



EUROPEISKA UNIONEN

EUROPAPARLAMENTET

RÅDET

Bryssel den 15 november 2023
(OR. en)

2022/0047 (COD)

PE-CONS 49/23

TELECOM 237
COMPET 781
MI 650
DATAPROTECT 205
JAI 1045
PI 116
CODEC 1418

LAGSTIFTNINGSAKTER OCH ANDRA INSTRUMENT

Ärende: EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om
harmoniserade regler för skälig åtkomst till och användning av data och om
ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828
(dataförordningen)

**EUROPAPARLAMENTETS OCH RÅDETS
FÖRORDNING (EU) 2023/...**

av den ...

**om harmoniserade regler för skälig åtkomst till och användning av data
och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828
(dataförordningen)**

(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 centralbankens yttrande¹,

¹ EUT C 402, 19.10.2022, s. 5.

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande¹,

med beaktande av Regionkommitténs yttrande²,

i enlighet med det ordinarie lagstiftningsförfarandet³, och

¹ EUT C 365, 23.9.2022, s. 18.

² EUT C 375, 30.9.2022, s. 112.

³ Europaparlamentets ståndpunkt av den ... (ännu inte offentliggjord i EUT) och rådets beslut av den ...

av följande skäl:

- (1) På senare år har datadriven teknik haft omdanande effekter på alla ekonomiska sektorer. Det ökade antalet produkter som är uppkopplade till internet har särskilt ökat volymen och det potentiella värdet av data för konsumenter, företag och samhälle. Högkvalitativa och interoperabla data från olika områden stärker konkurrenskraften och innovationen och säkerställer en hållbar ekonomisk tillväxt. Samma data kan användas och vidareutnyttjas för en mängd olika syften och i obegränsad omfattning, utan att dess kvalitet eller kvantitet sjunker.
- (2) Hinder för datadelning står i vägen för en optimal fördelning av data som gagnar samhället. Några exempel på sådana hinder är bristande incitament för datahållare att frivilligt ingå datadelningsavtal, osäkerhet om rättigheter och skyldigheter när det gäller data, kostnader för kontrakt och genomförande när det gäller tekniska gränssnitt, en högradigt fragmenterad information i stuprör, undermålig hantering av metadata, avsaknad av standarder för semantisk och teknisk interoperabilitet, flaskhalsar som hindrar dataåtkomst, brist på gemensam datadelningspraxis och missbruk av kontraktsmässiga obalanser när det gäller åtkomst till data och dataanvändning.

- (3) Inom sektorer som kännetecknas av förekomsten av mikroföretag och små företag och medelstora företag enligt definitionen i artikel 2.1 i bilagan till kommissionens rekommendation 2003/361/EG¹, finns det ofta en brist på digital kapacitet och färdigheter för att samla in, analysera och använda data, och åtkomsten begränsas ofta när det är en aktör som innehar data i systemet eller när interoperabiliteten är bristfällig mellan data, mellan datatjänster eller över gränser.
- (4) För att tillgodose den digitala ekonomins behov och undanröja hinder för en väl fungerande inre marknad för data är det nödvändigt att fastställa en harmoniserad ram som specificerar vem som har rätt att använda produktdata eller data från tillhörande tjänster samt villkoren och grunden för detta. Därför bör medlemsstaterna inte anta eller upprätthålla ytterligare nationella krav när det gäller frågor som omfattas av denna förordning, om det inte uttryckligen föreskrivs, eftersom detta skulle inverka på dess direkta och enhetliga tillämpning. Dessutom bör åtgärder på unionsnivå inte påverka tillämpningen av skyldigheter och åtaganden enligt internationella handelsavtal som ingås av unionen.

¹ Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

- (5) Denna förordning säkerställer att användare av en uppkopplad produkt eller tillhörande tjänst i unionen i rätt tid kan få åtkomst till de data som genereras genom användning av denna uppkopplade produkt eller tillhörande tjänst och att dessa användare kan använda dessa data, även genom att dela dem med tredje parter efter eget val. Genom denna förordning införs en skyldighet för datahållare att göra data tillgängliga för användare och tredje parter som väljs av användaren under vissa omständigheter. Denna förordning säkerställer också att datahållare gör data tillgängliga för datamottagare i unionen på rättvisa, rimliga och icke-diskriminerande villkor och på ett transparent sätt. Privaträttsliga bestämmelser är grundläggande i den allmänna ramen för datadelning. Därför anpassar denna förordning avtalsrättsliga bestämmelser och förhindrar att kontraktsmässiga obalanser som hindrar skälig åtkomst till och användning av data utnyttjas. Denna förordning säkerställer också att datahållare, om ett exceptionellt behov uppstår, ger offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan åtkomst till de data som är nödvändiga för utförandet av en specifik uppgift av allmänt intresse. Denna förordning syftar också till att underlätta byten av databehandlingstjänster och att förbättra interoperabiliteten för data och för datadelningsmekanismer och datadelningstjänster i unionen. Denna förordning bör inte tolkas som att den erkänner eller medför någon ny rättighet för datahållare att använda de data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst.

- (6) Datagenerering är resultatet av åtgärder från minst två aktörer, särskilt en uppkopplad produkts designer eller tillverkare, som i många fall också kan vara en leverantör av tillhörande tjänster, samt användaren av den uppkopplade produkten eller tillhörande tjänsten. Den ger upphov till frågor som rör rättvisa i den digitala ekonomin, eftersom de data som registreras av uppkopplade produkter eller tillhörande tjänster utgör ett viktigt underlag för eftermarknadstjänster, stödtjänster och andra tjänster. För att förverkliga de stora ekonomiska fördelarna med data, bland annat genom datadelning som bygger på frivilliga avtal och unionsföretagens utveckling av datadrivet värdeskapande, är en allmän metod för tilldelning av rättigheter avseende åtkomst till och användning av data att föredra framför tilldelning av exklusiva rättigheter avseende åtkomst och användning. I denna förordning föreskrivs horisontella regler som kan följas av unionsrätt eller nationell rätt som beaktar särskilda omständigheter inom de berörda sektorerna.

- (7) Den grundläggande rättigheten till skydd av personuppgifter skyddas i synnerhet genom Europaparlamentets och rådets förordningar (EU) 2016/679¹ och (EU) 2018/1725². Dessutom skyddar Europaparlamentets och rådets direktiv 2002/58/EG³ privatlivet och konfidentialiteten vid kommunikation, bland annat genom att fastställa villkor för all lagring av och åtkomst till personuppgifter och icke-personuppgifter i respektive från terminalutrustning. Dessa unionslagstiftningsakter ger grunden för en hållbar och ansvarsfull databehandling, även i de fall då datamängder innehåller en blandning av personuppgifter och icke-personuppgifter. Den här förordningen kompletterar, utan att påverka tillämpningen av, unionsrätt om skyddet av personuppgifter och integritet, i synnerhet förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv 2002/58/EG. Ingen bestämmelse i den här förordningen bör tillämpas eller tolkas så att den minskar eller begränsar rätten till skydd av personuppgifter eller rätten till integritet eller konfidentialitet vid kommunikation.

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 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).

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).

All behandling av personuppgifter enligt den här förordningen bör vara förenlig med unionens dataskyddslagstiftning, inbegripet kravet på en giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i tillämpliga fall, villkoren i artikel 9 i den förordningen och i artikel 5.3 i direktiv 2002/58/EG. Den här förordningen utgör inte någon rättslig grund för datahållarens insamling eller behandling av personuppgifter. Den här förordningen ålägger datahållare en skyldighet att göra personuppgifter tillgängliga för användare eller för tredje parter som väljs av en användare på den användarens begäran. Sådan åtkomst bör ges till personuppgifter som behandlas av datahållaren på grundval av någon av de rättsliga grunder som anges i artikel 6 i förordning (EU) 2016/679. Om användaren inte är den registrerade skapar den här förordningen inte någon rättslig grund för att tillhandahålla åtkomst till personuppgifter eller för att göra personuppgifter tillgängliga för en tredje part, och den bör inte tolkas som att den medför någon ny rättighet för datahållaren att använda personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst. I dessa fall kan det ligga i användarens intresse att underlätta uppfyllandet av kraven i artikel 6 i förordning (EU) 2016/679. Eftersom den här förordningen inte bör påverka registrerades dataskyddsrättigheter på ett ogynnsamt sätt, kan datahållaren i dessa fall tillmötesgå en begäran, bland annat genom att anonymisera personuppgifter eller, om lätt åtkomliga data innehåller personuppgifter angående flera registrerade, överföra endast personuppgifter som rör användaren.

- (8) Principerna om dataminimering, inbyggt dataskydd och dataskydd som standard är viktiga när behandlingen medför betydande risker för individers grundläggande rättigheter. Med beaktande av den aktuella tekniska nivån bör alla parter som deltar i datadelning, inbegripet datadelning som omfattas av denna förordning, genomföra tekniska och organisatoriska åtgärder för att skydda dessa rättigheter. Sådana åtgärder innefattar inte bara pseudonymisering och kryptering, utan även användningen av alltmer tillgänglig teknik som tillåter att algoritmer kombineras med data och ger möjlighet till värdefull inblick utan någon överföring mellan parterna eller någon onödig kopiering av rådata eller strukturerade data.
- (9) Denna förordning påverkar inte nationell avtalsrätt, inbegripet regler om avtals ingående, giltighet eller verkan, eller konsekvenserna av hävning av ett avtal, såvida inte annat föreskrivs i denna förordning. Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till att främja konsumenters intressen och säkerställa en hög nivå av konsumentskydd samt att skydda deras hälsa, säkerhet och ekonomiska intressen, i synnerhet rådets direktiv 93/13/EEG¹ och Europaparlamentets och rådets direktiv 2005/29/EG² och 2011/83/EU³.

¹ Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäligen villkor i konsumentavtal (EGT L 95, 21.4.1993, s. 29).

² Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenterna på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

³ Europaparlamentets och rådets direktiv 2011/83/EU av den 25 oktober 2011 om konsumenträttigheter och om ändring av rådets direktiv 93/13/EEG och Europaparlamentets och rådets direktiv 1999/44/EG och om upphävande av rådets direktiv 85/577/EEG och Europaparlamentets och rådets direktiv 97/7/EG (EUT L 304, 22.11.2011, s. 64).

- (10) Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter med föreskrifter om delning av, åtkomst till och användning av data i syfte att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, eller för tull- och skatteändamål, oavsett på grundval av vilken rättslig grund enligt fördraget om Europeiska unionens funktionssätt (EUF-fördraget) som sådana unionsrättsakter antogs, samt internationellt samarbete på det området, i synnerhet på grundval av Europarådets konvention om it-relaterad brottslighet (ETS nr 185), utfärdad i Budapest den 23 november 2001. Sådana rättsakter omfattar Europaparlamentets och rådets förordningar (EU) 2021/784¹, (EU) 2022/2065² och (EU) 2023/1543³ och Europaparlamentets och rådets direktiv (EU) 2023/1544⁴. Den här förordningen är inte tillämplig på insamling eller utbyte av, åtkomst till eller användning av data enligt Europaparlamentets och rådets förordning (EU) 2015/847⁵ och Europaparlamentets och rådets direktiv (EU) 2015/849⁶. Den här förordningen är inte tillämplig på områden som inte omfattas av unionsrätten och påverkar under inga omständigheter medlemsstaternas befogenheter i fråga om allmän säkerhet, försvar eller nationell säkerhet, tull- och skatteförvaltning eller medborgares hälsa och säkerhet, oavsett vilken typ av enhet som medlemsstaterna har bemyndigat att utföra uppgifter inom ramen för dessa befogenheter.

¹ Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (EUT L 172, 17.5.2021, s. 79).

² Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

³ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

⁴ Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 181).

⁵ Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006 (EUT L 141, 5.6.2015, s. 1).

⁶ Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).

- (11) Unionsrätt som fastställer den fysiska utformningen av och datakraven för produkter som ska släppas ut på unionsmarknaden bör inte påverkas, såvida det inte uttryckligen föreskrivs i denna förordning.
- (12) Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till fastställande av tillgänglighetskrav för vissa produkter och tjänster, i synnerhet Europaparlamentets och rådets direktiv (EU) 2019/882¹.
- (13) Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter som skyddar immateriella rättigheter, inbegripet Europaparlamentets och rådets direktiv 2001/29/EG², 2004/48/EG³ och (EU) 2019/790⁴.

¹ Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

² Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (EGT L 167, 22.6.2001, s. 10).

³ Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 30.4.2004, s. 45).

⁴ Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

- (14) Uppkopplade produkter som genom sina komponenter eller operativsystem erhåller, genererar eller samlar in data om sin prestanda, användning eller miljö och som kan kommunicera dessa data via en elektronisk kommunikationstjänst, via fysisk åtkomst eller via åtkomst i enheten, ofta benämnt sakernas internet, bör omfattas av denna förordning, med undantag av prototyper. Exempel på sådana elektroniska kommunikationstjänster är framför allt markbaserade telefonnät, kabel-tv-nät, satellitbaserade nät och NFC-nät (*near-field communication networks*). Uppkopplade produkter återfinns i alla aspekter av ekonomin och samhället, inbegripet i privat, civil eller kommersiell infrastruktur, fordon, hälso- och livsstilsprodukter, fartyg, flygplan, hushållsprodukter och konsumentvaror, medicinsk och hälsorelaterad utrustning och maskiner för jordbruk och industri. Tillverkarnas val av utformning och, i förekommande fall, unionsrätt eller nationell rätt som tillgodoser sektorsspecifika behov samt mål eller relevanta beslut från behöriga myndigheter bör avgöra vilka data en uppkopplad produkt kan göra tillgängliga.

- (15) Data representerar digitaliseringen av användaråtgärder och användarhändelser och bör därmed vara tillgängliga för användaren. Reglerna för åtkomst till och användning av data från uppkopplade produkter och tillhörande tjänster enligt denna förordning gäller både produktdata och data från en tillhörande tjänst. Med produktdata avses data som genereras genom användning av en uppkopplad produkt och som av tillverkaren har utformats för att kunna hämtas via den uppkopplade produkten av en användare, datahållare eller en tredje part, inbegripet, när så är lämpligt, tillverkaren. Med data från en tillhörande tjänst avses data som också representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som genereras när leverantören tillhandahåller en tillhörande tjänst. Data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst bör anses innefatta data som avsiktligt registrerats eller data som indirekt följer av användarens åtgärder, såsom data om den uppkopplade produktens miljö eller interaktion. Detta bör innefatta data om användningen av en uppkopplad produkt som genereras av ett användargränssnitt eller genom en tillhörande tjänst, och bör inte vara begränsat till information om att en sådan användning har ägt rum, utan innefatta alla data som genereras av den uppkopplade produkten till följd av sådan användning, till exempel data som genereras automatiskt av sensorer och data som registreras av inbäddade tillämpningar, inbegripet applikationer som visar maskinvarustatus och funktionsfel. Detta bör även innefatta data som genereras av den uppkopplade produkten eller en tillhörande tjänst när användaren är inaktiv, till exempel när användaren väljer att inte använda den uppkopplade produkten under en viss tid och i stället låter den vara i viloläge eller till och med avstängd, eftersom statusen för en uppkopplad produkt eller dess komponenter, till exempel dess batterier, kan variera när den uppkopplade produkten är i viloläge eller avstängd. Data som inte ändras väsentligt, dvs. data i obearbetad form, även kallade rådata eller primärdata som avser datapunkter som genereras automatiskt utan någon ytterligare form av behandling samt data som har förbehandlats i syfte att göra dem begripliga och användbara för senare behandling och analys, omfattas av denna förordning.

Sådana data innefattar data som samlas in från en enda sensor eller en uppkopplad grupp av sensorer i syfte att göra insamlade data begripliga för bredare användningsfall genom att fastställa en fysisk kvantitet eller kvalitet eller en förändring av en fysisk kvantitet, såsom temperatur, tryck, flödeshastighet, ljud, pH-värde, vätskenivå, position, acceleration eller hastighet. Begreppet *förbehandlade data* bör inte tolkas på ett sådant sätt att det införs en skyldighet för datahållaren att göra betydande investeringar i rensning och anpassning av data. De data som ska göras tillgängliga bör innefatta relevanta metadata, bland annat grundläggande information om sammanhang och tidsstämpel, för att göra datan användbar när den kombineras med andra data, såsom data sorterade och klassificerade med andra relaterade datapunkter, eller omformateras till ett allmänt använt format. Sådana data är potentiellt värdefulla för användaren och stöder innovation och utveckling av digitala och andra tjänster för att skydda miljön, människors hälsa och den cirkulära ekonomin, bland annat genom att underlätta underhåll och reparation av de uppkopplade produkterna i fråga. Information som avleds eller härleds från sådana data, som är resultatet av ytterligare investeringar i tilldelning av värden eller insikter från dessa data, särskilt med hjälp av komplexa proprietära algoritmer, inbegripet sådana som utgör en del av proprietär programvara, bör däremot inte anses omfattas av denna förordning och bör följaktligen inte omfattas av skyldigheten för en datahållare att göra dem tillgängliga för en användare eller datamottagare, såvida inte användaren och datahållaren kommit överens om något annat. Sådana data kan i synnerhet innefatta information som härleds från sensorfusion, där data infereras eller härleds från flera sensorer och samlas in i den uppkopplade produkten med hjälp av komplexa proprietära algoritmer och kan vara föremål för immateriella rättigheter.

- (16) Denna förordning gör det möjligt för användare av uppkopplade produkter att dra nytta av eftermarknadstjänster, stödtjänster och andra tjänster baserade på data som samlas in av sensorer som är inbyggda i sådana produkter, och insamlingen av dessa data är av potentiellt värde när det gäller att förbättra de uppkopplade produkternas prestanda. Det är viktigt att skilja mellan marknader för tillhandahållande av sådana sensorutrustade uppkopplade produkter och tillhörande tjänster, å ena sidan, och marknader för icke-tillhörande programvara och innehåll såsom text- och ljudinnehåll och audiovisuellt innehåll som ofta omfattas av immateriella rättigheter, å andra sidan. Därför bör denna förordning inte omfatta data som sådana uppkopplade produkter med sensorer genererar när användaren spelar in, överför, visar eller spelar innehåll, liksom själva innehållet, som ofta omfattas av immateriella rättigheter, bland annat för användning av en onlinetjänst. Denna förordning bör inte heller omfatta data som erhållits, genererats eller blivit åtkomliga från den uppkopplade produkten eller som överförts till den för lagring eller annan behandling till förmån för andra parter, som inte är användaren, vilket kan vara fallet med servrar eller molninfrastruktur som drivs av sina ägare uteslutande för tredje parts räkning, bland annat för användning av en onlinetjänst.

- (17) Det är nödvändigt att fastställa regler för produkter som vid tidpunkten för köp, hyra eller leasing är uppkopplade till en tillhörande tjänst på ett sådant sätt att den uppkopplade produkten inte skulle kunna utföra en eller flera av sina funktioner utan den eller för tjänster som tillverkaren eller en tredje part senare kopplar upp till produkten för att utöka eller anpassa den uppkopplade produktens funktionalitet. Sådana tillhörande tjänster inbegriper utbyte av data mellan den uppkopplade produkten och tjänsteleverantören och bör tolkas som att de uttryckligen är kopplade till driften av den uppkopplade produktens funktioner, till exempel tjänster som i tillämpliga fall överför kommandon till den uppkopplade produkten som kan påverka dess åtgärder eller beteende. Tjänster som inte påverkar driften av den uppkopplade produkten och som inte innebär att tjänsteleverantören överför data eller kommandon till den uppkopplade produkten bör inte betraktas som tillhörande tjänster. Sådana tjänster kan till exempel omfatta stödjande rådgivning, analyser eller finansiella tjänster samt reparation och underhåll som utförs regelbundet. Tillhörande tjänster kan erbjudas som en del av försäljnings-, hyres- eller leasingavtalet. Sådana tillhörande tjänster kan också tillhandahållas för produkter av samma typ, och användarna kan rimligtvis förvänta sig att de ska tillhandahållas med beaktande av den uppkopplade produktens art och eventuella offentliga uttalanden som gjorts av försäljaren, uthyraren eller leasegivaren eller för deras räkning, eller av andra personer i tidigare länkar i transaktionskedjan, inbegripet tillverkaren. Tillhörande tjänster kan i sig generera data av värde för användaren oberoende av datainsamlingskapaciteten i den uppkopplade produkt som de är sammankopplade med. Denna förordning bör också tillämpas på tillhörande tjänster som inte tillhandahålls av försäljaren, uthyraren eller leasegivaren själv, utan som tillhandahålls av tredje part. Om det är osäkert om tjänsten tillhandahålls som en del av försäljnings-, hyres- eller leasingavtalet bör denna förordning tillämpas. Varken strömförsörjning eller tillhandahållande av konnektivitet får tolkas som tillhörande tjänster enligt denna förordning.

- (18) Användaren av en uppkopplad produkt bör inte bara uppfattas som en fysisk eller juridisk person, såsom ett företag, en konsument eller ett offentligt organ som äger en uppkopplad produkt, har fått vissa tillfälliga rättigheter, till exempel genom ett hyres- eller leasingavtal, att få åtkomst till eller använda data som erhålls från den uppkopplade produkten, eller tar emot tillhörande tjänster för den uppkopplade produkten. Dessa åtkomsträttigheter bör, när det gäller personuppgifter som genereras av en uppkopplad produkt eller vid tillhandahållande av en tillhörande tjänst, inte på något sätt ändra eller inkräkta på rättigheterna för registrerade som kan interagera med den uppkopplade produkten eller tillhörande tjänsten. Användaren bär riskerna och åtnjuter fördelarna av användningen av den uppkopplade produkten och bör även ha åtkomst till de data som produkten genererar. Användaren bör därför ha rätt att utnyttja fördelarna av data som genereras av den berörda uppkopplade produkten och eventuella tillhörande tjänster. En ägare, uthyrare eller leasetagare bör också betraktas som användare, även när flera enheter kan betraktas som användare. När det rör sig om flera användare kan varje användare bidra på olika sätt till datagenereringen och ha ett intresse av flera olika former av användning, såsom förvaltning av fordonsparker för ett leasingföretag eller mobilitetslösningar för enskilda personer som använder en bildelningstjänst.

- (19) Med datakompetens avses färdigheter, kunskap och förståelse som gör det möjligt för användare, konsumenter och företag, särskilt mikroföretag och små och medelstora företag som omfattas av denna förordning, att dels bli medvetna om det potentiella värdet av de data de genererar, producerar och delar, dels bli motiverade att erbjuda och ge åtkomst till sina data i enlighet med relevanta rättsliga regler. Datakompetens bör omfatta mer än kunskaper om verktyg och teknik och syfta till att ge medborgare och företag förmåga och egenmakt att dra nytta av en inkluderande och rättvis datamarknad. En utbredning av åtgärder för datakompetens och införande av lämpliga uppföljningsåtgärder skulle kunna bidra till att förbättra arbetsvillkoren och i slutändan stödja dataekonomins konsolidering och innovationsbana i unionen. De behöriga myndigheterna bör främja verktyg och anta åtgärder för att förbättra datakompetensen bland de användare och enheter som omfattas av denna förordning samt öka medvetenheten om deras rättigheter och skyldigheter enligt denna förordning.

