unionen genom att fastställa regler avseende datalokaliseringskrav, tillgång till data för behöriga myndigheter och dataportering för professionella användare.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på behandling av andra elektroniska data än personuppgifter i unionen som

a) tillhandahålls som en tjänst till användare som är bosatta eller har ett verksamhetsställe i unionen, oavsett om tjänsteleverantören är etablerad i unionen eller inte, eller

b) utförs av en fysisk eller juridisk person som är bosatt eller har ett verksamhetsställe i unionen, för eget behov.

2. 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.

3. Denna förordning är inte tillämplig på verksamheter som inte omfattas av unionsrätten.

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, befogenheter och ansvar för databehandling utan avtalsenlig ersättning till privata parter, och inte heller lagar och andra författningar i medlemsstaterna som föreskriver genomförandet av dessa befogenheter och ansvar.

Artikel 3

Definitioner

I denna förordning avses med

1. *data*: andra data än personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679,

2. *behandling*: en åtgärd eller en kombination av åtgärder beträffande data eller datamängder i elektroniskt format, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *utkast till akt*: en text som utarbetats i syfte att den ska antas som en lag eller annan författning av allmän karaktär och som befinner sig på ett sådant förberedande stadium att väsentliga ändringar fortfarande kan göras,

4. *tjänsteleverantör*: en fysisk eller juridisk person som tillhandahåller databehandlingstjänster,

5. *datalokaliseringskrav*: 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,

6. *behörig myndighet*: en medlemsstats myndighet, eller varje annan enhet med behörighet enligt nationell rätt att utöva en offentlig funktion eller att utöva offentlig makt, som har befogenhet att för utförande av sitt uppdrag få tillgång till data som behandlas av en fysisk eller juridisk person, i enlighet med unionsrätten eller nationell rätt,

7. *användare*: en fysisk eller juridisk person, inbegripet en myndighet eller ett offentligrättsligt organ, som använder eller begär en databehandlingstjänst,

8. *professionell användare*: en fysisk eller juridisk person, inbegripet en myndighet eller ett offentligrättsligt organ, som använder eller begär en databehandlingstjänst för ändamål relaterade till den personens närings- eller yrkesverksamhet.

Artikel 4

Fri rörlighet för data inom unionen

1. Datalokaliseringskrav ska vara förbjudna såvida de inte är motiverade med hänsyn till allmän säkerhet, i överensstämmelse med proportionalitetsprincipen.

Första stycket i denna punkt påverkar inte vare sig punkt 3 eller datalokaliseringskrav vilka fastställts på grundval av befintlig unionsrätt.

2. Medlemsstaterna ska till kommissionen omedelbart överlämna varje utkast till akt som inför ett nytt datalokaliseringskrav eller gör ändringar i ett befintligt datalokaliseringskrav i enlighet med de förfaranden som fastställs i artiklarna 5, 6 och 7 i direktiv (EU) 2015/1535.

3. Senast den 30 maj 2021 ska medlemsstaterna säkerställa att alla befintliga datalokaliseringskrav som fastställs i lagar och andra författningar av allmän karaktär och som inte är förenliga med punkt 1 i denna artikel upphävs.

Senast den 30 maj 2021 ska en medlemsstat som anser att en befintlig åtgärd innehållande ett datalokaliseringskrav är förenlig med punkt 1 i denna artikel och därför kan fortsätta att gälla, underrätta kommissionen om den åtgärden, tillsammans med en motivering till varför den ska bibehållas. Utan att det påverkar tillämpningen av artikel 258 i EUF-fördraget ska kommissionen, inom sex månader från dagen för mottagandet av en sådan underrättelse, undersöka huruvida åtgärden är förenlig med punkt 1 i den här artikeln och vid behov lämna synpunkter till medlemsstaten i fråga, inbegripet en rekommendation om ändring eller upphävande av åtgärden om så krävs.

4. Medlemsstaterna ska göra information om eventuella datalokaliseringskrav som fastställts i lagar och andra författningar av allmän karaktär och som är tillämpliga på deras territorier allmänt tillgänglig via en nationell informationspunkt online som de ska hålla uppdaterad, eller lämna uppdaterad information om sådana datalokaliseringskrav till en central informationspunkt som inrättats enligt en annan unionsakt.

5. Varje medlemsstat ska meddela kommissionen webbadressen till den nationella informationspunkt som avses i punkt 4. Kommissionen ska offentliggöra länkarna till sådana punkter på sin webbplats, tillsammans med en konsoliderad och regelbundet uppdaterad förteckning över samtliga datalokaliseringskrav som avses i punkt 4, inbegripet sammanfattad information om de kraven.

Artikel 5

Tillgång till data för behöriga myndigheter

1. Denna förordning ska inte påverka behöriga myndigheters befogenheter att begära eller få tillgång till data för utförande av sina uppdrag i enlighet med unionsrätten eller nationell rätt. Behöriga myndigheter får inte nekas tillgång till data på grundval av att datan behandlas i en annan medlemsstat.

2. Om en behörig myndighet, efter att ha begärt tillgång till en användares data, inte får tillgång till datan, och om det inte finns någon särskild samarbetsmekanism enligt unionsrätten eller internationella avtal för utbyte av data mellan behöriga myndigheter i olika medlemsstater, får den behöriga myndigheten begära assistans från en behörig myndighet i en annan medlemsstat i enlighet med det förfarande som anges i artikel 7.

3. Om en begäran om assistans innefattar tillträde till en fysisk eller juridisk persons lokaler, inbegripet till utrustning och medel för databehandling, måste sådant tillträde vara förenligt med unionsrätten eller nationell processrätt.