- (20) I praktiken är inte alla data som genereras av uppkopplade produkter eller tillhörande tjänster lättillgängliga för sina användare, och ofta finns endast begränsade möjligheter när det gäller portabilitet för data som genereras av produkter som är uppkopplade till internet. Användarna kan inte få fram de data som krävs för att utnyttja leverantörer av reparationstjänster eller andra tjänster, och företagen kan inte sjösätta innovativa tjänster som är mer lättanvända och effektiva. Inom många sektorer kan tillverkarna, genom sin kontroll av de uppkopplade produkternas eller de tillhörande tjänsternas tekniska design, bestämma vilka data som genereras och hur åtkomsten till dem ska ske, trots att de inte har någon laglig rätt till dessa data. Det är därför nödvändigt att säkerställa att uppkopplade produkter utformas och tillverkas, och att tillhörande tjänster tillhandahålls, på ett sådant sätt att en användare utan kostnad alltid kan få enkel och säker åtkomst till produktdata och data från den tillhörande tjänsten, inklusive tillhörande metadata som är nödvändiga för att tolka och använda dessa data, i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format, även för hämtning, användning eller delning av data. Med *lätt åtkomliga data* avses produktdata och data från en tillhörande tjänst som en datahållare, utan oproportionell ansträngning, lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, till exempel genom den uppkopplade produktens utformning, datahållarens avtal med användaren om tillhandahållande av tillhörande tjänster och dess tekniska medel för åtkomst till data. Lätt åtkomliga data omfattar inte data som genereras genom användning av en uppkopplad produkt om den uppkopplade produkten inte har utformats för att lagra eller överföra sådana data utanför den komponent i vilken de genereras eller den uppkopplade produkten som helhet.

Denna förordning bör därför inte tolkas som att den inför en skyldighet att lagra data på en uppkopplad produkts centrala datorenhet. Avsaknaden av en sådan skyldighet bör inte hindra tillverkaren eller datahållaren att frivilligt komma överens med användaren om att göra sådana anpassningar. Designskyldigheterna i denna förordning påverkar inte heller tillämpningen av principen om uppgiftsminimering i artikel 5.1 c i förordning (EU) 2016/679, och de bör inte tolkas som att de medför en skyldighet att utforma uppkopplade produkter och tillhörande tjänster på ett sådant sätt att de lagrar eller på annat sätt behandlar andra personuppgifter än personuppgifter som är nödvändiga för de ändamål för vilka de behandlas. Unionsrätt eller nationell rätt kan införas för att ange ytterligare detaljer, till exempel produktdata som bör vara åtkomliga från uppkopplade produkter eller tillhörande tjänster, eftersom sådana data kan vara nödvändiga för effektiv drift eller reparation eller effektivt underhåll av dessa uppkopplade produkter eller tillhörande tjänster. Om senare uppdateringar eller ändringar av en uppkopplad produkt eller en tillhörande tjänst från tillverkarens eller någon annan parts sida leder till ytterligare tillgängliga data eller till en begränsning av data som ursprungligen var tillgängliga, bör sådana ändringar meddelas användaren i samband med uppdateringen eller ändringen.

- (21) Om flera personer eller enheter betraktas som användare, till exempel i fall av gemensamt ägande eller om en ägare, uthyrare eller leasetagare delar rättigheter till åtkomst till eller användning av data, bör utformningen av den uppkopplade produkten, den tillhörande tjänsten eller det berörda gränssnittet göra det möjligt för varje användare att få åtkomst till de data som de genererar. Användning av uppkopplade produkter som genererar data kräver vanligtvis att användaren skapar ett användarkonto. Genom ett sådant konto kan användaren identifieras av datahållaren, som kan vara tillverkaren. Det kan också användas som ett kommunikationsmedel och för att lämna in och behandla begäranden om åtkomst till data. Om flera tillverkare eller leverantörer av tillhörande tjänster har sålt, hyrt ut eller leasat uppkopplade produkter eller tillhandahållit tillhörande tjänster, tillsammans och till samma användare, bör användaren vända sig till var och en av de parter som den har ett avtal med. Tillverkare eller designer av en uppkopplad produkt som vanligtvis används av flera personer bör införa nödvändiga mekanismer som möjliggör separata användarkonton för enskilda personer, vid behov, eller gör det möjligt för flera personer att använda samma användarkonto. Kontolösningarna bör göra det möjligt för användarna att radera sina konton och radera tillhörande data och kan göra det möjligt för användarna att avsluta åtkomsten till eller användningen eller delningen av data, eller att lämna in begäranden om detta, särskilt med beaktande av situationer där äganderätten till eller användningen av den uppkopplade produkten förändras. Användaren bör beviljas åtkomst genom ett automatiskt beviljande som verkställs på grundval av en enkel begärandemekanism, utan att det krävs någon granskning eller något godkännande från tillverkaren eller datahållaren. Detta innebär att data endast bör göras tillgängliga när användaren faktiskt önskar åtkomst. I de fall då ett automatiserat beviljande av en begäran om dataåtkomst inte är möjligt, exempelvis via ett användarkonto eller en mobilapplikation som tillhandahålls tillsammans med den uppkopplade produkten eller tillhörande tjänsten, bör tillverkaren underrätta användaren om hur åtkomst kan fås till data.

- (22) Uppkopplade produkter får vara utformade så att vissa data görs direkt tillgängliga genom datalagring i enheten eller från en fjärrserver till vilken data kommuniceras. Åtkomst till datalagringen i enheten kan möjliggöras genom kabelbaserade eller trådlösa lokala nät som är anslutna till en allmänt tillgänglig elektronisk kommunikationstjänst eller ett mobilnät. Servern kan vara tillverkarens egen lokala serverkapacitet eller den lokala serverkapaciteten hos en tredje part eller en leverantör av molntjänster. Personuppgiftsbiträden enligt definitionen i artikel 4.8 i förordning (EU) 2016/679 anses inte agera som datahållare. De kan dock särskilt ges i uppdrag att göra data tillgängliga av den personuppgiftsansvarige enligt definitionen i artikel 4.7 i förordning (EU) 2016/679. Uppkopplade produkter får vara utformade så att de tillåter användaren eller en tredje part att behandla dessa data i den uppkopplade produkten, i en databehandlingsinstans hos tillverkaren eller i en miljö för informations- och kommunikationsteknik (IKT) som användaren eller den tredje parten väljer.

- (23) Virtuella assistenter spelar en allt viktigare roll i digitaliseringen av konsument- och yrkesmiljöerna och fungerar som ett användarvänligt gränssnitt för att spela upp innehåll, erhålla information eller aktivera produkter som är uppkopplade till internet. Virtuella assistenter kan fungera som en gemensam portal för exempelvis en smart hushållsmiljö och registrera betydande mängder relevanta data om hur användarna interagerar med produkter som är uppkopplade till internet, även produkter som är tillverkade av andra parter, och kan ersätta användningen av tillverkartillhandahållna gränssnitt såsom pekskärmar och mobilappar. Användaren kan önska göra sådana data tillgängliga för tredjepartstillverkare och möjliggöra nya smarta tjänster. Virtuella assistenter bör omfattas av den rätt till dataåtkomst som föreskrivs i denna förordning. Data som genereras när användaren interagerar med en uppkopplad produkt via en virtuell assistent som tillhandahålls av någon annan än tillverkararen av den uppkopplade produkten bör också omfattas av den rätt till dataåtkomst som föreskrivs i denna förordning. Det är dock endast data som härrör från interaktionen mellan användaren och en uppkopplad produkt eller tillhörande tjänst via den virtuella assistenten som bör omfattas av denna förordning. Data som produceras av den virtuella assistenten men som inte är förbundna med användningen av en uppkopplad produkt eller tillhörande tjänst omfattas inte av denna förordning.

- (24) Innan ett avtal ingås om köp, hyra eller leasing av en uppkopplad produkt bör försäljaren, uthyraren eller leasegivaren, som kan vara tillverkaren, förse användaren med information om de produktdata som den uppkopplade produkten har möjlighet att generera, inbegripet typ, format och uppskattad volym av sådana data, på ett tydligt och begripligt sätt. Detta kan inbegripa information om datastrukturer, dataformat, vokabulärer, klassificeringssystem, taxonomier och kodförteckningar, om sådana finns tillgängliga, samt tydlig och tillräcklig information om hur data kan lagras eller hämtas eller hur åtkomst kan fås till data, inbegripet information om användningsvillkor och tjänstekvalitet för programmeringsgränssnitt eller i tillämpliga fall tillhandahållande av programvaruutvecklingsverktyg. Den skyldigheten säkrar transparens när det gäller genererade produktdata och förenklar åtkomsten för användaren. Informationsskyldigheten skulle kunna fullgöras, till exempel genom en stabil webbadress (URL) som kan distribueras som en webblänk eller QR-kod och hänvisa till relevant information som försäljaren, uthyraren eller leasegivaren, som får vara tillverkaren, kan tillhandahålla användaren innan avtalet om köp, hyra eller leasing av en uppkopplad produkt ingås. Det är under alla omständigheter nödvändigt att användaren kan lagra informationen på ett sätt som medger åtkomst för användning i framtiden och som tillåter oförändrad återgivning av den lagrade informationen.

Datahållaren kan inte förväntas lagra data på obestämd tid med tanke på behoven hos användaren av den uppkopplade produkten men bör tillämpa en rimlig policy för lagring av data, i förekommande fall i enlighet med principen om lagringsminimering enligt artikel 5.1 e i förordning (EU) 2016/679, som möjliggör en effektiv tillämpning av rätten till dataåtkomst enligt den här förordningen. Skyldigheten att lämna information påverkar inte den personuppgiftsansvarigas skyldighet att lämna information till den registrerade enligt artiklarna 12, 13 och 14 i förordning (EU) 2016/679. Den potentiella datahållaren bör ha skyldighet att lämna information innan ett avtal om tillhandahållande av en tillhörande tjänst ingås, oavsett om datahållaren ingår ett avtal om köp, hyra eller leasing av en uppkopplad produkt. Om informationen ändras under den uppkopplade produktens livslängd eller under avtalsperioden för den tillhörande tjänsten, liksom när det ändamål för vilket dessa data ska användas ändras i förhållande till det ursprungligen angivna ändamålet, bör denna information också lämnas till användaren.

- (25) Denna förordning bör inte tolkas som att den medför någon ny rättighet för datahållare att använda produktdata eller data från en tillhörande tjänst. Om tillverkaren av en uppkopplad produkt är en datahållare, bör tillverkarens användning av icke-personuppgifter grundas på ett avtal mellan tillverkaren och användaren. Ett sådant avtal kan ingå i ett avtal om tillhandahållande av den tillhörande tjänsten, som kan ingås tillsammans med försäljnings-, hyres- eller leasingavtalet för den uppkopplade produkten. Varje avtalsvillkor som föreskriver att datahållaren får använda produktdata eller data från en tillhörande tjänst bör vara transparenta för användaren, även vad gäller det ändamål för vilket datahållaren avser att använda berörda data. Sådana ändamål skulle bland annat kunna vara att förbättra funktionen hos den uppkopplade produkten eller de tillhörande tjänsterna, att utveckla nya produkter eller tjänster eller att aggregera data i syfte att göra de resulterande härledda data tillgängliga för tredje parter, förutsatt att sådana härledda data inte gör det möjligt att identifiera de specifika data som överförs till datahållaren från den uppkopplade produkten eller gör det möjligt för en tredje part att härleda dessa data från datamängden. Varje ändring av avtalet bör vara beroende av användarens informerade samtycke. Denna förordning hindrar inte parter från att komma överens om avtalsvillkor vars effekt är att utesluta eller begränsa en datahållares användning av icke-personuppgifter, eller vissa kategorier av icke-personuppgifter. Den hindrar inte heller parter från att komma överens om att göra produktdata eller data från en tillhörande tjänst tillgängliga för tredje parter, direkt eller indirekt, inbegripet, i tillämpliga fall, via en annan datahållare. Denna förordning hindrar inte heller sektorsspecifika regleringskrav enligt unionsrätten, eller nationell rätt som är förenlig med unionsrätten, som skulle utesluta eller begränsa datahållarens användning av vissa sådana data av tydligt definierade skäl grundade på offentlig policy. Denna förordning hindrar inte att användare vid förbindelser mellan företag gör data tillgängliga för tredje parter eller datahållare enligt något lagligt avtalsvillkor, bland annat genom att samtycka till att begränsa eller inskränka vidare delning av sådana data, eller att de får proportionell ersättning, till exempel i utbyte mot att de avstår från sin rätt att använda eller dela sådana data. Trots att begreppet *datahållare* i allmänhet inte omfattar offentliga organ kan det dock omfatta offentliga företag.

- (26) För att främja uppkomsten av likvida, rättvisa och effektiva marknader för icke-personuppgifter bör användare av uppkopplade produkter kunna dela data med andra, även för kommersiella ändamål, med minimala rättsliga och tekniska insatser. Det är för närvarande ofta svårt för företag att motivera de personal- eller databehandlingskostnader som är nödvändiga för att förbereda datamängder som inte består av personuppgifter eller dataprodukter och erbjuda dem till potentiella motparter via dataförmedlingstjänster, inbegripet datamarknader. Ett betydande hinder för företagens delning av icke-personuppgifter är därför en följd av bristen på förutsägbarhet när det gäller ekonomisk avkastning från investeringar i kurer och tillgängliggörande av datamängder eller dataprodukter. För att möjliggöra uppkomsten av likvida, rättvisa och effektiva marknader för icke-personuppgifter i unionen måste det klargöras vilken part som har rätt att erbjuda sådana data på en marknad. Användare bör därför ha rätt att dela icke-personuppgifter med datamottagare för kommersiella och icke-kommersiella ändamål. Sådan datadelning kan utföras direkt av användaren, på begäran av användaren via en datahållare, eller genom dataförmedlingstjänster. Dataförmedlingstjänster, som regleras i Europaparlamentets och rådets förordning (EU) 2022/868¹, skulle kunna underlätta en dataekonomi genom att upprätta affärsförbindelser mellan användare, datamottagare och tredje parter och kan hjälpa användare att utöva sin rätt att använda data, till exempel genom att säkerställa anonymisering av personuppgifter eller aggregering av åtkomst till data från flera enskilda användare. Om data undantas från en datahållares skyldighet att göra dem tillgängliga för användare eller tredje parter kan omfattningen av sådana data specificeras i avtalet mellan användaren och datahållaren om tillhandahållande av en tillhörande tjänst så att användarna enkelt kan fastställa vilka data som är tillgängliga för dem för delning med datamottagare eller tredje parter. Datahållare bör inte göra produktdata som inte består av personuppgifter tillgängliga för tredje parter för kommersiella eller icke-kommersiella ändamål annat än för att fullgöra avtalet med användaren, utan att det påverkar rättsliga krav enligt unionsrätten eller nationell rätt och som innebär att en datahållare ska göra data tillgängliga. Vid behov bör datahållare genom avtal förbinda tredje parter att inte dela vidare data som de har mottagit från dem.

¹ Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1).

- (27) Inom sektorer som kännetecknas av koncentration av ett litet antal tillverkare som levererar uppkopplade produkter till slutanvändarna kan det förekomma att det endast finns ett begränsat antal alternativ för användarna vad gäller åtkomst till och användning och delning av data. Under sådana omständigheter kan avtal vara otillräckliga för att uppnå målet att stärka användarnas egenmakt, vilket gör det svårt för användarna att få ut ett värde från de data som genereras av de uppkopplade produkter som de köper, hyr eller leasar. Därmed finns det bara begränsade möjligheter för innovativa mindre företag att erbjuda databaserade lösningar på ett konkurrenskraftigt sätt och för en diversifierad dataekonomi i unionen. Denna förordning bör därför bygga vidare på senare tids utveckling inom enskilda sektorer, såsom uppförandekoden för delning av jordbruksdata genom avtal. Unionsrätt eller nationell rätt kan antas för att hantera sektorsspecifika behov och mål. Datahållare bör inte heller använda lätt åtkomliga data som är icke-personuppgifter för att få inblick i användarens ekonomiska situation, tillgångar eller produktionsmetoder eller i sådan användning från användarens sida som på något annat sätt skulle kunna undergräva användarens affärsmässiga ställning på de marknader där denne är verksam. Detta skulle kunna innefatta att använda kunskap om ett företags eller ett jordbruks allmänna resultat i avtalsförhandlingar med användaren om potentiella förvärv av användarens produkter eller jordbruksprodukter till skada för användaren, eller att använda sådan information i aggregerad form för inmatning i större databaser om vissa marknader, till exempel databaser om skördeavkastningen för den kommande skördesäsongen, eftersom en sådan användning indirekt skulle kunna påverka användaren negativt. Användaren bör förse med det tekniska gränssnitt som behövs för hantering av tillstånd, företrädesvis med detaljerade tillståndsalternativ, såsom ”tillåt en gång” eller ”tillåt när denna app eller tjänst används”, inklusive alternativet att återkalla sådana tillstånd.

- (28) I avtal mellan en datahållare och en konsument som är användare av en uppkopplad produkt eller tillhörande tjänst som genererar data bör unionens konsumentlagstiftning, särskilt direktiven 93/13/EEG och 2005/29/EG tillämpas för att säkerställa att en konsument inte omfattas av oskäliga avtalsvillkor. Vid tillämpningen av denna förordning bör oskäliga avtalsvillkor som ensidigt åläggs ett företag inte vara bindande för företaget.
- (29) Datahållare kan kräva lämplig användaridentifiering för att kontrollera en användares rätt till dataåtkomst. När det gäller personuppgifter som behandlas av ett personuppgiftsbiträde på uppdrag av den personuppgiftsansvarige bör datahållare säkerställa att begäran om åtkomst tas emot och hanteras av personuppgiftsbiträdet.
- (30) Användaren bör vara fri att använda dessa data för alla lagliga ändamål. Detta innefattar att tillhandahålla de data som användaren har erhållit vid utövandet av sina rättigheter enligt denna förordning åt en tredje part som erbjuder en eftermarknadstjänst som kan konkurrera med en tjänst som tillhandahålls av en datahållare, eller instruera datahållaren att göra detta. Begäran bör lämnas in av användaren eller en tredje part som har rätt att agera för användarens räkning, inbegripet en leverantör av en dataförmedlingstjänst. Datahållare bör säkerställa att de data som görs tillgängliga för den tredje parten är lika korrekta, fullständiga, tillförlitliga, relevanta och aktuella som de data som datahållaren själv kan ha eller har rätt att få åtkomst till från användningen av den uppkopplade produkten eller den tillhörande tjänsten. Eventuella immateriella rättigheter bör respekteras vid hanteringen av data. Det är viktigt att bevara incitamenten för investering i produkter med funktioner som baseras på användningen av data från sensorer som är inbyggda i dessa produkter.

- (31) I Europaparlamentets och rådets direktiv (EU) 2016/943¹ föreskrivs att anskaffande, utnyttjande eller röjande av en företagshemlighet ska anses som lagligt, bland annat om sådant anskaffande, utnyttjande eller röjande krävs eller medges enligt unionsrätten eller nationell rätt. Enligt denna förordning krävs att datahållare röjer vissa data för användarna, eller för de tredje parter som väljs av en användare, även när dessa data uppfyller kraven för skydd i egenskap av företagshemligheter; den bör dock tolkas på ett sådant sätt att skyddet för företagshemligheter enligt direktiv (EU) 2016/943 bevaras. I detta sammanhang bör datahållare kunna kräva att användarna, eller de tredje parter som väljs av en användare, bevarar konfidentialiteten hos data som betraktas som företagshemligheter. Datahållare bör därför identifiera företagshemligheter innan data röjs och ha möjlighet att komma överens med användarna, eller de tredje parter som väljs av en användare, om nödvändiga åtgärder för att bevara deras konfidentialitet, bland annat användning av standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder. Utöver användning av standardavtalsvillkor som ska utarbetas och rekommenderas av kommissionen skulle ett fastställande av uppförandekoder och tekniska standarder för skydd av företagshemligheter vid hantering av data kunna bidra till att syftet med denna förordning uppnås, och det bör därför uppmuntras. Om det inte finns något avtal om de nödvändiga åtgärderna eller om en användare, eller de tredje parter som väljs av en användare, underlåter att genomföra överenskomna åtgärder eller äventyrar konfidentialiteten för företagshemligheter bör datahållaren kunna hindra eller avbryta delningen av data som identifierats som företagshemligheter.

¹ Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

I sådana fall bör datahållaren meddela användaren eller den tredje parten beslutet skriftligen utan oskäligt dröjsmål och underrätta den behöriga myndigheten i den medlemsstat där datahållaren är etablerad om att den har hindrat eller avbrutit datadelningen och identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, vilka företagshemligheter som har äventyrats. Datahållare kan i princip inte avslå en begäran om åtkomst till data enligt denna förordning enbart på grundval av att vissa data anses vara en företagshemlighet, eftersom detta skulle undergräva de avsedda verkningarna av denna förordning. Under särskilda omständigheter bör dock en datahållare som är innehavare av en företagshemlighet från fall till fall kunna avslå en begäran om åtkomst till de specifika data i fråga om den kan visa för användaren eller den tredje parten att röjandet av den företagshemligheten, trots tekniska och organisatoriska åtgärder som vidtas av användaren eller av den tredje parten, med stor sannolikhet kommer att orsaka allvarlig ekonomisk skada. Allvarlig ekonomisk skada innebär allvarliga och irreparabla ekonomiska förluster. Datahållaren bör utan oskäligt dröjsmål vederbörligen motivera sitt avslag skriftligen för användaren eller den tredje parten och underrätta den behöriga myndigheten. Denna motivering bör bygga på objektiva faktorer som visar den konkreta risken för allvarlig ekonomisk skada som väntas uppstå till följd av ett visst röjande av data och skälen till att de åtgärder som vidtagits för att skydda de data som begärts inte anses vara tillräckliga. Eventuell negativ inverkan på cybersäkerheten kan beaktas i detta sammanhang. Om användaren eller en tredje part vill bestrida datahållarens beslut att vägra eller att hindra eller avbryta delningen av data kan användaren eller den tredje parten, utan att det påverkar rätten att få sin sak prövad i en domstol, lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål bör besluta huruvida och på vilka villkor datadelning bör inledas eller återupptas eller kan komma överens med datahållaren om att hänskjuta frågan till ett tvistlösningsorgan. Undantagen från rätten till dataåtkomst enligt denna förordning bör under inga omständigheter begränsa de registrerades rätt till tillgång och rätt till dataportabilitet enligt förordning (EU) 2016/679.

- (32) Syftet med denna förordning är inte enbart att främja utvecklingen av nya innovativa uppkopplade produkter eller tillhörande tjänster och stimulera innovation på eftermarknaderna, utan även att stimulera utvecklingen av helt nya tjänster som utnyttjar berörda data, även baserat på data från en rad olika uppkopplade produkter eller tillhörande tjänster. Samtidigt syftar denna förordning till att undvika att undergräva investeringsincitamenten för den typ av uppkopplad produkt som data erhålls från, exempelvis genom användning av data för utveckling av en konkurrerande uppkopplad produkt som av användarna betraktas som likvärdig eller utbytbar, särskilt på grund av den uppkopplade produktens egenskaper, pris och avsedda användning. I denna förordning föreskrivs inget förbud mot utveckling av en tillhörande tjänst med hjälp av data som erhålls enligt denna förordning, eftersom detta skulle ha en oönskad avskräckande effekt på innovation. Att förbjuda användning av data som görs tillgängliga enligt denna förordning för att utveckla konkurrerande uppkopplade produkter skyddar datahållares innovationsinsatser. Huruvida en uppkopplad produkt konkurrerar med den uppkopplade produkt som data härrör från beror på om de båda uppkopplade produkterna konkurrerar på samma produktmarknad. Detta bör fastställas på grundval av de principer i unionens konkurrenslagstiftning som fastslagits för att definiera den relevanta produktmarknaden. Lagliga ändamål för användningen av data kan dock omfatta bakåtkompilering, under förutsättning den uppfyller kraven i denna förordning och i unionsrätten eller nationell rätt. Detta kan vara fallet när det gäller reparation eller förlängning av en uppkopplad produkts livslängd eller tillhandahållande av eftermarknadstjänster för uppkopplade produkter.

- (33) En tredje part som ges tillgång till data kan vara en fysisk eller juridisk person, till exempel en konsument, ett företag, en forskningsorganisation, en organisation utan vinstsyfte eller en enhet som agerar i egenskap av näringsidkare. När en datahållare gör data tillgängliga för den tredje parten bör datahållaren inte missbruka sin ställning för att uppnå en konkurrensfördel på marknader där datahållaren och den tredje parten kan stå i direkt konkurrens med varandra. Datahållaren bör därför inte använda några lätt åtkomliga data för att få inblick i den tredje partens ekonomiska situation, tillgångar eller produktionsmetoder eller i användningen på något annat sätt som skulle kunna undergräva den tredje partens affärsmässiga ställning på de marknader där den tredje parten är verksam. Användaren bör kunna dela icke-personuppgifter med tredje parter för kommersiella ändamål. Efter överenskommelse med användaren, och om inte annat följer av bestämmelserna i denna förordning, bör tredje parter kunna överföra de rättigheter till dataåtkomst som användaren beviljat andra tredje parter, även i utbyte mot ersättning. Dataförmedlare mellan företag och system för hantering av personuppgifter (PIMS), kallade dataförmedlingstjänster i förordning (EU) 2022/868, kan stödja användarna eller de tredje parterna vid upprättandet av affärsförbindelser med ett obestämt antal potentiella motparter för alla lagliga ändamål som omfattas av den här förordningen. De skulle kunna spela en avgörande roll när det gäller att aggregera åtkomst till data så att stordataanalyser eller maskininlärning kan underlättas, förutsatt att användare har full kontroll över huruvida deras data ska tillhandahållas för sådan aggregering och de kommersiella villkor enligt vilka deras data kommer att användas.

- (34) Användningen av en uppkopplad produkt eller tillhörande tjänst kan, i synnerhet när användaren är en fysisk person, generera data som rör den registrerade. Behandlingen av sådana data omfattas av de regler som fastställs inom ramen för förordning (EU) 2016/679, även när personuppgifter och icke-personuppgifter i en datamängd hänger ouppslutligt samman. Den registrerade kan vara användaren eller en annan fysisk person. Personuppgifter får endast begäras av den personuppgiftsansvarige eller den registrerade. En användare som är den registrerade har under vissa omständigheter enligt förordning (EU) 2016/679 rätt att få åtkomst till sina personuppgifter, och dessa rättigheter påverkas inte av den här förordningen. Enligt den här förordningen har en användare som är en fysisk person dessutom rätt att få åtkomst till alla data som genereras genom användning av en uppkopplad produkt, oavsett om det handlar om personuppgifter eller icke-personuppgifter. Om användaren inte är den registrerade utan ett företag, inbegripet ett enmansföretag, och det inte är ett gemensamt hushåll som använder den uppkopplade produkten, ska användaren anses vara en personuppgiftsansvarig. Följaktligen måste en sådan användare som i egenskap av personuppgiftsansvarig avser att begära personuppgifter som genererats genom användning av en uppkopplad produkt eller tillhörande tjänst ha en rättslig grund för behandling av data i enlighet med artikel 6.1 i förordning (EU) 2016/679, såsom samtycke av den registrerade eller fullgörande av ett avtal som den registrerade är part i. En sådan användare bör säkerställa att den registrerade på lämpligt sätt informeras om de särskilda, uttryckligt angivna och berättigade ändamålen för behandlingen av berörda data, och om hur den registrerade kan utöva sina rättigheter i praktiken. Om datahållaren och användaren är gemensamt personuppgiftsansvariga i den mening som avses i artikel 26 i förordning (EU) 2016/679 måste de, på ett transparent sätt genom ett arrangemang sinsemellan, fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt den förordningen. Det bör anses att en sådan användare, när berörda data har gjorts tillgängliga, i sin tur kan bli datahållare, om användaren uppfyller kriterierna enligt den här förordningen och därmed omfattas av skyldigheten att göra data tillgängliga enligt den här förordningen.

- (35) Produktdata eller data från en tillhörande tjänst bör endast göras tillgängliga för en tredje part på användarens begäran. Denna förordning kompletterar därmed den rättighet som föreskrivs i artikel 20 i förordning (EU) 2016/679, nämligen att den registrerade har rätt att få ut sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig, när dessa uppgifter behandlas automatiserat på grundval av artikel 6.1 a eller artikel 9.2 a eller på grundval av ett avtal enligt artikel 6.1 b i den förordningen. Den registrerade har också rätt att få dessa personuppgifter överförda direkt från en personuppgiftsansvarig till en annan, men endast när detta är tekniskt möjligt. I artikel 20 i förordning (EU) 2016/679 specificeras att detta avser data som tillhandahålls av den registrerade, men det anges inte om det förutsätter en aktiv handling från den registrerades sida eller om det också gäller för situationer där en uppkopplad produkt eller tillhörande tjänst genom sin konstruktion på ett passivt sätt iakttar en registrerads beteende eller annan information som rör en registrerad.
- Rättigheterna enligt den här förordningen kompletterar rätten att få ut och portera personuppgifter enligt artikel 20 i förordning (EU) 2016/679 på ett antal sätt. Den förordningen ger användaren rätt att få åtkomst och ge tredje part tillgång till alla produktdata eller data från en tillhörande tjänst, oavsett om det rör sig om personuppgifter, utan någon skillnad mellan data som aktivt görs tillgängliga och data som passivt iakttas, och oavsett den rättsliga grunden för behandlingen. Till skillnad från artikel 20 i förordning (EU) 2016/679 kräver och säkerställer den här förordningen den tekniska genomförbarheten för tredjepartsåtkomst till alla typer av data som omfattas av den här förordningens tillämpningsområde, oavsett om det handlar om personuppgifter eller icke-personuppgifter, och därigenom säkerställs att tekniska hinder inte längre står i vägen för eller förhindrar åtkomsten till sådana data. Den ger också datahållare rätt att fastställa rimlig ersättning som ska betalas av tredje parter, men inte av användaren, för kostnader som uppstår när direkt åtkomst ges till de data som genereras av användarens uppkopplade produkt. Om en datahållare och en tredje part inte kan enas om villkoren för sådan direkt åtkomst bör den registrerade inte på något sätt hindras från att utöva de rättigheter som fastställs i förordning (EU) 2016/679, inbegripet rätten till dataportabilitet, genom att utnyttja rättsmedel i enlighet med den förordningen. Det bör i detta sammanhang förstås att enligt förordning (EU) 2016/679 tillåter ett avtal inte behandling av särskilda kategorier av personuppgifter från datahållarens eller den tredje partens sida.

- (36) Åtkomst till data som lagras och nås från terminalutrustning omfattas av direktiv 2002/58/EG och förutsätter ett samtycke från abonnenten eller användaren i den mening som avses i det direktivet, om det inte är strikt nödvändigt för tillhandhållandet av en informationssamhällestjänst som uttryckligen begärs av användaren eller abonnenten eller endast i syfte att överföra ett meddelande. Direktiv 2002/58/EG skyddar integriteten för en användares terminalutrustning i fråga om användningen av behandlings- och lagringskapacitet och insamling av information. Utrustning för sakernas internet betraktas som terminalutrustning om den är direkt eller indirekt ansluten till ett allmänt kommunikationsnät.
- (37) För att förhindra att användare utnyttjas bör tredje parter som fått tillgång till data på användarens begäran endast behandla dessa data för de ändamål som överenskommits med användaren och endast dela dem med annan tredje part med användarens samtycke till en sådan datadelning.

- (38) I enlighet med principen om uppgiftsminimering bör tredje parter endast få tillgång till information som är nödvändig för tillhandahållandet av den tjänst som begärts av användaren. När den tredje parten fått tillgång till data bör den behandla dessa data för de ändamål som överenskommits med användaren, utan inblandning från datahållaren. Det bör vara enkelt för användaren att vägra eller avbryta tredje parts tillgång till data eftersom det är användarens sak att godkänna åtkomsten. Varken tredje parter eller datahållare bör på något sätt göra det orimligt svårt för användaren att göra sina val eller utöva sina rättigheter, inbegripet genom att erbjuda användaren val på ett icke-neutralt sätt, eller genom att utöva tvång mot, vilseleda eller manipulera användaren eller undergräva eller inskränka användarens handlingsfrihet, beslutsfattande eller val, inbegripet genom ett digitalt användargränssnitt eller en del därav. I detta sammanhang bör tredje parter eller datahållare inte förlita sig på så kallade mörka mönster i designen av sina digitala gränssnitt. Mörka mönster är designtechniker som driver eller vilseleder konsumenter till beslut som har negativa konsekvenser för dem. Dessa manipulationstekniker kan användas för att övertyga användarna, i synnerhet utsatta konsumenter, att ägna sig åt oönskat beteende, för att vilseleda dem genom att ”puffa” dem så att de fattar beslut om att lämna ut data eller för att otillbörligt påverka de beslut som fattas av tjänstens användare på ett sådant sätt att det undergräver eller inskränker deras handlingsfrihet, beslutsfattande och valfrihet. Gemensamma och legitima affärsmetoder som är förenliga med unionsrätten bör inte i sig anses utgöra mörka mönster. Tredje parter och datahållare bör fullgöra sina skyldigheter enligt berörd unionsrätt, i synnerhet kraven i Europaparlamentets och rådets direktiv 98/6/EG¹ och 2000/31/EG² samt i direktiven 2005/29/EG och 2011/83/EU.

¹ Europaparlamentets och rådets direktiv 98/6/EG av den 16 februari 1998 om konsumentskydd i samband med prismärkning av varor som erbjuds konsumenter (EGT L 80, 18.3.1998, s. 27).

² 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).

- (39) Tredje parter bör också avstå från att använda data som omfattas av denna förordning för profilering av individer om inte sådan behandling är strikt nödvändig för tillhandahållandet av den tjänst som begärs av användaren, bland annat i samband med automatiserat beslutsfattande. Kravet att radera data när de inte längre krävs för det ändamål som överenskommits med användaren, om inte annat överenskommits när det gäller icke-personuppgifter, kompletterar den registrerades rätt till radering enligt artikel 17 i förordning (EU) 2016/679. När en tredje part är en leverantör av en dataförmedlingstjänst tillämpas de skyddsåtgärder för den registrerade som föreskrivs i förordning (EU) 2022/868. Den tredje parten får använda data för att utveckla en ny och innovativ uppkopplad produkt eller tillhörande tjänst men inte för att utveckla en konkurrerande uppkopplad produkt.

- (40) Uppstartsföretag, små företag, företag som betraktas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG samt företag från traditionella sektorer med mindre utvecklad digital kapacitet har svårt att få åtkomst till relevanta data. Denna förordning syftar till att underlätta åtkomsten till data för dessa enheter och samtidigt säkerställa att de motsvarande skyldigheterna är så proportionella som möjligt så att de inte blir alltför betungande. Samtidigt har ett litet antal mycket stora företag med betydande ekonomisk styrka vuxit fram i den digitala ekonomin genom ackumulering och aggregering av enorma datavolymer och den tekniska infrastrukturen för monetarisering av data. Dessa mycket stora företag inkluderar företag som tillhandahåller centrala plattformstjänster och kontrollerar hela plattformsekosystem i den digitala ekonomin och som befintliga eller nya marknadsaktörer inte kan utmana eller konkurrera med. Europaparlamentets och rådets förordning (EU) 2022/1925¹ syftar till att avhjälpa dessa ineffektiva aspekter och obalanser genom att tillåta att kommissionen utser ett företag till grindvakt, och inför ett antal skyldigheter för sådana grindvakter, inbegripet ett förbud mot att kombinera vissa data utan samtycke, och en skyldighet att säkerställa en rätt till effektiv dataportabilitet i enlighet med artikel 20 i förordning (EU) 2016/679. Enligt med förordning (EU) 2022/1925) och mot bakgrund av dessa företags unika möjlighet att förvärva data, är det inte nödvändigt för uppnåendet av den här förordningens mål, och därför oproportionellt för datahållare som omfattas av sådana skyldigheter, att låta grindvakter omfattas av rätten till dataåtkomst.

¹ Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1).

Om sådana företag omfattades skulle sannolikt även fördelarna med den här förordningen begränsas för mikroföretag och små och medelstora företag med avseende på en rättvis fördelning av datavärdet mellan marknadsaktörerna. Detta betyder att ett företag som tillhandahåller centrala plattformstjänster som har utsetts till grindvakt inte kan begära eller beviljas åtkomst till användares data som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst eller av en virtuell assistent enligt den här förordningen. Dessutom får tredje parter som får tillgång till data på begäran av användaren inte göra dessa data tillgängliga för en grindvakt. Den tredje parten får exempelvis inte lägga ut tjänstetillhandahållandet på entreprenad hos en grindvakt. Detta hindrar dock inte tredje parter från att använda databehandlingstjänster som erbjuds av en grindvakt. Det hindrar inte heller dessa företag från att erhålla och använda samma data på annat lagligt sätt. Åtkomsträttigheterna enligt den här förordningen bidrar till ett större urval av tjänster för konsumenter. Eftersom frivilliga avtal mellan grindvakter och datahållare inte påverkas, skulle begränsningen när det gäller beviljande av åtkomst för grindvakter inte utesluta dem från marknaden eller hindra dem från att erbjuda sina tjänster.

- (41) Med tanke på det nuvarande tekniska läget vore det alltför betungande för mikroföretag och små företag att införa ytterligare designskyldigheter avseende uppkopplade produkter som tillverkas eller designas av mikroföretag och små företag eller tillhörande tjänster som tillhandahålls av dem. Detta gäller dock inte om ett mikroföretag eller ett litet företag har ett partnerföretag eller ett anknutet företag i den mening som avses i punkt 3 i bilagan till rekommendation 2003/361/EG som inte betecknas som ett mikroföretag eller ett litet företag och när det tillverkar eller utformar en uppkopplad produkt eller tillhandahåller en tillhörande tjänst på entreprenad. I sådana situationer kan det företag som har lagt ut tillverkningen eller designen på entreprenad på ett mikroföretag eller ett litet företag ersätta detta på lämpligt sätt. Ett mikroföretag eller ett litet företag kan dock ändå omfattas av krav enligt denna förordning såsom datahållare, om det inte är den uppkopplade produktens tillverkare eller leverantör av tillhörande tjänster. En övergångsperiod bör vara tillämplig för ett företag som har betraktats som ett medelstort företag i mindre än ett år och för uppkopplade produkter under ett år från den dag då de släpptes ut på marknaden av ett medelstort företag. En sådan övergångsperiod på ett år ger det medelstora företaget möjlighet att anpassa och förbereda sig innan de utsätts för konkurrens på tjänstemarknaden för de uppkopplade produkter som de tillverkar, på grundval av de åtkomsträttigheter som föreskrivs i denna förordning. En sådan övergångsperiod är inte tillämplig när ett sådant medelstort företag har ett partnerföretag eller ett anknutet företag som inte betecknas som ett mikroföretag eller ett litet företag eller när ett sådant medelstort företag tillverkade eller utformade den uppkopplade produkten eller tillhandahöll den tillhörande tjänsten på entreprenad.

- (42) Med beaktande av mångfalden av uppkopplade produkter, vilka producerar data av olika art, volym och frekvens, uppvisar olika nivåer av datarelaterade risker och cybersäkerhetsrisker och ger ekonomiska möjligheter av olika värde, och för att säkerställa enhetlig datadelningspraxis på den inre marknaden, även mellan sektorer, samt uppmuntra och främja rättvis datadelningspraxis även på områden där ingen sådan rätt till dataåtkomst föreskrivs, fastställs i denna förordning övergripande regler om villkoren för åtkomst till data närhelst en datahållare enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten är skyldig att göra data tillgängliga för en datamottagare. Sådan åtkomst bör baseras på rättvisa, rimliga, icke-diskriminerande och transparenta villkor. Dessa allmänna åtkomstregler bör inte tillämpas på skyldigheter att göra data tillgängliga enligt förordning (EU) 2016/679. Frivillig datadelning påverkas inte av dessa regler. De icke-bindande standardavtalsvillkor för datadelning mellan företag som ska utarbetas och rekommenderas av kommissionen kan hjälpa parterna att ingå avtal som innehåller rättvisa, rimliga och icke-diskriminerande villkor och som genomförs på ett transparent sätt. Ingåendet av ett sådant avtal, som kan inkludera de icke-bindande standardavtalsvillkoren, bör inte innebära att rätten att dela data med tredje parter på något sätt är avhängig av att det finns ett sådant avtal. Om parterna inte kan ingå ett avtal om datadelning, inbegripet med stöd av tvistlösningsorgan, kan rätten att dela data med tredje parter inte åberopas i nationella domstolar.

- (43) På grundval av principen om avtalsfrihet bör parterna fortsatt vara fria att förhandla fram de exakta villkoren för att göra data tillgängliga i sina avtal, inom ramen för de allmänna åtkomstreglerna för tillgängliggörandet av data. Villkoren i sådana avtal kan omfatta tekniska och organisatoriska åtgärder, bland annat i samband med datasäkerhet.
- (44) För att säkerställa att villkoren för obligatorisk dataåtkomst är rättvisa för båda parter i ett avtal bör de allmänna reglerna för rätten till dataåtkomst hänvisa till regeln om undvikande av oskäligen avtalsvillkor.
- (45) Eventuella avtal mellan företag om att göra data tillgängliga bör vara icke-diskriminerande mellan jämförbara kategorier av datamottagare, oberoende av om parterna är stora företag, mikroföretag eller små och medelstora företag. För att kompensera bristen på information om villkoren i olika avtal, som gör det svårt för datamottagaren att bedöma om villkoren för att göra data tillgängliga är icke-diskriminerande, bör det vara datahållarnas ansvar att visa att ett avtalsvillkor inte är diskriminerande. Det rör sig inte om olaglig diskriminering om en datahållare använder olika avtalsvillkor för att göra data tillgängliga om dessa skillnader är motiverade av objektiva skäl. Dessa skyldigheter bör inte påverka tillämpningen av förordning (EU) 2016/679.

- (46) För att uppmuntra fortsatta investeringar i generering och tillgängliggörande av värdefulla data, inbegripet investeringar i relevanta tekniska verktyg, och samtidigt undvika alltför stora bördor för åtkomst till och användning av data som gör att datadelningen inte längre blir affärsmässigt lönsam, omfattar denna förordning principen att datahållare vid förbindelser mellan företag får begära en rimlig ersättning i de fall då dessa enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten är skyldiga att göra data tillgängliga för en datamottagare. Sådan ersättning bör inte anses utgöra betalning för dessa data som sådana. Kommissionen bör anta riktlinjer för beräkningen av en rimlig ersättning i dataekonomin.

- (47) För det första kan en rimlig ersättning för att fullgöra skyldigheten enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten att tillmötesgå en begäran om att göra data tillgängliga inbegripa ersättning för de kostnader som uppstår till följd av att data görs tillgängliga. Dessa kostnader kan vara tekniska kostnader, såsom kostnader som är nödvändiga för återgivning av data, spridning på elektronisk väg och lagring av data, men inte för datainsamling eller dataproduktion. Sådana tekniska kostnader kan även omfatta de behandlingskostnader som är nödvändiga för att göra data tillgängliga, inbegripet kostnader i samband med formatering av data. Kostnaderna för att göra data tillgängliga kan också omfatta kostnaderna för att i praktiken underlätta begäranden om datadelning. De kan också variera beroende på datavolymen och de åtgärder som vidtas för att göra data tillgängliga. Långsiktiga arrangemang mellan datahållare och datamottagare, exempelvis genom en abonnemangsmodell eller användning av smarta kontrakt, kan minska kostnaderna i regelbundna eller upprepade transaktioner i ett affärsförhållande. Kostnaderna för att göra data tillgängliga är antingen specifika för en viss begäran eller delade med andra begäranden. I det senare fallet bör en enda datamottagare inte betala hela kostnaden för att göra data tillgängliga. För det andra kan en rimlig ersättning också omfatta en marginal, utom i fråga om mikroföretag och små och medelstora företag samt forskningsorganisationer utan vinstsyfte. En marginal kan variera beroende på faktorer som rör dessa data som sådana, såsom deras volym, format eller art. Den kan beakta kostnaderna för att samla in data. En marginal kan därför minska om datahållaren har samlat in data för sin egen verksamhet utan betydande investeringar eller öka om investeringarna i datainsamlingen för datahållarens verksamhet är stora. Den kan begränsas eller till och med uteslutas i situationer där datamottagarens användning av data inte påverkar datahållarens egen verksamhet. Det faktum att data samgenereras av en uppkopplad produkt som ägs, hyrs eller leasas av användaren skulle också kunna sänka ersättningsbeloppet jämfört med andra situationer där data genereras av datahållaren, till exempel under tillhandahållandet av en tillhörande tjänst.

- (48) Det är inte nödvändigt att ingripa vid datadelning mellan stora företag eller när datahållaren är ett litet företag eller ett medelstort företag och datamottagaren är ett stort företag. I sådana fall anses företagen själva kunna förhandla fram en ersättning inom gränserna för vad som är rimligt och icke-diskriminerande.
- (49) För att skydda mikroföretag och små och medelstora företag från alltför betungande ekonomiska bördor som affärsmässigt sett skulle göra det alltför svårt för dem att utveckla och driva innovativa affärsmodeller, bör den rimliga ersättning för tillhandahållande av data som de betalar inte överstiga de kostnader som är direkt förknippad med att göra dessa data tillgängliga. Direkt förknippade kostnader är sådana kostnader som kan hänföras till enskilda begäranden, med beaktande av de nödvändiga tekniska gränssnitten eller tillhörande programvara och konnektivitet som ska inrättas permanent av datahållaren. Samma ordning bör gälla för forskningsorganisationer utan vinstsyfte.
- (50) I vederbörligen motiverade fall, exempelvis om det finns ett behov av att skydda konsumenters deltagande och konkurrensen eller främja innovation på vissa marknader, kan unionsrätten eller den nationella lagstiftning som antas i enlighet med unionsrätten omfatta reglerad ersättning för tillgängliggörandet av specifika typer av data.

- (51) Transparens är en viktig princip för att säkerställa att den ersättning som begärs av en datahållare är rimlig eller, om datamottagaren är ett mikroföretag, litet företag eller medelstort företag eller en forskningsorganisation utan vinstsyfte, att ersättningen inte överstiger de kostnader som är direkt förknippade med att göra berörda data tillgängliga för datamottagaren och kan hänföras till den enskilda begäran. För att ge datamottagare möjlighet att bedöma om och kontrollera att ersättningen uppfyller kraven i denna förordning bör datahållaren förse datamottagaren med tillräckligt detaljerad information om hur ersättningen beräknats.
- (52) Att tillgång säkerställs till alternativa sätt att lösa inhemska och gränsöverskridande tvister som uppstår i samband med tillhandahållandet av data bör gagna datahållare och datamottagare och därmed stärka förtroendet för datadelning. Om parterna inte kan enas om rättvisa, rimliga och icke-diskriminerande villkor för tillhandahållandet av data bör tvistlösningsorgan erbjuda parterna en enkel och snabb lågkostnadslösning. I denna förordning fastställs enbart de villkor som tvistlösningsorgan måste uppfylla för att bli certifierade, men det står medlemsstaterna fritt att anta särskilda regler för certifieringsförfarandet, bland annat för certifieringens upphörande eller återkallande. Bestämmelserna om tvistlösning i denna förordning bör inte kräva att medlemsstaterna inrättar tvistlösningsorgan.
- (53) Tvistlösningsförfarandet enligt denna förordning är ett frivilligt förfarande som gör det möjligt för användare, datahållare och datamottagare att komma överens om att hänskjuta sina tvister till tvistlösningsorgan. Parterna bör därför fritt kunna vända sig till ett tvistlösningsorgan efter eget val i eller utanför de medlemsstater där dessa parter är etablerade.