4. Medlemsstaterna får tillämpa effektiva, proportionella och avskräckande sanktioner för underlåtelse att fullgöra en skyldighet att tillhandahålla data, i enlighet med unionsrätten och nationell rätt.

I det fall en användare missbrukar sina rättigheter får en medlemsstat, om det är motiverat med hänsyn till att tillgången till data brådskar samt med beaktande av de berörda parternas intressen, vidta strikt proportionella interimistiska åtgärder mot den användaren. Om en interimistisk åtgärd innefattar krav på omlokalisering av data i mer än 180 dagar räknat från själva omlokaliseringen ska kommissionen underrättas om den inom nämnda 180-dagarsperiod. Kommissionen ska snarast möjligt granska åtgärden och dess förenlighet med unionsrätten och om så är lämpligt vidta nödvändiga åtgärder. Kommissionen ska utbyta information om erfarenheter i detta avseende med de nationella kontaktpunkter i medlemsstaterna som avses i artikel 7.

Artikel 6

Dataportering

1. Kommissionen ska uppmuntra och underlätta utarbetandet av självreglerande uppförandekoder på unionsnivå (nedan kallade *uppförandekoder*) i syfte att bidra till en konkurrenskraftig datadriven ekonomi baserad på principerna om öppenhet och interoperabilitet och med vederbörlig hänsyn till öppna standarder, omfattande bland annat följande aspekter:

a) Bästa praxis för att underlätta såväl byte av tjänsteleverantör som dataportering i ett strukturerat, allmänt förekommande och maskinläsbart format, inbegripet format med öppna standarder där så krävs eller begärs av den tjänsteleverantör som tar emot data.

b) Minimikrav i fråga om information för att säkerställa att professionella användare innan ett avtal om databehandling ingås ges tillräckligt detaljerad, tydlig och transparent information 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.

c) Ansatser i fråga om certifieringssystem som underlättar jämförelse av produkter och tjänster för professionella användare när det gäller databehandling, med beaktande av etablerade nationella eller internationella normer, i syfte att göra det lättare att jämföra dessa produkter och tjänster. Dessa ansatser får omfatta bland annat kvalitetsstyrning samt hantering av informationssäkerhet, driftskontinuitet och miljö.

d) Kommunikationsfärdplaner med multidisciplinär ansats för att öka medvetenheten om uppförandekoderna bland berörda parter.

2. Kommissionen ska säkerställa att uppförandekoderna utarbetas i nära samarbete med alla berörda parter, däribland sammanslutningar av små och medelstora företag och uppstartsföretag, användare och molntjänsteleverantörer.

3. Kommissionen ska uppmuntra tjänsteleverantörer att slutföra utarbetandet av uppförandekoderna senast den 29 november 2019 och att genomföra dem effektivt senast den 29 maj 2020.

Artikel 7

Förfarande för samarbete mellan myndigheter

1. Varje medlemsstat ska utse en kontaktpunkt som ska hålla kontakt med kontaktpunkterna i andra medlemsstater och kommissionen vad gäller tillämpningen av denna förordning. Medlemsstaterna ska underrätta kommissionen om de utsedda kontaktpunkterna och alla ändringar av dessa.

2. Om en behörig myndighet i en medlemsstat begär assistans från en annan medlemsstat enligt artikel 5.2 för att få tillgång till data ska den lämna in en vederbörligen motiverad begäran till den sistnämnda medlemsstatens utsedda kontaktpunkt. Begäran ska inbegripa en skriftlig förklaring av skälen och de rättsliga grunderna för begäran om tillgång till data.

3. Kontaktpunkten ska identifiera den relevanta behöriga myndigheten i sin medlemsstat och översända den begäran som mottagits enligt punkt 2 till den behöriga myndigheten.

4. Den tillfrågade behöriga myndigheten ska utan onödigt dröjsmål och inom en tidsram som står i proportion till hur brådskande begäran är, tillhandahålla ett svar innehållande de data som begärts eller information till den begärande behöriga myndigheten om att den tillfrågade behöriga myndigheten inte anser att villkoren för att begära assistans enligt denna förordning är uppfyllda.

5. All information som utbyts inom ramen för assistans som begärs och tillhandahålls enligt artikel 5.2 får användas endast med avseende på det ärende för vilket den har begärts.

6. Kontaktpunkterna ska ge användarna allmän information om denna förordning, inbegripet om uppförandekoderna.

Artikel 8

Utvärdering och riktlinjer

1. Senast den 29 november 2022 ska kommissionen lägga fram en rapport för Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén som utvärderar genomförandet av denna förordning, särskilt när det gäller

a) tillämpningen av denna förordning, särskilt på datamängder som består av både personuppgifter och andra data än personuppgifter, mot bakgrund av marknadsmässig och teknisk utveckling som kan komma att öka möjligheterna att avanonymisera data,

b) medlemsstaternas genomförande av artikel 4.1, särskilt undantaget avseende allmän säkerhet, och

c) huruvida uppförandekoderna utarbetas och genomförs effektivt samt huruvida tjänsteleverantörerna verkligen tillhandahåller information.

2. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att upprätta den rapport som avses i punkt 1.

3. Senast den 29 maj 2019 ska kommissionen offentliggöra informativ vägledning om samspelet mellan denna förordning och förordning (EU) 2016/679, särskilt med avseende på datamängder som består av både personuppgifter och andra data än personuppgifter.

Artikel 9

Slutbestämmelser

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning ska börja tillämpas sex månader efter det att den har offentliggjorts.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den 14 november 2018.

På Europaparlamentets vägnar	*På rådets vägnar*
A. TAJANI	K. EDTSTADLER
Ordförande	*Ordförande*