- (54) För att undvika fall där två eller fler tvistlösningsorgan används för samma tvist, i synnerhet i gränsöverskridande situationer, bör ett tvistlösningsorgan kunna avvisa en begäran om att lösa en tvist som redan har hänskjutits till ett annat tvistlösningsorgan eller en domstol i en medlemsstat.
- (55) För att säkerställa en enhetlig tillämpning av denna förordning bör tvistlösningsorganen beakta de icke-bindande standardavtalsvillkor som ska utarbetas och rekommenderas av kommissionen samt unionsrätt eller nationell rätt som anger skyldigheter vad gäller datadelning eller riktlinjer som utfärdas av sektorsmyndigheter för tillämpningen av sådan rätt.
- (56) Parter i tvistlösningsförfaranden bör inte hindras från att utöva sin grundläggande rätt till ett effektivt rättsmedel och en opartisk domstol. Därför bör beslutet att hänskjuta en tvist till ett tvistlösningsorgan inte innebära att dessa parter berövas sin rätt att få sin sak prövad i en domstol i en medlemsstat. Tvistlösningsorganen bör offentliggöra årliga verksamhetsrapporter.

- (57) Datahållare kan vidta lämpliga tekniska skyddsåtgärder för att förhindra olaglig utlämning av eller olaglig åtkomst till data. Dessa åtgärder får emellertid varken diskriminera mellan datamottagare eller hindra användarnas eller datamottagarnas åtkomst till eller användning av data. Om en datamottagare använder otillbörliga metoder, såsom vilseledande av datahållaren genom att tillhandahålla falsk information med uppsåt att använda data för olagliga ändamål, inbegripet utveckling av en konkurrerande uppkopplad produkt på grundval av dessa data, kan datahållaren och, i tillämpliga fall och om det inte rör sig om samma person, innehavaren av en företagshemlighet eller dataanvändaren begära att den tredje parten eller datamottagaren utan oskäligt dröjsmål ska vidta korrigerande eller avhjälpande åtgärder. Alla sådana begäranden, särskilt begäranden om att avsluta produktion, erbjudande eller utsläppande på marknaden av varor, härledda data eller tjänster samt begäranden om att avsluta import, export eller lagring av varor som innebär intrång eller om att förstöra dem, bör bedömas mot bakgrund av deras proportionalitet i förhållande till intressena hos datahållaren, innehavaren av en företagshemlighet eller användaren.
- (58) Om en part har en starkare förhandlingsposition finns det en risk för att den kan utnyttja denna till nackdel för den andra avtalsslutande parten vid förhandlingarna om åtkomst till data så att åtkomsten till dessa data blir mindre affärsmässigt lönsam eller till och med ekonomiskt oöverkomlig. Sådana avtalsmässiga obalanser skadar alla företag som saknar en meningsfull förmåga att förhandla om villkoren för åtkomst till data och som kanske inte har något annat val än att godta de avtalsvillkor som de erbjuds. Därför bör oskäligen avtalsvillkor för åtkomst till och användning av data eller avtalsrättsligt ansvar och påföljder vid överträdelse eller uppsägning av datarelaterade skyldigheter inte vara bindande för företag när dessa villkor åläggs dessa företag ensidigt.

- (59) Regler om avtalsvillkor bör ta hänsyn till principen om avtalsfrihet som ett grundläggande begrepp i förbindelserna mellan företag. Därför bör inte alla avtalsvillkor omfattas av en skälighetsprövning utan endast de villkor som ensidigt åläggs. Detta omfattar situationer där en part tillhandahåller ett visst avtalsvillkor och det andra företaget inte kan påverka innehållet i detta villkor trots ett förhandlingsförsök. Ett avtalsvillkor som helt enkelt föreskrivs av en part och godtas av det andra företaget eller ett villkor som förhandlats fram och sedan i ändrad lydelse godkänns av avtalsslutande parterna bör inte anses som ensidigt ålagt.
- (60) Dessutom bör reglerna om oskäligen avtalsvillkor tillämpas endast på de delar av ett avtal som rör tillgängliggörandet av data, alltså avtalsvillkor som rör åtkomst till och användning av data samt avtalsrättsligt ansvar och påföljder vid överträdelse eller uppsägning av datarelaterade skyldigheter. Andra delar av samma avtal, som inte rör tillgängliggörandet av data, bör inte vara föremål för skälighetsprövningen enligt denna förordning.

- (61) Kriterier för identifiering av oskäligen avtalsvillkor bör endast tillämpas på orimliga avtalsvillkor, i de fall då en starkare förhandlingsposition har missbrukats. De allra flesta avtalsvillkor som affärsmässigt gynnar en part mer än en annan, inbegripet sådana som är normala i avtal mellan företag, är ett normalt uttryck för principen om avtalsfrihet och fortsätter att gälla. Att i hög grad avvika från god affärssed omfattar i denna förordning bland annat att objektivt försämra möjligheten för den part som ensidigt har ålagts villkoret att skydda sitt berättigade kommersiella intresse av de data som berörs.
- (62) För att säkerställa rättssäkerheten fastställs i denna förordning en förteckning över villkor som alltid anses vara oskäligen och en förteckning över villkor som antas vara oskäligen. I det senare fallet bör det företag som inför avtalsvillkoret kunna motbevisa presumtionen om oskälighet genom att visa att det avtalsvillkor som anges i förteckningen i denna förordning inte är oskäligt i det konkreta fallet. Om ett avtalsvillkor inte finns med i förteckningen över villkor som alltid anses vara oskäligen eller som antas vara oskäligen bör den allmänna oskälighetsbestämmelsen gälla. I detta hänseende bör de villkor som förtecknas som oskäligen avtalsvillkor i denna förordning fungera som måttstock för tolkningen av den allmänna oskälighetsbestämmelsen. Slutligen kan också icke-bindande standardavtalsvillkor för datadelningsavtal mellan företag som utarbetas och rekommenderas av kommissionen vara till hjälp för affärspartner som förhandlar fram avtal. Om ett avtalsvillkor förklaras vara oskäligt bör det berörda avtalet fortsätta att gälla utan detta villkor, såvida inte det oskäligen avtalsvillkoret inte kan avskiljas från övriga avtalsvillkor.

- (63) Vid situationer då det finns exceptionella behov kan det vara nödvändigt för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan att vid fullgörandet av sina lagstadgade skyldigheter av allmänt intresse använda befintliga data, i förekommande fall inbegripet åtföljande metadata, för att hantera ett allmänt nödläge eller annan exceptionell situation. Exceptionella behov är omständigheter som är oförutsebara och tidsbegränsade, till skillnad från andra omständigheter som kan vara planerade, schemalagda, periodiska eller ofta förekommande. Begreppet datahållare omfattar i allmänhet inte offentliga organ, men det kan omfatta offentliga företag. Organisationer som bedriver forskning och organisationer som finansierar forskning kan också organiseras som offentliga organ eller offentlighetsrättsliga organ. För att minska bördan för företag bör mikroföretag och små företag endast omfattas av skyldigheten att förse offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan med data i situationer med exceptionella behov om sådana data krävs för att hantera ett allmänt nödläge och det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte i tid, på ett ändamålsenligt sätt och på likvärdiga villkor kan erhålla sådana data på alternativa sätt.

- (64) Vid allmänna nödlägen, såsom hot mot folkhälsan, nödsituationer till följd av naturkatastrofer, inbegripet sådana som förvärras av klimatförändringar och miljöförstöring, samt vid större katastrofer orsakade av människor, såsom större cybersäkerhetsincidenter, bör allmänintresset av dataanvändningen väga tyngre än datahållarnas intresse av att fritt förfoga över de data de innehar. I sådana fall bör datahållare åläggas att göra dessa data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan på deras begäran. Förekomsten av ett allmänt nödläge bör fastställas eller förklaras i enlighet med unionsrätten eller nationell rätt och på grundval av relevanta förfaranden, inbegripet berörda internationella organisationers förfaranden. I sådana fall bör det offentliga organet visa att de data som omfattas av begäran annars inte skulle kunna erhållas i tid, på ett ändamålsenligt sätt och på likvärdiga villkor, till exempel genom ett annat företags frivilliga tillhandahållande av data eller genom sökning i en offentlig databas.

- (65) Ett exceptionellt behov kan också bero på andra situationer än nödlägen. I sådana fall bör ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ha rätt att begära endast icke-personuppgifter. Det offentliga organet bör visa att dessa data är nödvändiga för att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställningen av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge. En sådan begäran kan dessutom göras endast när det offentliga organet, kommissionen, Europeiska centralbanken eller ett unionsorgan har identifierat specifika data som annars inte skulle kunna erhållas i tid, på ett ändamålsenligt sätt eller på likvärdiga villkor och har uttömt alla andra till buds stående medel för att erhålla sådana data, till exempel att erhålla data genom frivilliga avtal, inbegripet att köpa in icke-personuppgifter på marknaden genom att erbjuda marknadspris, eller att förlita sig på befintliga skyldigheter att göra data tillgängliga eller att anta nya lagstiftningsåtgärder som skulle kunna säkerställa att data finns tillgängliga i tid. Sådana villkor och principer för begäranden som rör ändamålsbegränsning, proportionalitet, transparens och tidsbegränsning bör också tillämpas. När det gäller begäranden om data som är nödvändiga för framställning av officiell statistik bör det begärande offentliga organet också visa huruvida det enligt nationell rätt har rätt att köpa in icke-personuppgifter på marknaden.

- (66) Denna förordning bör inte tillämpas på eller föregripa frivilliga arrangemang för utbyte av data mellan privata och offentliga enheter, inbegripet mikroföretags och små och medelstora företags tillhandahållande av data, och påverkar inte tillämpningen av unionsrättsakter som föreskriver att offentliga enheter ska begära information från privata enheter. Skyldigheter för datahållare att tillhandahålla data som motiveras av behov av icke-exceptionell art, i synnerhet när datauppsättningen och datahållarna är kända eller dataanvändningen kan ske regelbundet, såsom är fallet med rapporteringsskyldigheter och skyldigheter kopplade till den inre marknaden, bör inte påverkas av denna förordning. Kraven på åtkomst till data för kontroll av efterlevnaden av tillämpliga regler, även då offentliga organ anförtror efterlevnadskontrollen åt andra enheter än offentliga organ, bör inte heller påverkas av denna förordning.
- (67) Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt och nationell rätt om åtkomst till och användning av data för statistiska ändamål, särskilt Europaparlamentets och rådets förordning (EG) nr 223/2009¹ samt nationella rättsakter som rör officiell statistik.
- (68) Offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan bör förlita sig på sina befogenheter enligt unionsrätten eller nationell rätt för utövandet av sina uppgifter när det gäller förhindrande, utredning, upptäckt eller lagföring av brott eller administrativa förseelser eller verkställandet av straffrättsliga och administrativa påföljder samt insamlingen av data för skatte- eller tulländamål. Denna förordning påverkar därmed inte lagstiftningsakter om delning eller användning av data eller åtkomst till data inom dessa områden.

¹ Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

- (69) I enlighet med artikel 6.1 och 6.3 i förordning (EU) 2016/679 är en proportionell, begränsad och förutsebar ram på unionsnivå nödvändig när den rättsliga grunden föreskrivs för datahållares tillhandahållande av data, vid exceptionella behov, till offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan, både för att säkerställa rättslig förutsebarhet och för att minimera de administrativa bördorna för företagen. Därför bör begäranden avseende dataåtkomst från offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan till datahållare vara specifika, transparenta och proportionella i fråga om innehållets omfång och detaljrikedom. Begärans syfte och den avsedda användningen av begärda data bör specificeras och förklaras tydligt, med tillräckligt utrymme för den begärande enheten att utföra sina specifika uppgifter i allmänhetens intresse på ett flexibelt sätt. Begäran bör också respektera legitima intressen hos den datahållare som mottar begäran. Datahållarnas börda bör minimeras genom att begärande enheter åläggs att iaktta engångsprincipen, som förhindrar att samma data begärs mer än en gång av mer än ett offentligt organ, kommissionen, Europeiska centralbanken eller unionsorgan. För att säkerställa transparens bör begäranden om data som görs av kommissionen, Europeiska centralbanken eller unionsorgan offentliggöras utan oskäligt dröjsmål av den enhet som begär dessa data. Europeiska centralbanken och unionsorgan bör underrätta kommissionen om sina begäranden. Om begäran om data har gjorts av ett offentligt organ bör det organet även underrätta datasamordnaren i den medlemsstat där det offentliga organet är etablerat. Det bör säkerställas att alla begäranden finns tillgängliga online. Efter mottagandet av en underrättelse om en begäran om data kan den behöriga myndigheten besluta att bedöma om begäran är lagenlig och utöva sina uppgifter i samband med verkställandet och tillämpningen av den här förordningen. Datasamordnaren bör säkerställa att alla begäranden som gjorts av offentliga organ är tillgängliga online.

- (70) Syftet med skyldigheten att tillhandahålla data är att säkerställa att offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan har den kunskap som krävs för att hantera, förhindra eller bidra till återhämtningen från allmänna nödlägen eller att bidra till fullgörandet av de specifika uppgifter som uttryckligen föreskrivs i lagstiftning. De data som erhålls av dessa enheter kan vara affärsmässigt känsliga. Därför bör varken Europaparlamentets och rådets förordning (EU) 2022/868 eller Europaparlamentets och rådets direktiv (EU) 2019/1024¹ tillämpas på data som tillhandahålls enligt den här förordningen och bör inte anses som öppna data som är tillgängliga för vidareutnyttjande av tredje parter. Detta bör dock inte påverka tillämpligheten för direktiv (EU) 2019/1024 på vidareutnyttjandet av officiell statistik där data som erhållits enligt den här förordningen har använts för framtagandet, förutsatt att vidareutnyttjandet inte inkluderar de data som finns i underlaget. Förutsatt att villkoren i den här förordningen uppfylls bör möjligheten till utbyte av data för forskningsändamål eller för utveckling, framställning och spridning av officiell statistik inte påverkas. Offentliga organ bör också ha rätt att utbyta data som erhållits enligt den här förordningen med andra offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan för att hantera de exceptionella behov som begäran om data avser.

¹ Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (EUT L 172, 26.6.2019, s. 56).

- (71) Datahållare bör ha möjlighet att antingen avslå en begäran som gjorts av ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan eller begära en ändring av utan onödigt dröjsmål och under alla omständigheter senast inom fem eller 30 arbetsdagar, beroende på vilken typ av exceptionellt behov som åberopas i begäran. I förekommande fall bör datahållaren ha denna möjlighet om den inte har kontroll över begärda data, det vill säga om den inte har omedelbar tillgång till datan och inte kan avgöra dess tillgänglighet. En giltig begäran att inte göra data tillgängliga bör föreligga om det kan visas att begäran liknar en tidigare begäran för samma ändamål som gjorts av ett annat offentligt organ eller, kommissionen, Europeiska centralbanken eller ett unionsorgan och datahållaren har underrättats om radering av uppgifter enligt denna förordning. En datahållare som avvisar begäran eller begär en ändring av den bör meddela den motivering som ligger till grund för detta till det offentliga organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som begär data. I de fall då rätten av sitt eget slag avseende databaser enligt Europaparlamentets och rådets direktiv 96/9/EG¹ gäller för de datamängder som begärts, bör datahållare utöva sina rättigheter på ett sådant sätt att det inte hindrar ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan från att erhålla dessa data eller från att dela dessa data, i enlighet med denna förordning.

¹ Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser (EGT L 77, 27.3.1996, s. 20).

- (72) I händelse av ett exceptionellt behov i samband med hantering av ett allmänt nödläge bör offentliga organ om möjligt använda icke-personuppgifter. Vid begäranden som grundar sig på ett exceptionellt behov som inte rör ett allmänt nödläge får personuppgifter inte begäras. När personuppgifter omfattas av begäran bör datahållaren anonymisera datan. När det är strikt nödvändigt att inkludera personuppgifter i de data som görs tillgängliga för ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan, eller när anonymisering visar sig vara omöjlig, bör den enhet som begär uppgifterna visa att det är strikt nödvändigt och att behandlingen sker för specifika och begränsade ändamål. De tillämpliga reglerna om skydd av personuppgifter bör följas. Vid tillhandahållandet och den senare användningen av dessa data bör det finnas skyddsåtgärder avseende rättigheterna och intressena för de individer som berörs av uppgifterna.
- (73) Data som görs tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan baserat på ett exceptionellt behov bör endast användas för de ändamål som de begärdes för, om inte den datahållare som gjorde uppgifterna tillgängliga uttryckligen godkänt att de används för andra ändamål. Dessa data bör raderas när de inte längre behövs för de ändamål som anges i begäran, om inte annat överenskommits, och datahållaren bör underrättas om detta. Denna förordning bygger på de befintliga bestämmelserna om tillgång i unionen och medlemsstaterna och ändrar inte nationella rätt om allmänhetens tillgång till handlingar inom ramen för insynsskyldigheten. Data bör raderas när de inte längre behövs för att uppfylla sådana insynsskyldigheter.

- (74) Vid vidareutnyttjande av data som tillhandahållits av datahållare bör offentliga organ, kommissionen eller Europeiska centralbanken eller unionsorgan iaktta både befintlig tillämplig unionsrätt eller nationell rätt och avtalsskyldigheter som datahållaren omfattas av. De bör avstå från att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens uppkopplade produkt eller tillhörande tjänst samt från att dela data med en tredje part för dessa ändamål. De bör även ge datahållarna offentligt erkännande på deras begäran och bör ansvara för att mottagna datas säkerhet upprätthålls. När röjandet av datahållarens företagshemligheter för offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan är strikt nödvändig för uppfyllandet av det ändamål för vilka data har begärts, bör konfidentialiteten för sådant röjande garanteras innan uppgifterna röjs.

- (75) När skydd av en betydande kollektiv nytthet berörs, som vid hantering av ett allmänt nödläge, bör det offentliga organ, kommissionen, Europeiska centralbanken eller det unionsorgan som berörs inte förväntas ersätta företagen för de data som erhålls. Allmänna nödlägen är ovanliga händelser och det är inte alla sådana nödlägen som kräver användning av data som innehas av företag. Samtidigt kan skyldigheten att tillhandahålla data utgöra en betydande börda för mikroföretag och små företag. De bör därför ha rätt att kräva ersättning även i samband med hantering av ett allmänt nödläge. Datahållarnas affärsverksamhet kommer därför sannolikt inte påverkas negativt av att offentliga organ, kommissionen eller Europeiska centralbanken eller unionsorgan använder sig av denna förordning. Fall som rör andra exceptionella behov än hantering av allmänna nödlägen är förmodligen vanligare, och därför bör datahållare i sådana fall ha rätt till en rimlig ersättning som inte bör överstiga de tekniska och organisatoriska kostnaderna för att tillgodose begäran och den rimliga marginal som krävs för att göra data tillgängliga för det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet. Ersättningen bör inte anses utgöra betalning för själva uppgifterna eller anses obligatorisk. Datahållare bör inte kunna kräva ersättning om nationell rätt hindrar nationella statistikbyråer eller andra nationella myndigheter med ansvar för statistikframställning från att kompensera datahållare för att de gör data tillgängliga. Det offentliga organet, kommissionen, Europeiska centralbanken eller det berörda unionsorganet bör kunna ifrågasätta den ersättningsnivå som datahållaren begär genom att hänskjuta ärendet till den behöriga myndigheten i den medlemsstat där datahållaren är etablerad.

- (76) Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan bör ha rätt att dela de data som erhållits till följd av en begäran med andra enheter eller personer när det är nödvändigt för genomförandet av forskningsverksamhet eller analysverksamhet som de själva inte kan utföra, under förutsättning att sådan verksamhet är förenlig med det ändamål för vilket data begärdes. De bör i god tid informera datahållaren om sådan delning. Sådana data får också under samma omständigheter delas med de nationella statistikbyråerna och Eurostat för utveckling, framställning och spridning av officiell statistik. Denna forskningsverksamhet bör dock vara förenlig med det ändamål som uppgifterna begärdes för och datahållaren bör underrättas om vidare delning av de data som tillhandahållits. De individer som bedriver forskning eller de forskningsorganisationer med vilka dessa data får delas bör agera antingen på icke vinstdrivande grund eller inom ramen för ett uppdrag i det allmännas intresse som erkänns av staten. Organisationer över vilka kommersiella företag har ett avsevärt inflytande, som innebär att de kan utöva kontroll på grund av strukturella situationer, vilket skulle kunna medföra förmånstillträde till forskningsresultat, bör inte anses som forskningsorganisationer vid tillämpningen av denna förordning.

- (77) När ett gränsöverskridande allmänt nödläge eller ett annat exceptionellt behov ska hanteras får begäranden om data riktas till datahållare i andra medlemsstater än den där det begärande offentliga organet är beläget. I ett sådant fall bör det begärande offentliga organet underrätta den behöriga myndigheten i den medlemsstat där datahållaren är etablerad, så att den kan pröva begäran mot de kriterier som fastställs i denna förordning. Detsamma bör gälla ansökningar från kommissionen, Europeiska centralbanken eller ett unionsorgan. Om personuppgifter begärs bör det offentliga organet underrätta den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 i den medlemsstat där det offentliga organet är etablerat. Den berörda behöriga myndigheten bör ha rätt att råda det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet att samarbeta med de offentliga organen i den medlemsstat där datahållaren är etablerad om behovet av att säkerställa en minimal administrativ börda för datahållaren. När den behöriga myndigheten har motiverade invändningar vad gäller begärans förenlighet med den här förordningen bör den avslå begäran från det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet, som bör beakta dessa invändningar innan ytterligare åtgärder vidtas, inbegripet en inlämning på nytt av begäran.

- (78) Möjligheten för kunder av databehandlingstjänster, inbegripet molntjänster och edgetjänster, att byta från en databehandlingstjänst till en annan och samtidigt behålla en miniminivå av tjänstefunktioner utan att tjänsterna drabbas av driftstopp, eller att använda flera leverantörers tjänster samtidigt utan onödiga hinder och kostnader för dataöverföring, är ett centralt villkor för en mer konkurrenspräglad marknad med lägre inträdeshinder för nya leverantörer av databehandlingstjänster och för en säkerställd ytterligare motståndskraft hos användarna av dessa tjänster. Kunder som omfattas av kostnadsfria erbjudanden bör också omfattas av de bestämmelser om byte som fastställs i denna förordning, så att dessa erbjudanden inte leder till en inlåsningsituation för kunderna.
- (79) Europaparlamentets och rådets förordning (EU) 2018/1807¹ uppmuntrar leverantörer av databehandlingstjänster att utveckla och effektivt genomföra självreglerande uppförandekoder som omfattar bästa praxis när det gäller bland annat att underlätta byten av leverantör av databehandlingstjänster och dataportering. Mot bakgrund av att de självregleringsramar som utvecklades till följd av detta har fått begränsad användning, och den allmänna avsaknaden av öppna standarder och gränssnitt, är det nödvändigt att anta ett antal minimiregleringsskyldigheter för leverantörer av databehandlingstjänster för att undanröja förkommersiella, kommersiella, tekniska, avtalsmässiga, ekonomiska och organisatoriska hinder, vilka inte är begränsade till begränsad dataöverföringshastighet vid kundens utträde, som hindrar effektiva byten av databehandlingstjänster.

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).

- (80) Databehandlingstjänster bör omfatta tjänster som möjliggör allmän nätverkstillgång på begäran till en konfigurerbar, skalbar och elastisk gemensam pool av distribuerade dataresurser. Dessa dataresurser innefattar sådana resurser som nät, servrar eller annan virtuell eller fysisk infrastruktur, programvara, inbegripet verktyg för programvaruutveckling, samt lagring, applikationer och tjänster. Databehandlingstjänstens kunds förmåga att ensidigt självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av databehandlingstjänster, kan beskrivas som att den kräver minsta möjliga administration och som att den innehåller minsta möjliga interaktion mellan leverantör och kund. Termen *allmän* används för att beskriva den datorkapacitet som tillhandahålls över nätet och som nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar (däribland webbläsare, mobilenheter och arbetsstationer). Termen *skalbar* avser datorresurser som leverantören av databehandlingstjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk* används för att beskriva datorresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas eller minskas i takt med arbetsbördan. Termen *gemensam pool* används för att beskriva datorresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten, men där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen *distribuerad* används för att beskriva de datorresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning. Termen *mycket distribuerad* används för att beskriva databehandlingstjänster som involverar databehandling som sker närmare den plats där data genereras eller samlas in, exempelvis i en uppkopplad databehandlingsenhet. *Edge computing*, som är en form av sådan mycket distribuerad databehandling, förväntas generera nya affärsmodeller och modeller för leverans av molntjänster, som bör vara öppna och interoperabla från början.

- (81) Det allmänna begreppet *databehandlingstjänster* omfattar ett stort antal tjänster med ett mycket brett spektrum av olika ändamål, funktioner och tekniska upplägg. Såsom det allmänt förstås av leverantörer och användare och i linje med vedertagna standarder, gäller databehandlingstjänster en eller flera av följande tre modeller för leverans av databehandlingstjänster, nämligen infrastruktur som en tjänst (IaaS), plattform som en tjänst (PaaS) och programvara som en tjänst (SaaS). Dessa tjänsteleveransmodeller utgör en specifik, färdigförpackad kombination av IKT-resurser som erbjuds av en leverantör av databehandlingstjänster. Dessa tre grundläggande modeller för leverans av databehandling kompletteras ytterligare med nya varianter, som var och en består av en särskild kombination av IKT-resurser, såsom lagring som en tjänst och databas som en tjänst. Databehandlingstjänster kan kategoriseras på grundval av ytterligare detaljrikedom delas in i en icke uttömmande förteckning över uppsättningar av databehandlingstjänster som har samma primära syfte och huvudsakliga funktioner samt samma typ av databehandlingsmodeller, vilka inte är kopplade till tjänstens operativa egenskaper (samma tjänstetyp). Tjänster som är av samma tjänstetyp kan ha samma modell för databehandlingstjänster, men två databaser kan förefalla ha samma primära syfte, men med beaktande av deras databehandlingsmodell, distributionsmodell och de användningsfall som de riktar sig till skulle sådana databaser kunna ingå i en mer detaljerad underkategori av liknande tjänster. Tjänster av samma tjänstetyp kan ha olika och konkurrerande egenskaper såsom prestanda, säkerhet, motståndskraft och tjänstekvalitet.

- (82) Att undergräva utvinningen av de exporterbara data som tillhör kunden från den ursprungliga leverantören av databehandlingstjänster kan hindra återställandet av tjänstefunktionerna i infrastrukturen hos destinationsleverantören av databehandlingstjänster. För att underlätta kundens utträdesstrategi, undvika onödiga och betungande uppgifter och säkerställa att kunden inte förlorar några av sina data till följd av bytesprocessen bör den ursprungliga leverantören av databehandlingstjänster i förväg informera kunden om omfattningen av de data som kan exporteras när den kunden väl beslutar sig för att byta till en annan tjänst som tillhandahålls av en annan leverantör av databehandlingstjänster eller gå över till lokal IKT-infrastruktur. Exporterbara data bör åtminstone omfatta in- och utdata, inklusive metadata, som direkt eller indirekt genereras eller samgenereras genom kundens användning av databehandlingstjänsten, med undantag för tillgångar eller data som tillhör leverantören av databehandlingstjänster eller en tredje part. Exporterbara data bör inte omfatta sådana tillgångar eller data som tillhör leverantören av databehandlingstjänster eller tredje parter och som omfattas av immateriella rättigheter eller utgör företagshemligheter för den leverantören eller den tredje parten, eller data med anknytning till tjänstens integritet och säkerhet, vars export kommer att utsätta leverantörerna av databehandlingstjänster för cybersäkerhetssårbarheter. Dessa undantag bör inte hindra eller försena bytesprocessen.

- (83) Digitala tillgångar avser element i digitalt format för vilka kunden har nyttjanderätten, inbegripet applikationer och metadata som rör konfigureringsinställningar, säkerhet och förvaltning av åtkomst- och kontrollrättigheter, och andra element såsom uttryck för virtualiseringsteknik, inbegripet virtuella maskiner och behållare. Digitala tillgångar kan överföras om kunden har nyttjanderätt oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från. Dessa andra element är avgörande för en effektiv användning av kundens data och applikationer i miljön hos destinationsleverantören av databehandlingstjänster.
- (84) Denna förordning syftar till att underlätta byten av databehandlingstjänster, på ett sätt som omfattar villkor och åtgärder som är nödvändiga för att en kund ska kunna avsluta ett avtal om en databehandlingstjänst, ingå ett eller flera nya avtal med olika leverantörer av databehandlingstjänster, portera sina exporterbara data och digitala tillgångar, och när så är tillämpligt, dra nytta av funktionell likvärdighet.

- (85) Byte är en kundstyrd process som består av flera steg, inbegripet datautvinning, vilket avser nedladdning av data från ekosystemet hos en ursprunglig leverantör av databehandlingstjänster, anpassning, om data är strukturerade på ett sätt som inte överensstämmer med målplatsens schema, och uppladdning av data till en ny destination. I en specifik situation som beskrivs i denna förordning bör separation av en viss tjänst från avtalet och överföring av den till en annan leverantör också betraktas som byte. Bytesprocessen hanteras ibland för kundens räkning av en tredjepartsenhet. Därför bör kundens alla rättigheter och skyldigheter som fastställs i denna förordning, inbegripet skyldigheten att samarbeta i god tro, anses vara tillämpliga på en sådan tredjepartsenhet under dessa omständigheter. Leverantörer av databehandlingstjänster och kunder har olika ansvarsnivåer, beroende på vilka steg i processen som avses. Exempelvis ansvarar den ursprungliga leverantören av databehandlingstjänster för utvinning av data i ett maskinläsbart format, men det åligger kunden och destinationsleverantören av databehandlingstjänster att ladda upp data till den nya miljön, såvida inte en särskild, professionell övergångstjänst har erhållits. En kund som avser att utöva rättigheter rörande ett byte, vilka föreskrivs i denna förordning, bör informera den ursprungliga leverantören av databehandlingstjänster om beslutet att antingen byta till en annan leverantör av databehandlingstjänster, byta till lokal IKT-infrastruktur eller radera kundens tillgångar och radera dennes exporterbara data.

- (86) Funktionell likvärdighet innebär att man på grundval av kundens exporterbara data och digitala tillgångar återställer en miniminivå av funktionalitet i miljön för en ny databehandlingstjänst av samma tjänstetyp efter ett byte, där destinationstjänsten för databehandling levererar ett väsentligen jämförbart resultat som svar på samma input för delade funktioner som tillhandahålls kunden enligt avtalet. Leverantörer av databehandlingstjänster kan endast förväntas underlätta funktionell likvärdighet för de funktioner som både de ursprungliga tjänsterna och destinationstjänsterna för databehandling erbjuder oberoende av varandra. Denna förordning medför inte en skyldighet att underlätta funktionell likvärdighet för andra leverantörer av databehandlingstjänster än de som erbjuder tjänster enligt IaaS-leveransmodellen.
- (87) Databehandlingstjänster används inom olika sektorer och varierar i fråga om komplexitet och tjänstetyp. Detta är en viktig aspekt när det gäller porteringsprocessen och tidsramarna. En förlängning av övergångsperioden på grund av att det är tekniskt omöjligt att slutföra bytesprocessen inom den givna tidsramen bör dock endast åberopas i vederbörligen motiverade fall. Bevisbördan i detta avseende bör helt och hållet ligga på leverantören av den berörda databehandlingstjänsten. Detta påverkar inte kundens ensamrätt att förlänga övergångsperioden en gång med en tidsperiod som kunden anser lämpligare för sina egna behov. Kunden får åberopa denna rätt till förlängning före eller under övergångsperioden, med beaktande av att avtalet fortfarande är tillämpligt under övergångsperioden.

- (88) Bytesavgifter är sådana avgifter som leverantörer av databehandlingstjänster debiterar sina kunder för bytesprocessen. Syftet med dessa avgifter är vanligen att föra vidare de kostnader som den ursprungliga leverantören av databehandlingstjänster kan komma att ådra sig på grund av bytesprocessen till den kund som vill byta leverantör. Vanliga exempel på bytesavgifter är kostnader som rör överföringen av data från en leverantör till en annan leverantör av databehandlingstjänster eller till en lokal IKT-infrastruktur (*uttagsavgifter för data*) eller kostnader för särskilda stödåtgärder under bytesprocessen. Onödigt höga uttagsavgifter för data och andra omotiverade avgifter utan anknytning till faktiska byteskostnader hindrar kunderna från att byta, begränsar det fria flödet av data, riskerar att begränsa konkurrensen samt skapar inlåsnings effekter för kunderna genom att de minskar incitamenten att välja en annan eller ytterligare en tjänsteleverantör. Bytesavgifter bör därför avskaffas tre år från dagen för denna förordnings ikraftträdande. Leverantörer av databehandlingstjänster bör kunna ta ut nedsatta bytesavgifter till och med den dagen.

- (89) En ursprunglig leverantör av databehandlingstjänster bör kunna utkontraktera vissa uppgifter och ersätta tredjepartsenheter för att fullgöra de skyldigheter som föreskrivs i denna förordning. En kund bör inte bära de kostnader som uppstår till följd av utkontraktering av tjänster som ingått av den ursprungliga leverantören av databehandlingstjänster under bytesprocessen, och sådana kostnader bör betraktas som omotiverade såvida de inte täcker arbete som utförs av leverantören av databehandlingstjänster på kundens begäran för ytterligare stöd i bytesprocessen som går utöver leverantörens bytesskyldigheter enligt vad som uttryckligen föreskrivs i denna förordning. Ingenting i denna förordning hindrar en kund från att ersätta tredjepartsenheter för stöd i migreringsprocessen eller parter från att komma överens om avtal om databehandlingstjänster med en fast löptid, inbegripet proportionella straffavgifter för förtida uppsägning för att täcka förtida uppsägning av dessa avtal, i enlighet med unionsrätten eller nationell rätt. För att främja konkurrens bör det gradvisa avskaffandet av avgifter som hör ihop med bytet mellan olika leverantörer av databehandlingstjänster specifikt omfatta avskaffandet av de uttagsavgifter för data som en leverantör av databehandlingstjänst debiterar en kund. Standardavgifter för tillhandahållandet av själva databehandlingstjänsterna är inte bytesavgifter. Dessa standardavgifter är inte föremål för avskaffande och gäller fram till dess att avtalet om tillhandahållande av relevant tjänst upphör att gälla. Denna förordning gör det möjligt för kunden att begära tillhandahållande av ytterligare tjänster som går utöver leverantörens bytesskyldigheter enligt denna förordning. Dessa ytterligare tjänster kan utföras och debiteras av leverantören när de utförs på kundens begäran och kunden samtycker till priset för dessa tjänster i förväg.

- (90) Det krävs en ambitiös och innovationsfrämjande regleringsstrategi för interoperabilitet för att råda bot på inlåsning till en säljare, som undergräver både konkurrensen och utvecklingen av nya tjänster. Interoperabilitet mellan databehandlingstjänster involverar flera olika gränssnitt och lager av infrastruktur och programvara och kan sällan reduceras till ett binärt test av om interoperabilitet är möjlig eller ej. I stället blir uppbyggnaden av sådan interoperabilitet föremål för en kostnads-nyttanalys som är nödvändig för att fastställa om det är värt att eftersträva de resultat som rimligen kan förutses. ISO/IEC 19941:2017 utgör en viktig internationell standard som utgör en referens för uppnåendet av målen i denna förordning, eftersom den omfattar tekniska överväganden som klargör komplexiteten i en sådan process.
- (91) I de fall då leverantörer av databehandlingstjänster i sin tur är kunder till databehandlingstjänster som tillhandahålls av en tredjepartsleverantör, kommer de själva att omfattas av effektivare byten, samtidigt som de fortfarande är bundna av denna förordnings skyldigheter när det gäller det egna tjänsteutbudet.

- (92) Leverantörer av databehandlingstjänster bör åläggas att erbjuda allt bistånd och stöd som de har kapacitet till och i proportion till deras respektive skyldigheter, som krävs för att göra bytesprocessen till en tjänst hos en annan leverantör av databehandlingstjänster framgångsrik, effektiv och säker. Denna förordning kräver inte att leverantörer av databehandlingstjänster utvecklar nya kategorier av databehandlingstjänster, inbegripet inom eller på grundval av IKT-infrastrukturen hos andra leverantörer av databehandlingstjänster för att garantera funktionell likvärdighet i en annan miljö än de egna systemen. En ursprunglig leverantör av databehandlingstjänster har inte tillgång till eller inblick i miljön hos destinationsleverantören av databehandlingstjänster. Funktionell likvärdighet bör inte tolkas som en skyldighet för den ursprungliga leverantören av databehandlingstjänster att återuppbygga tjänsten i fråga inom infrastrukturen hos destinationsleverantören av databehandlingstjänster. Den ursprungliga leverantören av databehandlingstjänster bör i stället vidta alla rimliga åtgärder inom ramen för sina befogenheter i syfte att underlätta processen med att uppnå funktionell likvärdighet genom tillhandahållande av kapacitet, adekvat information, dokumentation, tekniskt stöd och, vid behov, de nödvändiga verktygen.

- (93) Leverantörer av databehandlingstjänster bör också vara skyldiga att undanröja befintliga hinder och inte införa nya, även för kunder som vill byta till en lokal IKT-infrastruktur. Hindren kan bland annat vara förkommersiella, kommersiella, tekniska, avtalsmässiga eller organisatoriska. Leverantörer av databehandlingstjänster bör också vara skyldig att undanröja hinder för separation av en viss enskild tjänst från andra databehandlingstjänster som tillhandahålls enligt ett avtal och göra relevant tjänst tillgänglig för byte, om det inte finns några större och påvisade tekniska hinder för sådan separation.
- (94) Under hela bytesprocessen bör en hög säkerhetsnivå upprätthållas. Detta innebär att den ursprungliga leverantören av databehandlingstjänster bör utöka den säkerhetsnivå som den åtagit sig för tjänsten till att omfatta alla tekniska villkor som leverantören ansvarar för under bytesprocessen, såsom nätanslutningar eller fysiska enheter. Befintliga rättigheter avseende uppsägning av avtal, inbegripet de som infördes genom förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU) 2019/770¹, bör inte påverkas. Den här förordningen bör inte tolkas som att den hindrar en leverantör av databehandlingstjänster från att tillhandahålla sina kunder nya och förbättrade tjänster, egenskaper och funktioner eller från att konkurrera med andra leverantörer av databehandlingstjänster på denna grund.

¹ Europaparlamentets och rådets direktiv (EU) 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster (EUT L 136, 22.5.2019, s. 1).

- (95) Den information som leverantörer av databehandlingstjänster ska tillhandahålla kunden kan stödja kundens utträdesstrategi. Informationen bör omfatta förfaranden för att påbörja ett byte från databehandlingstjänsten, de maskinläsbara dataformat till vilka användarens data kan exporteras, verktygen för export av data, inklusive ett öppet gränssnitt och säkerställa kompatibilitet med harmoniserade standarder eller gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer, information om kända tekniska restriktioner och begränsningar som kan påverka bytesprocessen och den beräknade tid som krävs för att slutföra bytesprocessen.
- (96) För att främja interoperabilitet och byten av databehandlingstjänster bör användare och leverantörer av databehandlingstjänster överväga att använda genomförandeverktyg och verktyg för kontroll av efterlevnaden, i synnerhet de som kommissionen offentliggör i form av en *EU Cloud Rulebook* och en vägledning om offentlig upphandling av databehandlingstjänster. Standardavtalsklausuler är särskilt fruktbara eftersom de ökar förtroendet för databehandlingstjänster, för att upprätta ett mer balanserat förhållande mellan användare och leverantörer av databehandlingstjänster och för att förbättra rättssäkerheten vad gäller de villkor som är tillämpliga på byten till andra databehandlingstjänster. I det sammanhanget bör användare och leverantörer av databehandlingstjänster överväga att använda sådana standardavtalsklausuler eller andra självreglerande verktyg för regelefterlevnad förutsatt att de till fullo uppfyller kraven i denna förordning som utarbetats av relevanta organ eller expertgrupper som inrättats inom ramen för unionsrätten.

- (97) För att underlätta byte av databehandlingstjänster bör alla berörda parter, inbegripet såväl ursprungliga leverantörer som destinationsleverantörer av databehandlingstjänster, samarbeta i god tro för att möjliggöra en effektiv bytesprocess och säker och snabb överföring av nödvändiga data i ett allmänt använt, maskinläsbart format och genom öppna gränssnitt samtidigt som störningar i tjänsten undviks och dess kontinuitet bibehålls.
- (98) Databehandlingstjänster som rör tjänster där de flesta av huvudfunktionerna har skräddarsytts för att tillgodose en enskild kunds specifika behov eller där alla komponenter har utvecklats för en enskild kunds ändamål bör undantas från vissa av de skyldigheter som gäller för byte av databehandlingstjänster. Detta bör inte omfatta tjänster som leverantören av databehandlingstjänster erbjuder i stor kommersiell skala via sin tjänstekatalog. Det hör till skyldigheterna för leverantören av databehandlingstjänster att innan ett avtal ingås vederbörligen informera potentiella kunder för sådana tjänster om vilka skyldigheter enligt denna förordning som inte är tillämpliga på de berörda tjänsterna. Ingenting hindrar leverantören av databehandlingstjänster från att så småningom börja erbjuda sådana tjänster i stor skala, i vilket fall den leverantören måste uppfylla alla de skyldigheter för byte som anges i denna förordning.

- (99) I linje med minimikravet på att tillåta byte mellan leverantörer av databehandlingstjänster syftar denna förordning också till att förbättra interoperabiliteten för parallell användning av flera databehandlingstjänster med kompletterande funktioner. Detta gäller situationer där kunder inte säger upp ett avtal för att byta till en annan leverantör av databehandlingstjänster, utan där flera tjänster från olika leverantörer används parallellt, på ett interoperabelt sätt, för att dra nytta av de kompletterande funktionerna hos de olika tjänsterna i kundens systemstruktur. Det erkänns dock att uttaget av data från en leverantör av databehandlingstjänster till en annan för att underlätta parallell användning av tjänster kan vara en pågående verksamhet, till skillnad från det engångsuttag som behövs som en del av bytesprocessen. Leverantörer av databehandlingstjänster bör därför kunna fortsätta att ta ut avgifter för datauttag, som inte överstiger de uppkomna kostnaderna, för parallell användning efter tre år från dagen för denna förordnings ikraftträdande. Detta är viktigt bland annat för en lyckad spridning av multimolnstrategier, som ger kunderna möjlighet att genomföra framtidssäkrade IKT-strategier och som kan minska beroendet av individuella leverantörer av databehandlingstjänster. Att främja en multimolnstrategi för kunder som använder sig av databehandlingstjänster kan också bidra till att öka deras digitala operativa motståndskraft, vilket erkänts med avseende på institutioner som tillhandahåller finansiella tjänster i Europaparlamentets och rådets förordning (EU) 2022/2554¹.

¹ Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

- (100) Öppna interoperabilitetsspecifikationer och standarder som utvecklats i enlighet med bilaga II till Europaparlamentets och rådets förordning (EU) nr 1025/2012¹ på området interoperabilitet och portabilitet förväntas möjliggöra den molnmiljö med flera säljare som är en förutsättning för öppen innovation i den europeiska dataekonomin. Eftersom marknadsgenomslaget för identifierade standarder inom ramen för det initiativ för samordning av molnbaserad standardisering som avslutades 2016 har varit begränsat, är det också nödvändigt att kommissionen förlitar sig på att parterna på marknaden utvecklar relevanta öppna interoperabilitetsspecifikationer för att hålla jämna steg med den snabba tekniska utvecklingen inom denna industri. Sådana öppna interoperabilitetsspecifikationer kan sedan antas av kommissionen i form av gemensamma specifikationer. I de fall där marknadsdrivna processer inte har visat sig fungera för fastställandet av gemensamma specifikationer eller standarder för att främja molninteroperabilitet i praktiken på nivåerna PaaS och SaaS bör kommissionen dessutom, på grundval av den här förordningen och i enlighet med förordning (EU) nr 1025/2012, kunna begära att europeiska standardiseringsorgan utarbetar sådana standarder för specifika tjänstetyper som fortfarande saknar sådana. Kommissionen kommer också att uppmana marknadsaktörerna att utveckla relevanta öppna interoperabilitetsspecifikationer.

¹ Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

Efter samråd med berörda aktörer bör kommissionen, genom genomförandeakter, kunna föreskriva användningen av harmoniserade standarder för interoperabilitet eller gemensamma specifikationer för specifika typer av tjänster genom en referens i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster. Leverantörer av databehandlingstjänster bör säkerställa kompatibilitet med dessa harmoniserade standarder och gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer, vilket inte bör inverka negativt på säkerheten eller integriteten för data. Det kommer endast att refereras till harmoniserade standarder för interoperabla databehandlingstjänster och gemensamma specifikationer baserade på öppna interoperabilitetsspecifikationer om de uppfyller de kriterier som anges i den här förordningen, som har samma innebörd som kraven i bilaga II till förordning (EU) nr 1025/2012 och de interoperabilitetsaspekter som definieras i den internationella standarden ISO/IEC 19941:2017. Dessutom bör standardiseringen ta hänsyn till mikroföretags och små och medelstora företags behov.

- (101) Tredjeländer kan anta lagar och andra författningar som syftar till att direkt överföra eller ge statlig åtkomst till icke-personuppgifter som finns utanför det egna landets gränser, inbegripet inom unionen. Rättsliga avgöranden eller beslut av rättsliga eller administrativa myndigheter, däribland brottsbekämpande myndigheter, i tredjeländer som innehåller krav på sådan överföring eller åtkomst till icke-personuppgifter ska vara verkställbara, om de grundar sig på ett gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. I andra fall kan det uppstå situationer där en begäran om överföring av eller åtkomst till icke-personuppgifter inom ramen för tredje lands lagstiftning står i strid med en skyldighet att skydda sådana data enligt unionsrätten eller enligt den berörda medlemsstats nationella rätt, i synnerhet när det gäller skyddet av individers grundläggande rättigheter, såsom rätten till säkerhet och rätten till ett effektivt rättsmedel, eller en medlemsstats grundläggande intressen med avseende på nationell säkerhet eller försvar samt skyddet av kommersiellt känsliga uppgifter och skyddet av immateriella rättigheter, inbegripet dess avtalsskyldigheter i fråga om konfidentialitet i enlighet med sådan lagstiftning. I avsaknad av internationella avtal som reglerar sådana frågor bör överföring av eller åtkomst till icke-personuppgifter endast tillåtas om det har kontrollerats att tredjelandets rättssystem omfattar krav på att beslutets skäl och proportionalitet anges, att domstolsavgörandet eller beslutet är specifikt till sin karaktär och att den motiverade invändningen från mottagaren är föremål för prövning av en behörig tredjelandsdomstol som har befogenhet att vederbörligen beakta de relevanta rättsliga intressena för leverantören av sådana data. När det är möjligt enligt villkoren för tredjelandsmyndighetens begäran om dataåtkomst bör leverantören av databehandlingstjänster kunna informera den kund vars data omfattas av begäran innan åtkomst beviljas för sådana data för att kontrollera om denna åtkomst potentiellt kan strida mot unionsrätten eller nationell rätt, såsom reglerna om skydd av kommersiellt känsliga uppgifter, inbegripet skyddet av företagshemligheter och immateriella rättigheter samt avtalsåtaganden avseende konfidentialitet.

- (102) För att främja förtroendet för data är det viktigt att det i möjligaste mån genomförs skyddsåtgärder för unionens medborgare, organ på den offentliga sektorn och företagen för att säkra deras kontroll över sina data. Dessutom bör unionsrätten och unionens värden och standarder med avseende på bland annat säkerhet, dataskydd och integritet samt konsumentskydd upprätthållas. För att förhindra olaglig statlig åtkomst till icke-personuppgifter av myndigheter i tredjeländer bör leverantörer av databehandlingstjänster som omfattas av denna förordning, däribland molntjänster och edgetjänster, vidta alla rimliga åtgärder för att förhindra åtkomst till system där icke-personuppgifter lagras, inbegripet, när så är lämpligt, genom kryptering av data, frekventa revisioner, verifierad anslutning till relevanta certifieringssystem för säkerhetsförsäkras och ändring av företagspolicyer.

- (103) Standardisering och semantisk interoperabilitet bör ha en nyckelroll för tekniska lösningar som säkerställer interoperabilitet inom och mellan gemensamma europeiska dataområden, som är ändamåls- eller sektorsspecifika eller sektorsöverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bland annat utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällesinitiativ. Genom denna förordning fastställs vissa väsentliga krav för interoperabilitet. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare, som är enheter som underlättar eller deltar i datadelning inom gemensamma europeiska dataområden, inbegripet datahållare, bör uppfylla dessa krav när det gäller element som står under deras kontroll. Efterlevnaden av de reglerna kan säkerställas genom uppfyllelse av de väsentliga krav som fastställs i denna förordning eller förmodas genom efterlevnad av harmoniserade standarder eller gemensamma specifikationer via presumtion om överensstämmelse. För att främja överensstämmelse med interoperabilitetskraven är det nödvändigt att föreskriva presumtion om överensstämmelse för interoperabilitetslösningar som motsvarar harmoniserade standarder – eller delar av sådana – i enlighet med förordning (EU) nr 1025/2012, vilken utgör det grundläggande regelverket för utarbetande av standarder som möjliggör sådana presumtioner. Kommissionen bör bedöma hindren för interoperabilitet och prioritera standardiseringsbehov, på grundval av vilka den kan begära att en eller flera europeiska standardiseringsorganisationer, enligt förordning (EU) nr 1025/2012, ska utarbeta utkast till harmoniserade standarder som tillgodoser de väsentliga krav som fastställs i den här förordningen.

Om en sådan begäran inte leder till harmoniserade standarder eller om sådana harmoniserade standarder är otillräckliga för att säkerställa överensstämmelse med de väsentliga kraven i den här förordningen, bör kommissionen kunna anta gemensamma specifikationer för dessa områden, förutsatt att den därvid vederbörligen respekterar standardiseringsorganisationernas roll och funktioner. Gemensamma specifikationer bör endast antas som en exceptionell nödlösning för att underlätta efterlevnad av de väsentliga kraven i den här förordningen, när standardiseringsprocessen är blockerad eller när fastställandet av lämpliga harmoniserade standarder försenas. Om en sådan försening beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen beakta detta innan den överväger att fastställa gemensamma specifikationer. Gemensamma specifikationer bör utarbetas på ett öppet och inkluderande sätt och i förekommande fall beakta råd från Europeiska datainnovationsstyrelsen, som inrättats genom förordning (EU) 2022/868. Gemensamma specifikationer inom olika sektorer skulle också kunna antas, i enlighet med unionsrätten eller nationell rätt, på grund av specifika behov inom dessa sektorer. Kommissionen bör också få möjlighet att föreskriva utarbetandet av harmoniserade standarder för interoperabla databehandlingstjänster.

- (104) För att främja interoperabiliteten för verktyg för automatiserat genomförande av datadelningsavtal är det nödvändigt att fastställa väsentliga krav för smarta kontrakt som yrkespersoner skapar för andra eller integrerar i applikationer som stöder genomförandet av avtal om datadelning. För att främja sådana smarta kontrakts överensstämmelse med dessa väsentliga krav är det nödvändigt att föreskriva presumtion om överensstämmelse för smarta kontrakt som uppfyller harmoniserade standarder – eller delar av sådana – i enlighet med förordning (EU) nr 1025/2012. Begreppet *smart kontrakt* i den här förordningen är teknikneutralt. Smarta kontrakt kan till exempel kopplas till en elektronisk liggare. De väsentliga kraven bör endast gälla säljare av smarta kontrakt, men inte när de internt utvecklar smarta kontrakt uteslutande för eget bruk. Det väsentliga kravet på att säkerställa att smarta kontrakt kan avbrytas och sägas upp förutsätter ömsesidigt samtycke från parterna i datadelningsavtalet. Tillämpligheten av de relevanta bestämmelserna i civilrätt, avtalsrätt och konsumentskyddslagstiftning på datadelningsavtal förblir eller bör förbli opåverkad av användningen av smarta kontrakt för automatiserat genomförande av sådana avtal.

- (105) För att visa att de väsentliga kraven i denna förordning är uppfyllda bör försäljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra i samband med genomförandet av ett avtal eller en del av det om att göra data tillgängliga inom ramen för denna förordning utföra en bedömning av överensstämmelse och utfärda en EU-försäkran om överensstämmelse. En sådan bedömning av överensstämmelse bör omfattas av de allmänna principerna i Europaparlamentets och rådets förordning (EG) nr 765/2008¹ och Europaparlamentets och rådets beslut (EG) nr 768/2008².
- (106) Utöver skyldigheten för professionella utvecklare av smarta kontrakt att uppfylla väsentliga krav är det också viktigt att uppmuntra de deltagare inom dataområden som erbjuder data eller databaserade tjänster till andra deltagare inom och mellan gemensamma europeiska dataområden att stödja interoperabilitet mellan verktyg för datadelning, inbegripet smarta kontrakt.

¹ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

² Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

- (107) För att säkerställa tillämpning och genomdrivande av denna förordning bör medlemsstaterna utse en eller flera behöriga myndigheter. Om en medlemsstat utser mer än en behörig myndighet bör den också bland dem utse en datasamordnare. De behöriga myndigheterna bör samarbeta med varandra. Genom att utöva sina utredningsbefogenheter i enlighet med tillämpliga nationella förfaranden bör de behöriga myndigheterna kunna söka efter och erhålla information, särskilt om en enhets verksamhet som omfattas av deras behörighet och, inbegripet i samband med gemensamma utredningar, med vederbörlig hänsyn till det faktum att åtgärder för tillsyn och efterlevnadskontroll avseende en enhet som omfattas av en annan medlemsstats behörighet bör antas av den behöriga myndigheten i den andra medlemsstaten, i förekommande fall, i enlighet med förfarandena för gränsöverskridande samarbete. De behöriga myndigheterna bör bistå varandra i god tid, särskilt när en behörig myndighet i en medlemsstat har relevant information för en utredning som utförs av de behöriga myndigheterna i andra medlemsstater, eller kan samla in sådan information som de behöriga myndigheterna i den medlemsstat där enheten är etablerad inte har tillgång till. De behöriga myndigheterna och datasamordnarna bör anges i ett offentligt register som upprätthålls av kommissionen. Datasamordnaren skulle kunna bidra till att underlätta samarbete i gränsöverskridande situationer, som när en behörig myndighet i en viss medlemsstat inte vet vilken myndighet den bör vända sig till i datasamordnarens medlemsstat, till exempel om ärendet rör mer än en behörig myndighet eller sektor. Datasamordnaren bör bland annat fungera som gemensam kontaktpunkt för alla frågor som rör tillämpningen av denna förordning. Om ingen datasamordnare har utsetts bör den behöriga myndigheten åta sig de uppgifter som tilldelas datasamordnaren enligt denna förordning. De myndigheter som ansvarar för tillsynen över uppfyllandet av rätten på området dataskydd och de behöriga myndigheter som utses inom ramen för unionsrätten eller nationell rätt bör ansvara för denna förordnings tillämpning inom sina behörighetsområden. För att undvika intressekonflikter bör de behöriga myndigheter som ansvarar för tillämpningen och efterlevnaden av denna förordning på området för tillhandahållande av data efter en begäran på grundval av ett exceptionellt behov inte ha rätt att lämna in en sådan begäran.

- (108) Fysiska och juridiska personer bör, för att hävda sina rättigheter enligt denna förordning vid överträdelse av deras rättigheter enligt denna förordning, ha rätt att söka omprövning genom att inkomma med ett klagomål. Datasamordnaren bör, på begäran, förse fysiska och juridiska personer med all nödvändig information för att de ska kunna lämna in sina klagomål till den relevanta behöriga myndigheten. Dessa myndigheter bör vara skyldiga att samarbeta för att säkerställa att ett klagomål hanteras på rätt sätt och löses effektivt och i god tid. För att utnyttja mekanismen för nätverket för konsumentskyddssamarbete och möjliggöra representativa åtgärder omfattar denna förordning en ändring av bilagorna till Europaparlamentets och rådets förordning (EU) 2017/2394¹ och Europaparlamentets och rådets direktiv (EU) 2020/1828².

¹ Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004 (EUT L 345, 27.12.2017, s. 1).

² Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om gruppanspråk för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

- (109) De behöriga myndigheterna bör säkerställa att överträdelser av de skyldigheter som fastställs i denna förordning blir föremål för påföljder. Sådana påföljder kan bland annat inkludera ekonomiska sanktioner, varningar, reprimander eller förelägganden om att affärsmetoder ska uppfylla de skyldigheter som föreskrivs i denna förordning. Påföljder som fastställs av medlemsstaterna bör vara ändamålsenliga, proportionella och avskräckande och bör ta hänsyn till rekommendationerna från Europeiska datainnovationsstyrelsen och på så sätt bidra till att största möjliga enhetlighet uppnås vid fastställandet och tillämpningen av påföljder. När så är lämpligt bör de behöriga myndigheterna använda sig av interimistiska åtgärder för att begränsa effekterna av en påstådd överträdelse medan utredningen av överträdelsen pågår. När de gör detta bör de ta hänsyn till bland annat överträdelsens art, allvar, omfattning och varaktighet med tanke på det allmänintresse som står på spel, omfattningen och typen av verksamhet som bedrivs samt överträdarens ekonomiska kapacitet. De bör även ta hänsyn till om den överträdande parten till överträdelsen systematiskt eller återkommande underlåter att uppfylla sina skyldigheter enligt den här förordningen. För att säkerställa efterlevnaden av principen *ne bis in idem*, och i synnerhet för att undvika att samma överträdelse av skyldigheterna enligt den här förordningen bestraffas mer än en gång, och för, bör en medlemsstat som avser att utöva sin behörighet gentemot en överträdare som inte är etablerad och inte har utsett en rättslig företrädare i unionen utan oskäligt dröjsmål informera alla datasamordnare och kommissionen.

- (110) Europeiska datainnovationsstyrelsen bör ge råd till och bistå kommissionen i samordningen av nationell praxis och politik på de områden som omfattas av den här förordningen samt i uppnåendet av dess mål när det gäller teknisk standardisering för att förbättra interoperabiliteten. Den bör också spela en nyckelroll när det gäller att underlätta omfattande diskussioner mellan behöriga myndigheter om tillämpningen och efterlevnaden av den här förordningen. Detta informationsutbyte är utformat för att öka den faktiska tillgången till rättslig prövning samt kontrollen av efterlevnad och rättsligt samarbete i hela unionen. De behöriga myndigheterna bör bland annat använda Europeiska datainnovationsstyrelsen som en plattform för att utvärdera, samordna och anta rekommendationer om fastställande av påföljder för överträdelser av den här förordningen. Den bör göra det möjligt för behöriga myndigheter att, med bistånd av kommissionen, samordna det optimala tillvägagångssättet för att fastställa och ålägga sådana påföljder. Detta tillvägagångssätt förhindrar fragmentering samtidigt som medlemsstaterna ges flexibilitet, och bör leda till effektiva rekommendationer som stöder en konsekvent tillämpning av den här förordningen. Europeiska datainnovationsstyrelsen bör också ha en rådgivande roll i standardiseringsprocesserna och antagandet av gemensamma specifikationer genom genomförandeakter, i antagandet av delegerade akter för att inrätta en övervakningsmekanism för uttags- och bytesavgifter som åläggs av leverantörer av databehandlingstjänster och för att ytterligare specificera de väsentliga kraven för interoperabilitet mellan data, för mekanismer och tjänster för datadelning samt för de gemensamma europeiska dataområdena. Den bör också ge råd till och bistå kommissionen vid antagandet av riktlinjerna med interoperabilitetsspecifikationer för de gemensamma europeiska dataområdenas funktion.

- (111) För att hjälpa företagen att utarbeta och förhandla fram avtal bör kommissionen utveckla och rekommendera icke-bindande standardavtalsvillkor för avtal om datadelning mellan företag, vid behov med beaktande av villkoren inom enskilda sektorer och befintlig praxis för frivilliga datadelningsmekanismer. Dessa standardavtalsvillkor bör i första hand fungera som ett praktiskt verktyg som hjälper i synnerhet mikroföretag och små och medelstora företag att ingå avtal. När sådana standardavtalsvillkor används brett och på ett integrerat sätt bör de också ha den positiva effekten att de påverkar utformningen av avtal avseende åtkomst till och användning av data och därmed mer generellt leder till rättvisare avtalsförhållanden för åtkomst till och delning av data.
- (112) För att undanröja risken för att innehavare av data i databaser som erhålls eller genereras med hjälp av fysiska komponenter, såsom sensorer, i en uppkopplad produkt och en tillhörande tjänst eller andra maskingenererade data, åberopar rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG och de därigenom i synnerhet hindrar ett effektivt utövande av användarnas rätt till åtkomst till och användning av data och deras rätt att dela data med tredje parter enligt denna förordning, bör det klargöras att rätten av sitt eget slag inte gäller för sådana databaser. Detta påverkar inte den eventuella tillämpningen av rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG på databaser som innehåller data som inte omfattas av denna förordning, förutsatt att kraven om skydd enligt punkt 1 i den artikeln är uppfyllda.

- (113) För att ta hänsyn till tekniska aspekter av databehandlingstjänster bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på komplettering av denna förordning för att införa en mekanism för övervakning av de avgifter som leverantörer av databehandlingstjänster på marknaden tar ut vid leverantörsbyten och för att ytterligare specificera de väsentliga kraven avseende interoperabilitet för deltagare i dataområden som erbjuder andra deltagare data eller datatjänster när det gäller interoperabilitet. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning¹. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

¹ EUT L 123, 12.5.2016, s. 1.

- (114) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter med avseende på antagandet av gemensamma specifikationer för att säkerställa interoperabiliteten för data, för datadelningsmekanismer och tjänster, samt för gemensamma europeiska dataområden, gemensamma specifikationer för interoperabla databehandlingstjänster, och gemensamma specifikationer för smarta kontrakt. Genomförandebefogenheter bör även tilldelas kommissionen med avseende på att offentliggöra hänvisningar till harmoniserade standarder och gemensamma specifikationer för interoperabla databehandlingstjänster i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011¹.
- (115) Denna förordning bör inte påverka tillämpningen av regler som avser behov som är specifika för enskilda sektorer eller områden av allmänt intresse. Sådana regler kan innefatta ytterligare krav som avser de tekniska aspekterna av åtkomsten till data, såsom gränssnitt för dataåtkomst, eller hur dataåtkomsten kan tillhandahållas, exempelvis direkt från en produkt eller via dataförmedlingstjänster. Sådana regler kan också omfatta begränsningar av datahållares rätt till åtkomst till eller användning av användardata, eller andra aspekter utöver dataåtkomst och dataanvändning, såsom styrningsaspekter eller säkerhetskrav, inbegripet cybersäkerhetskrav. Denna förordning bör inte heller påverka tillämpningen av mer specifika regler i samband med utvecklingen av gemensamma europeiska dataområden eller, med förbehåll för de undantag som anges i denna förordning, unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

¹ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

- (116) Denna förordning bör inte påverka tillämpningen av konkurrensreglerna, särskilt artiklarna 101 och 102 i EUF-fördraget. De åtgärder som föreskrivs i denna förordning bör inte användas för att begränsa konkurrensen på ett sätt som strider mot EUF-fördraget.
- (117) För att ge de aktörer som omfattas av denna förordning möjlighet att anpassa sig till de nya reglerna i denna förordning och inrätta de nödvändiga tekniska arrangemangen bör dessa regler börja gälla från och med den ... [20 månader från dagen för denna förordnings ikraftträdande].
- (118) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.1 och 42.2 i förordning (EU) 2018/1725 och avgav sina yttranden den 4 maj 2022.
- (119) Eftersom målen för denna förordning, nämligen att säkerställa en rättvis fördelning av värdet från data bland aktörer i dataekonomin och främja en rättvis åtkomst till och användning av data för att bidra till genomförandet av en verklig inre marknad för data, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar och den gränsöverskridande användningen av data, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Kapitel I

Allmänna bestämmelser

Artikel 1

Innehåll och tillämpningsområde

1. I denna förordning fastställs harmoniserade regler om bland annat
 - a) att göra produktdata och data från en tillhörande tjänst tillgängliga för användaren av den uppkopplade produkten eller den tillhörande tjänsten,
 - b) datahållares tillhandahållande av data till datamottagare,
 - c) datahållares tillhandahållande av data till offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan, när det finns ett exceptionellt behov av dessa data för utförandet av en specifik uppgift av allmänt intresse,
 - d) att underlätta byten av databehandlingstjänster,
 - e) att införa skyddsåtgärder mot olaglig åtkomst för tredje part till icke-personuppgifter, och
 - f) utveckling av interoperabilitetsstandarder för åtkomst till, överföring och användning av data.

2. Denna förordning omfattar personuppgifter och icke-personuppgifter, inbegripet följande typer av data i följande sammanhang:
- a) Kapitel II är tillämpligt på data, med undantag för innehåll, avseende uppkopplade produkters och tillhörande tjänsters prestanda, användning och miljö.
 - b) Kapitel III är tillämpligt på data från den privata sektorn som omfattas av lagstadgade skyldigheter i fråga om datadelning.
 - c) Kapitel IV är tillämpligt på data från den privata sektorn som är åtkomliga och används på grundval av avtal mellan företag.
 - d) Kapitel V är tillämpligt på data från den privata sektorn med fokus på icke-personuppgifter.
 - e) Kapitel VI är tillämpligt på data och tjänster som behandlas av leverantörer av databehandlingstjänster.
 - f) Kapitel VII är tillämpligt på icke-personuppgifter som innehas i unionen av leverantörer av databehandlingstjänster.
3. Denna förordning är tillämplig på följande:
- a) Tillverkare av uppkopplade produkter som släpps ut på marknaden i unionen och leverantörer av tillhörande tjänster, oberoende av dessa tillverkares och leverantörers etableringsort.

- b) Användare i unionen av uppkopplade produkter eller tillhörande tjänster som avses i led a.
 - c) Datahållare, oberoende av etableringsort, som gör data tillgängliga för datamottagare i unionen.
 - d) Datamottagare i unionen som ges tillgång till data.
 - e) Offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan som begär att datahållare gör data tillgängliga när det finns ett exceptionellt behov av dessa data för utförandet av en specifik uppgift av allmänt intresse samt de datahållare som tillhandahåller data till följd av en sådan begäran.
 - f) Leverantörer av databehandlingstjänster, oberoende av deras etableringsort, som tillhandahåller sådana tjänster till kunder i unionen.
 - g) Deltagare i dataområden och leverantörer av applikationer som använder smarta kontrakt och personer vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra i samband med genomförandet av ett avtal.
4. När det i denna förordning hänvisas till uppkopplade produkter eller tillhörande tjänster anses sådana hänvisningar även omfatta virtuella assistenter, i den mån de interagerar med en uppkopplad produkt eller tillhörande tjänst.

5. Denna förordning påverkar inte tillämpningen av unionsrätt och nationell rätt om skydd av personuppgifter, integritet och konfidentialitet vid kommunikation samt terminalutrustningens integritet, som ska tillämpas på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i denna förordning, i synnerhet inte förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv 2002/58/EG, inbegripet tillsynsmyndigheternas befogenheter och behörighet och registrerades rättigheter. I den mån användare är registrerade ska de rättigheter som fastställs i kapitel II i den här förordningen komplettera registrerades rättigheter till tillgång och rättigheter till dataportabilitet enligt artiklarna 15 och 20 i förordning (EU) 2016/679. Om den här förordningen står i strid med unionsrätt om skydd av personuppgifter eller integritet eller med nationell lagstiftning som antagits i enlighet med sådan unionsrätt, ska relevant unionsrätt eller nationell rätt om skydd av personuppgifter eller integritet äga företräde.
6. Denna förordning ska inte tillämpas på eller föregripa frivilliga arrangemang för utbyte av data mellan privata och offentliga enheter, i synnerhet frivilliga arrangemang för datadelning.

Denna förordning påverkar inte unionsrättsakter eller nationella rättsakter som föreskriver delning, åtkomst till och användning av data för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, eller för tull- och skatteändamål, i synnerhet förordningarna (EU) 2021/784, (EU) 2022/2065 och (EU) 2023/1543 samt direktiv (EU) 2023/1544, eller internationellt samarbete på det området. Den här förordningen är inte tillämplig på insamling, delning, eller användning av eller åtkomst till data enligt förordning (EU) 2015/847 och direktiv (EU) 2015/849. Den här förordningen är inte tillämplig på områden som inte omfattas av unionsrätten och påverkar under inga omständigheter medlemsstaternas befogenheter i fråga om allmän säkerhet, försvar eller nationell säkerhet, oavsett vilken typ av enhet som medlemsstaterna har anförtrott att utföra uppgifter inom ramen för dessa befogenheter eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning. Den här förordningen påverkar inte medlemsstaternas befogenheter i fråga om tull- och skatteförvaltning eller medborgares hälsa och säkerhet.

7. Denna förordning kompletterar metoden för självreglering i förordning (EU) 2018/1807 genom att lägga till allmänt tillämpliga skyldigheter för byte av molntjänster.
8. Denna förordning påverkar inte tillämpningen av unionsrättsakter och nationella rättsakter som skyddar immateriella rättigheter, i synnerhet direktiv 2001/29/EG, 2004/48/EG och (EU) 2019/790.

9. Denna förordning kompletterar, och påverkar inte tillämpningen av, unionsrätt som syftar till att främja konsumenters intressen och säkerställa en hög nivå av konsumentskydd samt att skydda deras hälsa, säkerhet och ekonomiska intressen, i synnerhet direktiv 93/13/EEG, 2005/29/EG och 2011/83/EU.
10. Denna förordning hindrar inte ingåendet av frivilliga avtal om laglig datadelning, inbegripet avtal som ingås på ömsesidig grund, som uppfyller kraven i denna förordning.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *data*: varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, fakta eller information, även i form av ljudupptagningar, bildupptagningar eller audiovisuella upptagningar.
2. *metadata*: en strukturerad beskrivning av innehållet i eller användningen av data som underlättar sökningen i eller användningen av dessa data.
3. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.
4. *icke-personuppgifter*: andra data än personuppgifter.

5. *uppkopplad produkt*: alla varor som erhåller, genererar eller samlar in data om sin användning eller om sin miljö, och som kan kommunicera produktdata via en elektronisk kommunikationstjänst, fysisk åtkomst, åtkomst genom uppkoppling eller åtkomst i enheten, och vars huvudfunktion inte är att lagra, behandla eller överföra data för någon annan part än användaren.
6. *tillhörande tjänst*: en digital tjänst, annan än en elektronisk kommunikationstjänst, inbegripet programvara, som är ansluten till produkten vid tidpunkten för köp, hyra eller leasing på ett sådant sätt att den uppkopplade produkten inte skulle kunna utföra en eller flera av sina funktioner utan den, eller som senare ansluts till produkten av tillverkaren eller en tredje part för att lägga till, uppdatera eller anpassa funktioner hos den uppkopplade produkten.
7. *behandling*: en åtgärd eller kombination av åtgärder som utförs på data eller datamängder, oberoende av om de utförs automatiserat eller ej, 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.
8. *databehandlingstjänst*: en digital tjänst som tillhandahålls en kund och som möjliggör allmän nätverkstillgång på begäran till en gemensam pool av konfigurerbara, skalbara och elastiska databehandlingsresurser av centraliserad, distribuerad eller mycket distribuerad art och som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller interaktion med tjänsteleverantören.

9. *samma tjänstetyp*: en uppsättning databehandlingstjänster som delar samma primära mål, databehandlingstjänstmodell och huvudsakliga funktioner.
10. *dataförmedlingstjänst*: dataförmedlingstjänst enligt definitionen i artikel 2.11 i förordning (EU) 2022/868.
11. *registrerad*: registrerad som avses i artikel 4.1 i förordning (EU) 2016/679.
12. *användare*: en fysisk eller juridisk person som äger en uppkopplad produkt eller till vilken tillfälliga rättigheter att använda den uppkopplade produkten har överlåtits genom avtal, eller som erhåller tillhörande tjänster.
13. *datahållare*: en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med denna förordning, tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda och tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats.
14. *datamottagare*: en fysisk eller juridisk som agerar för syften kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke och som är en annan än användaren av en uppkopplad produkt eller tillhörande tjänst, för vilken datahållaren gör data tillgängliga, inbegripet en tredje part på begäran från användaren till datahållaren eller i enlighet med en rättslig skyldighet enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten.

15. *produktdata*: data som genereras genom användning av en uppkopplad produkt och som tillverkaren har utformat för att kunna hämtas via en elektronisk kommunikationstjänst, via fysisk åtkomst eller åtkomst i enheten av en användare, datahållare eller en tredje part, inbegripet tillverkaren i tillämpliga fall.
16. *data från en tillhörande tjänst*: data som representerar digitaliseringen av användaråtgärder eller användarhändelser som kan härledas från den uppkopplade produkten och som registreras avsiktligt av användaren eller genereras som en biprodukt av användarens åtgärd under tillhandahållandet av en tillhörande tjänst av leverantören.
17. *lätt åtkomliga data*: produktdata och data från en tillhörande tjänst som en datahållare lagligen erhåller eller lagligen kan erhålla från den uppkopplade produkten eller tillhörande tjänsten, utan oproportionella ansträngningar som går utöver en enkel åtgärd.
18. *företagshemlighet*: företagshemlighet enligt definitionen i artikel 2.1 i direktiv (EU) 2016/943.
19. *innehavare av en företagshemlighet*: en innehavare av en företagshemlighet enligt definitionen i artikel 2.2 i direktiv (EU) 2016/943.
20. *profilering*: profilering enligt definitionen i artikel 4.4 i förordning (EU) 2016/679.
21. *tillhandahållande på marknaden*: leverans av en uppkopplad produkt för distribution, förbrukning eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller gratis.

22. *utsläppande på marknaden*: det första tillhandahållandet av en uppkopplad produkt på unionens marknad.
23. *konsument*: en fysisk person som agerar för ändamål som faller utanför den personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.
24. *företag*: en fysisk eller juridisk person som när det gäller avtal eller praxis som omfattas av denna förordning agerar för syften som är kopplade till personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.
25. *små företag*: små företag enligt definitionen i artikel 2.2 i bilagan till rekommendation 2003/361/EG.
26. *mikroföretag*: ett mikroföretag enligt definitionen i artikel 2.3 i bilagan till rekommendation 2003/361/EG.
27. *unionsorgan*: de unionsorgan och unionsbyråer som inrättats genom eller enligt akter som antagits på grundval av fördraget om Europeiska unionen, EUF-fördraget eller fördraget om upprättandet av Europeiska atomenergigemenskapen.
28. *offentliga organ*: medlemsstaternas nationella, regionala eller lokala myndigheter och medlemsstaternas offentligrättsliga organ, eller sammanslutningar som bildats av en eller flera sådana myndigheter eller ett eller flera sådana organ.

29. *allmänt nödläge*: en exceptionell situation under en begränsad tid, såsom ett hot mot folkhälsan, ett nödläge till följd av naturkatastrofer eller en större katastrof orsakad av människan, däribland en större cybersäkerhetsincident, med negativa konsekvenser för befolkningen i unionen, en medlemsstat eller en del av en medlemsstat, och som medför en risk för allvarliga och bestående återverkningar på levnadsvillkoren eller den ekonomiska och finansiella stabiliteten, eller avsevärd och omedelbar värdeminskning av ekonomiska tillgångar i unionen eller berörda medlemsstater, och som fastställs och officiellt utlyses i enlighet med relevanta förfaranden i unionsrätten eller nationell rätt.
30. *kund*: en fysisk eller juridisk person som har ingått ett avtalsförhållande med en leverantör av databehandlingstjänster i syfte att använda en eller flera databehandlingstjänster.
31. *virtuella assistenter*: programvara som kan behandla uppmaningar, uppdrag eller frågor, inbegripet sådana baserade på ljud, skrift, gester eller rörelse, och som baserat på dessa uppmaningar, uppdrag eller frågor ger åtkomst till andra tjänster eller kontrollerar uppkopplade produkters funktioner.
32. *digitala tillgångar*: element i digitalt format, inbegripet applikationer, för vilka kunden har nyttjanderätt, oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från.
33. *lokal IKT-infrastruktur*: IKT-infrastruktur och databehandlingsresurser som ägs, hyrs eller leasas av kunden, är belägna i kundens egen datacentral och drivs av kunden eller en tredje part.

34. *byte*: process som inbegriper en ursprunglig leverantör av databehandlingstjänster, en kund till en databehandlingstjänst och, i tillämpliga fall, en destinationsleverantör av databehandlingstjänster, varigenom kunden till en databehandlingstjänst byter från användning av en databehandlingstjänst till användning av en annan databehandlingstjänst av samma tjänstetyp eller en annan tjänst som erbjuds av en annan leverantör av databehandlingstjänster, eller till lokal IKT-infrastruktur, inbegripet genom extrahering, anpassning och uppladdning av data.
35. *uttagsavgifter för data*: avgifter för dataöverföring som tas ut av kunder för att de ska kunna extrahera sina data genom nätverket från IKT-infrastrukturen hos en leverantör av databehandlingstjänster till en annan leverantörs system eller till lokal IKT-infrastruktur.
36. *bytesavgifter*: andra avgifter än standardavgifter eller straffavgifter för förtida uppsägning som en leverantör av databehandlingstjänster tar ut av en kund för de åtgärder som föreskrivs i denna förordning för att byta till en annan leverantörs system eller till lokal IKT-infrastruktur.
37. *funktionell likvärdighet*: att på grundval av kundens exporterbara data och digitala tillgångar återställa en miniminivå av funktionalitet i miljön för en ny databehandlingstjänst av samma tjänstetyp efter bytesprocessen, där destinationstjänsten för databehandling levererar ett väsentligen jämförbart resultat som svar på samma input för delade funktioner som tillhandahålls kunden enligt avtalet.

38. *exporterbara data*: vid tillämpning av artiklarna 23–31 och 35, in- och utdata, inklusive metadata, som direkt eller indirekt genereras eller samgenereras genom kundens användning av databehandlingstjänsten, med undantag för tillgångar eller data som skyddas genom immateriella rättigheter, eller som utgör en företagshemlighet, som tillhör leverantörer av databehandlingstjänster eller tredje parter.
39. *smart kontrakt*: ett datorprogram som används för automatiserat genomförande av ett avtal eller en del därav med hjälp av en sekvens av elektroniska dataposter och som säkerställer deras integritet och korrektheten hos deras kronologiska ordningsföljd.
40. *interoperabilitet*: förmågan hos två eller fler dataområden eller kommunikationsnät, system, uppkopplade produkter, applikationer, databehandlingstjänster eller komponenter att utbyta och använda data för att utföra sina funktioner.
41. *öppen interoperabilitetsspecifikation*: en teknisk specifikation på informations- och kommunikationsteknikområdet som är resultatinriktad på att uppnå interoperabilitet mellan databehandlingstjänster.
42. *gemensamma specifikationer*: ett dokument, som inte är en standard, vilket omfattar tekniska lösningar som gör det möjligt att uppfylla vissa krav och skyldigheter som fastställs enligt denna förordning.
43. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

Kapitel II

Datadelning mellan företag och konsumenter och mellan företag

Artikel 3

Skyldighet att göra produktdata och data från tillhörande tjänster tillgängliga för användaren

1. Uppkopplade produkter ska utformas och tillverkas, och tillhörande tjänster ska utformas och tillhandahållas, så att produktdata och data från tillhörande tjänster, inbegripet relevanta metadata som krävs för att tolka och använda dessa data, som standard är direkt tillgängliga för användaren, när detta är relevant och tekniskt möjligt, på ett enkelt, säkert och kostnadsfritt sätt i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format.
2. Innan ett avtal om köp, hyra eller leasing av en uppkopplad produkt ingås ska försäljaren, uthyraren eller leasegivaren, som får vara tillverkaren, lämna åtminstone följande information till användaren i ett tydligt och begripligt sätt:
 - a) Typen, formatet och den uppskattade mängden produktdata som den uppkopplade produkten kan generera.
 - b) Huruvida den uppkopplade produkten kan generera data kontinuerligt och i realtid.
 - c) Huruvida den uppkopplade produkten kan lagra data på enheten eller på en fjärrserver, inbegripet, i förekommande fall, den planerade lagringstiden.

- d) Hur användaren kan få åtkomst till, hämta eller, i relevanta fall, radera datan, inbegripet de tekniska medlen för detta, samt deras användningsvillkor och tjänstekvalitet.

3. Innan ett avtal om tillhandahållande av en tillhörande tjänst ingås ska leverantören av en sådan tjänst lämna åtminstone följande information till användaren på ett tydligt och begripligt sätt:

- a) Arten, den uppskattade mängden och insamlingsfrekvensen för de produktdata som den presumtiva datahållaren förväntas erhålla och, i förekommande fall, villkoren för användarens åtkomst till eller hämtning av sådana data, inbegripet den presumtiva datahållarens arrangemang för datalagring och lagringstiden.
- b) Arten och den uppskattade mängden av de data från tillhörande tjänster som ska genereras samt villkoren för användarens åtkomst till eller hämtning av sådana data, inbegripet den presumtiva datahållarens arrangemang för datalagring och lagringstiden.
- c) Huruvida den presumtiva datahållaren förväntar sig att själv använda lätt åtkomliga data och de ändamål för vilka dessa data ska användas, och om den avser att tillåta en eller flera tredje parter att använda dessa data för ändamål som överenskommits med användaren.
- d) Den presumtiva datahållarens och, i tillämpliga fall, andra databehandlingsparter, identitet, såsom dennes företagsnamn och den geografiska adress där denne är etablerad.
- e) De kommunikationsmedel som gör det möjligt att snabbt kontakta den presumtiva datahållaren och effektivt kommunicera med denna.

- f) Hur användaren kan begära att data delas med en tredje part och, i förekommande fall, avsluta datadelningen.
- g) Användarens rätt att lämna in ett klagomål om överträdelse av någon av bestämmelserna i detta kapitel till den behöriga myndighet som utsetts enligt artikel 37.
- h) Huruvida en presumtiv datahållare är innehavare av en företagshemlighet som ingår i de data som är åtkomliga från den uppkopplade produkten eller som genereras under tillhandahållandet av en tillhörande tjänst, och, om den presumtiva datahållaren inte är innehavaren av en företagshemlighet, identiteten på innehavaren av en företagshemlighet.
- i) Varaktigheten för avtalet mellan användaren och den presumtiva datahållaren samt villkoren för att säga upp ett sådant avtal.

Artikel 4

Användares och datahållares rättigheter och skyldigheter

när det gäller att få åtkomst till, använda och tillgängliggöra produktdata och data från tillhörande tjänster

1. Om användaren inte har direkt åtkomst till data från den uppkopplade produkten eller den tillhörande tjänsten ska datahållare utan oskäligt dröjsmål göra lätt åtkomliga data samt relevanta metadata som är nödvändiga för att tolka och använda dessa data, tillgängliga för användaren, av samma kvalitet som den som är tillgänglig för datahållaren, på ett enkelt, säkert och kostnadsfritt sätt i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format och, i tillämpliga fall och där så är tekniskt genomförbart, kontinuerligt och i realtid. Detta ska göras på grundval av en enkel begäran på elektronisk väg om det är tekniskt möjligt.

2. Användare och datahållare får genom avtal begränsa eller förbjuda åtkomst till, användning eller ytterligare datadelning, om sådan behandling skulle kunna undergräva säkerhetskraven för den uppkopplade produkten, i enlighet med unionsrätten eller nationell rätt, och leda till allvarliga negativa effekter på fysiska personers hälsa, säkerhet eller trygghet. Behöriga myndigheter får tillhandahålla användare och datahållare teknisk expertis i detta sammanhang. Om datahållaren vägrar att dela data enligt denna artikel ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.
3. Utan att det påverkar användarens rätt att när som helst begära prövning vid en domstol i en medlemsstat får användaren, i samband med en tvist med datahållaren om de avtalsenliga begränsningar eller förbud som avses i punkt 2,
 - a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, eller
 - b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.
4. Datahållare får inte göra det orimligt svårt för användaren att göra val eller utöva rättigheter enligt denna artikel, till exempel genom att erbjuda användaren val på ett icke-neutralt sätt eller genom att undergräva eller försämra användarens självständighet, beslutsfattande eller val via strukturen, utformningen, funktionen eller driftssättet för ett digitalt användargränssnitt eller en del därav.

5. För att kontrollera om en fysisk eller juridisk person kan anses vara en användare vid tillämpning av punkt 1 får en datahållare inte kräva att denna person lämnar någon information utöver vad som är nödvändigt. Datahållare får inte spara någon information, i synnerhet inte loggdata, om användarens åtkomst till de data som begärs utöver vad som är nödvändigt för ett korrekt utförande av användarens begäran om åtkomst och för säkerheten och underhållet av datainfrastrukturen.
6. Företagshemligheter ska bevaras och får endast röjas om datahållaren och användaren före utlämnandet vidtar alla nödvändiga åtgärder för att bevara deras konfidentialitet, särskilt avseende tredje parter. Datahållaren, eller om det inte är samma person, innehavaren av en företagshemlighet, ska identifiera de data som skyddas som företagshemligheter, inbegripet i relevanta metadata, och ska komma överens med användaren om de proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten för delade data, särskilt i förhållande till tredje parter, såsom standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder.

7. Om det inte finns någon överenskommelse om de nödvändiga åtgärder som avses i punkt 6, eller om användaren underlåter att genomföra de åtgärder som överenskommit enligt punkt 6 eller äventyrar företagshemligheternas konfidentialitet, får datahållaren hindra eller, i förekommande fall, avbryta delningen av data som identifierats som företagshemligheter. Datahållarens beslut ska vara vederbörligen motiverat och lämnas skriftligen till användaren utan oskäligt dröjsmål. I sådana fall ska datahållaren underrätta den behöriga myndighet som utsetts enligt artikel 37 om att den har hindrat eller avbrutit datadelning och identifiera vilka åtgärder som inte har överenskommit eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats.
8. Om en datahållare som är en innehavare av en företagshemlighet kan visa att det är högst sannolikt att denne kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de tekniska och organisatoriska åtgärder som vidtagits av användaren enligt punkt 6 i denna artikel, får den datahållaren, under exceptionella omständigheter och från fall till fall, avslå en begäran om åtkomst till de specifika data som avses. Detta påvisande ska vara vederbörligen motiverat på grundval av objektiva faktorer, särskilt verkställbarheten av skyddet av företagshemligheter i tredjeländer, begärda datas art och grad av konfidentialitet samt den uppkopplade produktens unika och nya karaktär, och ska tillhandahållas användaren skriftligen utan oskäligt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.

9. Utan att det påverkar en användares rätt att när som helst begära prövning vid en domstol i en medlemsstat, får en användare som vill bestrida en datahållares beslut att vägra eller att hindra eller avbryta datadelning enligt punkterna 7 och 8
- a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål ska besluta huruvida och på vilka villkor datadelning ska inledas eller återupptas, eller
 - b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.
10. Användaren får inte använda de data som erhållits till följd av en begäran som avses i punkt 1 för att utveckla en uppkopplad produkt som konkurrerar med den uppkopplade produkt som dessa data härrör från och inte heller dela dessa data med en tredje part i detta syfte och får inte använda sådana data för att skaffa sig inblick i tillverkarens, eller i förekommande fall datahållarens, ekonomiska situation, tillgångar och produktionsmetoder.
11. Användaren får inte, för att få åtkomst till data, använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur som utformats för att skydda data.
12. Om användaren inte är den registrerade vars personuppgifter begärs ska datahållaren tillgängliggöra personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst för användaren endast om det finns en giltig rättslig grund för behandling enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, om villkoren i artikel 9 i den förordningen och i artikel 5.3 i direktiv 2002/58/EG är uppfyllda.

13. En datahållare får endast använda lätt åtkomliga data som är icke-personuppgifter på grundval av ett avtal med användaren. En datahållare får inte använda sådana data för att få inblick i användarens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva användarens kommersiella ställning på de marknader där användaren är verksam.
14. Datahållare får inte göra sådana produktdata som är icke-personuppgifter tillgängliga för tredje parter för kommersiella eller icke-kommersiella ändamål annat än för att fullgöra avtalet med användaren. Vid behov ska datahållare genom avtal förbinda tredje parter att inte dela vidare data som de har mottagit från dem.

Artikel 5

Användarens rätt att dela data med tredje parter

1. På begäran av en användare, eller av en part som agerar för en användares räkning, ska datahållaren utan oskäligt dröjsmål för en tredje part tillgängliggöra lätt åtkomliga data samt de relevanta metadata som är nödvändiga för att tolka och använda dessa data, av samma kvalitet som den som är tillgänglig för datahållaren, på ett enkelt och säkert sätt, kostnadsfritt för användaren, i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format och, när så är relevant och tekniskt genomförbart, kontinuerligt och i realtid. Data ska göras tillgänglig av datahållaren för den tredje parten i enlighet med artiklarna 8 och 9.

2. Punkt 1 ska inte gälla lätt åtkomliga data i samband med testning av nya uppkopplade produkter, ämnen eller processer som ännu inte har släppts ut på marknaden, såvida inte tredje parts användning av dem är tillåten enligt avtal.
3. Ett företag som har utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925 ska inte vara en godtagbar tredje part enligt den här artikeln och får därför inte
 - a) på något sätt söka utverka eller erbjuda kommersiellt incitament till en användare, inbegripet genom att tillhandahålla ekonomisk eller annan ersättning, för att användaren ska göra data som användaren har erhållit till följd av en begäran enligt artikel 4.1 tillgängliga för en av företagets tjänster,
 - b) söka utverka eller erbjuda kommersiellt incitament till en användare för att användaren ska begära att datahållaren gör data tillgängliga för en av företagets tjänster enligt punkt 1 i denna artikel,
 - c) från en användare ta emot data som användaren har erhållit till följd av en begäran enligt artikel 4.1.
4. För att kontrollera om en fysisk eller juridisk person kan anses vara en användare eller en tredje part vid tillämpning av punkt 1 ska användaren eller den tredje parten inte vara skyldig att tillhandahålla någon information utöver vad som är nödvändigt. Datahållare får inte spara någon information om den tredje partens åtkomst till begärda data utöver vad som är nödvändigt för ett korrekt utförande av den tredje partens begäran om åtkomst och för säkerheten och underhållet av datainfrastrukturen.

5. Den tredje parten får inte, för att få åtkomst till data, använda tvångsmedel eller missbruka luckor i en datahållares tekniska infrastruktur som utformats för att skydda data.
6. En datahållare får inte använda lätt åtkomliga data för att få inblick i den tredje partens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa, på något annat sätt som skulle kunna undergräva den tredje partens kommersiella ställning på de marknader där den tredje parten är verksam, såvida inte den tredje parten har gett sitt tillstånd till sådan användning och har teknisk möjlighet att när som helst och på ett enkelt sätt återkalla det tillståndet.
7. Om användaren inte är den registrerade vars personuppgifter begärs ska alla personuppgifter som genereras genom användning av en uppkopplad produkt eller tillhörande tjänst, endast göras tillgängliga av datahållaren eller den tredje parten om det finns en giltig rättslig grund för behandlingen enligt artikel 6 i förordning (EU) 2016/679 och, i förekommande fall, om villkoren i artikel 9 i den förordningen och i artikel 5.3 i direktiv 2002/58/EG är uppfyllda.
8. Om datahållaren och den tredje parten underlåter att komma överens om arrangemangen för överföring av data får detta inte hindra eller inkräkta på den registrerades utövande av sina rättigheter enligt förordning (EU) 2016/679, i synnerhet inte när det gäller rätten till dataportabilitet enligt artikel 20 i den förordningen.

9. Företagshemligheter ska bevaras och får endast röjas för tredje parter i den mån sådant röjande är absolut nödvändigt för att uppfylla det syfte som överenskommits mellan användaren och den tredje parten. Datahållaren, eller, om det inte är samma person, innehavaren av en företagshemlighet, ska identifiera de data som skyddas som företagshemligheter, inbegripet i relevanta metadata, och ska komma överens med den tredje parten om alla proportionella tekniska och organisatoriska åtgärder som är nödvändiga för att bevara konfidentialiteten för delade data, såsom standardavtalsvillkor, avtal om konfidentialitet, strikta åtkomstprotokoll, tekniska standarder och tillämpning av uppförandekoder.
10. Om det inte finns någon överenskommelse om de nödvändiga åtgärder som avses i punkt 9 eller om den tredje parten underlåter att genomföra de åtgärder som överenskommits enligt punkt 9 eller äventyrar företagshemligheternas konfidentialitet, får datahållaren hindra eller, i förekommande fall, avbryta delningen av data som identifierats som företagshemligheter. Datahållarens beslut ska vara vederbörligen motiverat och lämnas skriftligen till den tredje parten utan oskäligt dröjsmål. I sådana fall ska datahållaren underrätta den behöriga myndighet som utsetts enligt artikel 37 om att den har hindrat eller avbrutit datadelning och identifiera vilka åtgärder som inte har överenskommits eller genomförts och, i förekommande fall, för vilka företagshemligheter konfidentialiteten har äventyrats.

11. Om en datahållare som är en innehavare av en företagshemlighet kan visa att det är högst sannolikt att denne kommer att lida allvarlig ekonomisk skada till följd av röjandet av företagshemligheter, trots de tekniska och organisatoriska åtgärder som vidtagits av den tredje parten enligt punkt 9 i denna artikel, får den datahållaren, under exceptionella omständigheter och från fall till fall, avslå en begäran om åtkomst till de specifika data som avses. Detta påvisande ska vara vederbörligen motiverat på grundval av objektiva faktorer, särskilt verkställbarheten av skyddet av företagshemligheter i tredjeländer, begärda datas art och grad av konfidentialitet samt den uppkopplade produktens unika och nya karaktär, och ska tillhandahållas den tredje parten skriftligen utan oskäligt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.
12. Utan att det påverkar tredje parts rätt att när som helst begära prövning vid en domstol i en medlemsstat, får en tredje part som vill bestrida en datahållares beslut att vägra eller att hindra eller avbryta datadelning enligt punkterna 10 och 11
- a) i enlighet med artikel 37.5 b lämna in ett klagomål till den behöriga myndigheten, som utan oskäligt dröjsmål ska besluta huruvida och på vilka villkor datadelningen ska inledas eller återupptas, eller
 - b) komma överens med datahållaren om att hänskjuta ärendet till ett tvistlösningsorgan i enlighet med artikel 10.1.
13. Den rätt som avses i punkt 1 får inte på ett ogynnsamt sätt påverka registrerades rättigheter enligt tillämplig unionsrätt och nationell rätt om skydd av personuppgifter.

Artikel 6

Skyldigheter för tredje parter som tar emot data på användarens begäran

1. En tredje part ska behandla de data som gjorts tillgängliga för den enligt artikel 5 endast för de ändamål och på de villkor som överenskommits med användaren med förbehåll för unionsrätt och nationell rätt om skyddet av personuppgifter, inbegripet den registrerades rättigheter när det gäller personuppgifter. Den tredje parten ska radera dessa data när de inte längre är nödvändiga för det överenskomna ändamålet, såvida inte annat överenskommits med användaren när det gäller personuppgifter.
2. Den tredje parten får inte
 - a) göra det orimligt svårt för användaren att göra sina val eller utöva sina rättigheter enligt artikel 5 och den här artikeln, inbegripet genom att erbjuda användaren val på ett icke-neutralt sätt, eller utöva tvång mot, vilseleda eller manipulera användaren eller genom att undergräva eller inskränka användarens självständighet, beslutsfattande eller val, inbegripet genom ett digitalt användargränssnitt eller en del därav,
 - b) utan hinder av artikel 22.2 a och c i förordning (EU) 2016/679 använda de data som den tar emot för profilering, såvida det inte är nödvändigt för att tillhandahålla den tjänst som begärs av användaren,

- c) göra de data som den tar emot tillgängliga för en annan tredje part, såvida inte datan görs tillgängliga på grundval av ett avtal med användaren, och förutsatt att den andra tredje parten vidtar alla nödvändiga åtgärder som överenskommits mellan datahållaren och den tredje parten för att bevara företagshemligheters konfidentialitet,
- d) göra de data som den tar emot tillgängliga för ett företag som har utsetts till grindvakt enligt artikel 3 i förordning (EU) 2022/1925,
- e) använda de data som den mottar för att utveckla en produkt som konkurrerar med den uppkopplade produkt från vilken de data som åtkommits härrör eller dela dessa data med en annan tredje part för det ändamålet; tredje parter får inte heller använda produktdata eller data från en tillhörande tjänst som är icke-personuppgifter och som gjorts tillgängliga för dem för att få inblick i datahållarens ekonomiska situation, tillgångar och produktionsmetoder, eller användning av dessa,
- f) använda de data som den mottar på ett sätt som inverkar negativt på säkerheten för den uppkopplade produkten eller de tillhörande tjänsterna,
- g) bortse från specifika åtgärder som överenskommits med en datahållare eller med innehavaren av företagshemligheter enligt artikel 5.9 och äventyra konfidentialiteten för företagshemligheter,
- h) hindra en användare som är en konsument, inbegripet på grundval av ett avtal, från att göra mottagna data tillgängliga för andra parter.

Artikel 7

Tillämpningsområdet för skyldigheter vad gäller datadelning mellan företag och konsumenter och mellan företag

1. Skyldigheterna i detta kapitel ska inte gälla data som genereras genom användning av uppkopplade produkter som tillverkas eller utformas, eller tillhörande tjänster som tillhandahålls av, ett mikroföretag eller ett litet företag, förutsatt att det företaget inte har ett partnerföretag eller ett anknutet företag i den mening som avses i artikel 3 i bilagan till rekommendation 2003/361/EG som inte betecknas som ett mikroföretag eller ett litet företag och när det mikroföretaget eller det lilla företaget inte tillverkar eller utformar en uppkopplad produkt eller tillhandahåller en tillhörande tjänst på entreprenad.

Detsamma ska gälla för data som genereras genom användning av uppkopplade produkter som har tillverkats eller tillhörande tjänster som har tillhandahållits av ett företag som har betecknats som ett medelstort företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, i mindre än ett år och för uppkopplade produkter under ett år från den dag då de släpptes ut på marknaden av ett medelstort företag.

2. Avtalsvillkor som till nackdel för användaren utesluter tillämpning av, avviker från eller ändrar verkan av användarens rättigheter enligt detta kapitel ska inte vara bindande för användaren.

Kapitel III

Skyldigheter för datahållare som är skyldiga att göra data tillgängliga enligt unionsrätten

Artikel 8

Villkor enligt vilka datahållare gör data tillgängliga för datamottagare

1. Om en datahållare inom ramen för förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 eller enligt annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, ska datahållaren komma överens med en datamottagare om villkoren för att göra data tillgängliga och ska göra detta på rättvisa, rimliga och icke-diskriminerande villkor och på ett öppet sätt i enlighet med detta kapitel och kapitel IV.
2. Ett avtalsvillkor om åtkomst till och användning av data eller om ansvar och rättsmedel vid överträdelse eller uppsägning av datarelaterade skyldigheter ska inte vara bindande om det utgör ett oskäligt avtalsvillkor i den mening som avses i artikel 13 eller om det, till användarens nackdel, utesluter tillämpningen av, avviker från eller ändrar verkan av användarens rättigheter enligt kapitel II.

3. En datahållare får inte, avseende åtgärder som vidtagits för att göra data tillgängliga, diskriminera mellan jämförbara kategorier av datamottagare, inbegripet datahållarens partnerföretag eller anknutna företag, när data görs tillgängliga. Om en datamottagare anser att de förhållanden under vilka data har gjorts tillgängliga för denne är diskriminerande, ska datahållaren utan oskäligt dröjsmål ge datamottagaren information, på dennes motiverade begäran, som visar att det inte har förekommit någon diskriminering.
4. En datahållare får inte, inbegripet på exklusiv grund, göra data tillgängliga för en datamottagare, såvida inte användaren begär detta enligt kapitel II.
5. Datahållare och datamottagare ska inte vara skyldiga att tillhandahålla någon information utöver vad som är nödvändigt för att kontrollera efterlevnaden av de avtalsvillkor som överenskommits för tillgängliggörande av data eller vad som är nödvändigt för uppfyllandet av deras skyldigheter enligt denna förordning eller annan tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten.
6. Om inte annat föreskrivs i unionsrätten, inbegripet artiklarna 4.6 och 5.9 i denna förordning, eller i nationell lagstiftning som antagits i enlighet med unionsrätten, ska en skyldighet att göra data tillgängliga för en datamottagare inte medföra någon skyldighet att röja företagshemligheter.

Artikel 9

Ersättning för tillgängliggörande av data

1. Ersättning som en datahållare och en datamottagare kommer överens om för att göra data tillgängliga i förbindelser mellan företag ska vara icke-diskriminerande och rimlig och får inbegripa en marginal.

2. När datahållaren och datamottagaren kommer överens om ersättning ska de särskilt beakta följande:
 - a) Kostnader för att göra data tillgängliga, inbegripet särskilt de kostnader som är nödvändiga för formatering av data, spridning med elektroniska medel och lagring.
 - b) Investeringar i insamling och framställning av data, i förekommande fall med beaktande av huruvida andra parter har bidragit till att inhämta, generera eller samla in datan i fråga.
3. Den ersättning som avses i punkt 1 kan också bero på datans volym, format och karaktär.
4. Om datamottagaren är ett mikroföretag eller ett litet eller medelstort företag eller en icke-vinstdrivande forskningsorganisation och om en sådan datamottagare inte har partnerföretag eller anknutna företag som inte räknas som mikroföretag eller små eller medelstora företag, får den överenskomna ersättningen inte överstiga de kostnader som anges i punkt 2 a.
5. Kommissionen ska anta riktlinjer för beräkningen av rimlig ersättning, med beaktande av råd från Europeiska datainnovationsstyrelsen som avses i artikel 42.
6. Denna artikel ska inte hindra annan unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten från att utesluta ersättning för tillgängliggörande av data eller föreskriva lägre ersättning.

7. Datahållaren ska ge datamottagaren tillräckligt detaljerad information om grunden för beräkningen av ersättningen så att datamottagaren kan bedöma huruvida kraven i punkt 1 och, i tillämpliga fall, punkterna 1–4 är uppfyllda.

Artikel 10

Tvistlösning

1. Användare, datahållare och datamottagare ska ha tillgång till ett tvistlösningsorgan, som certifierats i enlighet med punkt 5 i denna artikel, för att lösa tvister enligt artiklarna 4.3, 4.9 och 5.12 samt tvister avseende rättvisa, rimliga och icke-diskriminerande villkor för och öppet redovisande av data i enlighet med detta kapitel och kapitel IV.
2. Tvistlösningsorganen ska informera de berörda parterna om avgifter eller mekanismer som används för att fastställa avgifter innan dessa parter begär ett beslut.
3. När det gäller tvister som hänskjutits till ett tvistlösningsorgan enligt artiklarna 4.3, 4.9 och 5.12, om tvistlösningsorganet avgör en tvist till förmån för användaren eller datamottagaren, ska datahållaren bära alla de avgifter som tas ut av tvistlösningsorganet och ersätta den användaren eller den datamottagaren för alla andra rimliga kostnader som denne har ådragit sig i samband med tvistlösningen. Om tvistlösningsorganet avgör en tvist till förmån för datahållaren ska användaren eller datamottagaren inte vara skyldig att ersätta några avgifter eller andra utgifter som datahållaren har betalat eller ska betala i samband med tvistlösningen, såvida inte tvistlösningsorganet finner att användaren eller datamottagaren uppenbart har handlat i ond tro.

4. Kunder och leverantörer av databehandlingstjänster ska ha tillgång till ett tvistlösningsorgan, som certifierats i enlighet med punkt 5 i denna artikel, för att lösa tvister som rör överträdelser av kundernas rättigheter och de skyldigheter som leverantörer av databehandlingstjänster har, i enlighet med artiklarna 23–31.
5. Den medlemsstat där tvistlösningsorganet är etablerat ska på begäran av det organet certifiera detta, om organet har visat att det uppfyller samtliga följande villkor:
 - a) Det är opartiskt och oberoende, och ska fatta sina beslut i enlighet med tydliga, icke-diskriminerande och rättvisa förfaranderegler.
 - b) Det har den sakkunskap som krävs, i synnerhet när det gäller rättvisa, rimliga och icke-diskriminerande villkor, inbegripet ersättning, och om att göra data tillgängliga på ett öppet sätt, vilket innebär att organet på ett effektivt sätt kan fastställa dessa villkor.
 - c) Det kan enkelt nås genom elektronisk kommunikationsteknik.
 - d) Det kan anta beslut på ett snabbt, effektivt och kostnadseffektivt sätt på minst ett av unionens officiella språk.
6. Medlemsstaterna ska underrätta kommissionen om de tvistlösningsorgan som certifierats i enlighet med punkt 5. Kommissionen ska offentliggöra en förteckning över dessa organ på en särskild webbplats och hålla den uppdaterad.

7. Ett tvistlösningsorgan ska vägra att behandla en begäran om lösning av en tvist som redan har hänskjutits till ett annat tvistlösningsorgan eller till en domstol i en medlemsstat.
8. Ett tvistlösningsorgan ska ge parterna möjlighet att inom rimlig tid framföra sina synpunkter i frågor som dessa parter har begärt ska prövas vid det organet. I detta sammanhang ska varje part i en tvist förses med inlagorna från den andra parten i tvisten och eventuella utlåtanden från experter. Parterna ska ges möjlighet att lämna synpunkter på sådana inlagor och utlåtanden.
9. Ett tvistlösningsorgan ska fatta sitt beslut i en fråga som hänskjutits till det inom 90 dagar efter mottagandet av en begäran enligt punkterna 1 och 4. Detta beslut ska vara skriftligt eller på ett varaktigt medium och ska åtföljas av en motivering.
10. Tvistlösningsorganen ska utarbeta och offentliggöra årliga verksamhetsrapporter. Sådana årliga rapporter ska innehålla i synnerhet följande information:
 - a) En sammanställning av utgången av tvister.
 - b) Den genomsnittliga tid det har tagit att lösa tvister.
 - c) De vanligaste skälen till tvister.

11. För att underlätta utbytet av information och bästa praxis får ett tvistlösningsorgan besluta att inkludera rekommendationer i den rapport som avses i punkt 10 om hur problem kan undvikas eller lösas.
12. Ett tvistlösningsorgans beslut ska endast vara bindande för parterna om parterna uttryckligen och innan tvistlösningsförfarandet inleds har samtyckt till att beslutet är bindande.
13. Denna artikel påverkar inte parters rätt att söka ett effektivt rättsmedel inför en domstol i en medlemsstat.

Artikel 11

Tekniska skyddsåtgärder om obehörig användning eller obehörigt utlämnande av data

1. En datahållare får vidta lämpliga tekniska skyddsåtgärder, inbegripet smarta kontrakt och kryptering, för att förhindra obehörig åtkomst till data, inbegripet metadata, och för att säkerställa överensstämmelse med artiklarna 4, 5, 6, 8 och 9 samt med de överenskomna avtalsvillkoren för tillgängliggörande av data. Sådana tekniska skyddsåtgärder får varken diskriminera mellan datamottagare eller hindra en användares rätt att erhålla en kopia av eller hämta, använda eller få åtkomst till data eller tillhandahålla tredje parter data enligt artikel 5 eller någon rätt för tredje part enligt unionsrätten eller nationell lagstiftning som antagits i enlighet med unionsrätten. Användare, tredje parter och datamottagare får inte ändra eller avlägsna sådana tekniska skyddsåtgärder såvida inte datahållaren samtycker till detta.

2. Under de omständigheter som avses i punkt 3 ska den tredje parten eller datamottagaren utan oskäligt dröjsmål tillmötesgå begärandena från datahållaren och, i tillämpliga fall och om det inte är samma person, innehavaren av en företagshemlighet eller användaren, om
- a) att radera de data som tillhandahållits av datahållaren och eventuella kopior av dessa,
 - b) att avsluta produktion, erbjudande eller utsläppande på marknaden eller användning av varor, härledda data eller tjänster som framställts på grundval av kunskap som erhållits genom sådana data, eller import, export eller lagring av varor som innebär intrång för dessa ändamål, och förstöra alla varor som innebär intrång, om det finns en allvarlig risk för att den olagliga användningen av dessa data kommer att orsaka datahållaren, innehavaren av en företagshemlighet eller användaren betydande skada eller om en sådan åtgärd inte skulle vara oproportionell med hänsyn till intressena för datahållaren, innehavaren av en företagshemlighet eller användaren,
 - c) att informera användaren om den obehöriga användningen eller det obehöriga röjandet av data och om de åtgärder som vidtagits för att bringa den obehöriga användningen eller det obehöriga röjandet av dessa data att upphöra,
 - d) att ersätta den part som lider skada till följd av missbruk eller röjande av sådana data som olagligen åtkommit eller använts.
3. Punkt 2 ska vara tillämplig om en tredje part eller en datamottagare
- a) i syfte att erhålla data har lämnat falsk information till en datahållare, använt bedrägliga eller tvingande medel eller missbrukat luckor i datahållarens tekniska infrastruktur som är utformad för att skydda dessa data,

- b) har använt de data som gjorts tillgängliga för obehöriga ändamål, inbegripet utveckling av en konkurrerande uppkopplad produkt i den mening som avses i artikel 6.2 e,
 - c) olagligen har lämnat ut data till en annan part,
 - d) inte har upprätthållit de tekniska och organisatoriska åtgärder som överenskommits enligt artikel 5.9, eller
 - e) har ändrat eller avlägsnat tekniska skyddsåtgärder som tillämpas av datahållaren enligt punkt 1 i denna artikel utan datahållarens samtycke.
4. Punkt 2 ska också vara tillämplig om en användare ändrar eller avlägsnar tekniska skyddsåtgärder som datahållaren tillämpar eller inte upprätthåller de tekniska och organisatoriska åtgärder som vidtagits av användaren i samförstånd med datahållaren eller, om det inte är samma person, innehavaren av företagshemligheter, för att bevara företagshemligheter, samt med avseende på varje annan part som tar emot data från användaren i strid med denna förordning.
5. Om datamottagaren handlar i strid med artikel 6.2 a eller b ska användarna ha samma rättigheter som datahållarna enligt punkt 2 i den här artikeln.

Artikel 12

Omfattningen av skyldigheterna för datahållare som enligt unionsrätten är skyldiga att göra data tillgängliga

1. Detta kapitel ska tillämpas om en datahållare i förbindelser mellan företag är skyldig att göra data tillgängliga för en datamottagare enligt artikel 5 eller enligt tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten.

2. Ett avtalsvillkor i ett datadelningsavtal som, till nackdel för en part eller, där detta är tillämpligt, till nackdel för användaren, utesluter tillämpningen av detta kapitel, avviker från det eller ändrar dess verkan, ska inte vara bindande för den parten.

Kapitel IV

Oskäliga avtalsvillkor i samband med åtkomst till och användning av data mellan företag

Artikel 13

Oskäliga avtalsvillkor som ensidigt åläggs ett annat företag

1. Ett avtalsvillkor om åtkomst till och användning av data eller om ansvar och rättsmedel vid överträdelse eller uppsägande av datarelaterade skyldigheter som ett företag ensidigt har ålagt ett annat företag ska inte vara bindande för det senare företaget om det är oskäligt.
2. Ett avtalsvillkor som återspeglar tvingande bestämmelser i unionsrätten eller bestämmelser i unionsrätten som skulle vara tillämpliga om frågan inte reglerades i avtalsvillkoren, ska inte anses vara oskäligt.
3. Ett avtalsvillkor är oskäligt om det är av sådan art att dess användning i hög grad avviker från god affärssed vid åtkomst till och användning av data i strid med god tro och god sed.

4. Ett avtalsvillkor ska i synnerhet vara oskäligt med avseende på tillämpningen av punkt 3 om det har till syfte eller verkan att
- a) utesluta eller begränsa ansvaret för den part som ensidigt ålagt villkoret för uppsåtliga handlingar eller grov oaktsamhet,
 - b) utesluta de rättsmedel som står till buds för den part som ensidigt har ålagts villkoret i händelse av underlåtenhet att fullgöra avtalsförpliktelser eller utesluta ansvar för den part som ensidigt ålade avtalsvillkoret vid ett åsidosättande av dessa skyldigheter,
 - c) ge den part som ensidigt har föreskrivit villkoret ensamrätt att avgöra om de data som lämnas är i överensstämmelse med avtalet eller att tolka något avtalsvillkor.
5. Ett avtalsvillkor ska antas vara oskäligt med avseende på tillämpningen av punkt 3 om det har till syfte eller verkan att
- a) på ett olämpligt sätt begränsa rättsmedlen vid underlåtenhet att fullgöra avtalsförpliktelser eller begränsa ansvaret vid ett åsidosättande av dessa skyldigheter eller utvidga ansvaret för det företag som ensidigt har ålagts villkoret,

- b) tillåta den part som ensidigt införde villkoret att få åtkomst till och använda den andra avtalsslutande partens data på ett sätt som avsevärt skadar den andra avtalsslutande partens legitima intressen, särskilt när sådana data innehåller kommersiellt känsliga data eller skyddas av företagshemligheter eller immateriella rättigheter,
- c) hindra den part som ensidigt har ålagts villkoret att använda de data som den parten har tillhandahållit eller genererat under avtalsperioden, eller att begränsa användningen av sådana data i en sådan omfattning att den parten inte har rätt att använda, samla in, få åtkomst till eller kontrollera sådana data eller utnyttja värdet av sådana data på ett adekvat sätt,
- d) hindra den part som ensidigt har ålagts villkoret att säga upp avtalet inom rimlig tid,
- e) hindra den part som ensidigt har ålagts villkoret att erhålla en kopia av de data som den parten har tillhandahållit eller genererat under avtalets löptid eller inom en rimlig tidsperiod efter det att avtalet sagts upp,
- f) göra det möjligt för den part som ensidigt ålägger villkoret att säga upp avtalet med oskäligt kort varsel, med beaktande av varje rimlig möjlighet för den andra avtalsslutande parten att byta till en alternativ och jämförbar tjänst och den ekonomiska skada som följer av en sådan uppsägning, såvida det inte finns tungt vägande skäl för detta,

- g) göra det möjligt för den part som ensidigt ålägger villkoret att väsentligt ändra det pris som anges i avtalet eller andra materiella villkor för de data som ska delas med avseende på deras art, format, kvalitet eller kvantitet, om inget giltigt skäl och ingen rätt för den andra parten att säga upp avtalet vid en sådan ändring anges i avtalet.

Första stycket g ska inte påverka villkor genom vilka den part som ensidigt ålägger villkoret förbehåller sig rätten att ensidigt ändra villkoren i ett avtal med obestämd löptid, förutsatt att det i avtalet anges ett giltigt skäl för sådana ensidiga ändringar, att den part som ensidigt ålägger villkoret är skyldig att underrätta den andra avtalsslutande parten med rimligt varsel om sådana avsedda ändringar och att den andra avtalsslutande parten har rätt att utan kostnad säga upp avtalet vid en ändring.

6. Ett avtalsvillkor ska anses vara ensidigt ålagt i den mening som avses i denna artikel om det har tillhandahållits av en avtalsslutande part och den andra avtalsslutande parten inte har kunnat påverka dess innehåll trots försök att förhandla om det. Det åligger den avtalsslutande part som har tillhandahållit avtalsvillkoret att bevisa att villkoret inte har införts ensidigt. Den avtalspart som har tillhandahållit det omtvistade avtalsvillkoret kan inte göra gällande att villkoret är ett oskäligt avtalsvillkor.
7. Om det oskäligen avtalsvillkoret kan avskiljas från övriga villkor i avtalet ska dessa återstående villkor vara bindande.

8. Denna artikel är inte tillämplig på avtalsvillkor som anger avtalets huvudsakliga syfte eller på prisets lämplighet i förhållande till de data som lämnas i utbyte.
9. Parterna i ett avtal som omfattas av punkt 1 ska inte utesluta tillämpningen av denna artikel, avvika från den eller ändra dess verkan.

Kapitel V

Göra data tillgängliga för offentliga organ, kommissionen, europeiska centralbanken och unionsorgan på grundval av exceptionella behov

Artikel 14

Skyldighet att göra data tillgängliga på grundval av exceptionella behov

Om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan visar att det föreligger ett exceptionellt behov, enligt artikel 15, av att använda vissa data, inbegripet de relevanta metadata som är nödvändiga för tolkningen och användningen av dessa data, för att fullgöra sina lagstadgade skyldigheter av allmänt intresse, ska datahållare som är andra juridiska personer än offentliga organ och som innehar dessa data göra dem tillgängliga på vederbörligen motiverad begäran.

Artikel 15

Exceptionellt behov av att använda data

1. Ett exceptionellt behov av att använda vissa data i den mening som avses i detta kapitel ska vara begränsat i tid och omfattning och ska anses föreligga endast under någon av följande omständigheter:
 - a) Om de begärda data är nödvändiga för att hantera ett allmänt nödläge och det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte i tid, på ett ändamålsenligt sätt och på likvärdiga villkor kan erhålla sådana data på alternativa sätt.
 - b) Under omständigheter som inte omfattas av led a och endast när det gäller icke-personuppgifter, om
 - i) ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan agerar på grundval av unionsrätten eller nationell rätt och har identifierat specifika data, vars avsaknad hindrar den eller det från att utföra en specifik uppgift av allmänt intresse som uttryckligen föreskrivs i lag, såsom framställning av officiell statistik eller begränsning av eller återhämtning från ett allmänt nödläge, och

- ii) det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet har uttömt alla andra till buds stående medel för att erhålla sådana data, inbegripet inköp av data på marknaden genom att erbjuda marknadspris, eller genom att förlita sig på befintliga skyldigheter för att göra data tillgängliga eller antagande av nya lagstiftningsåtgärder som skulle kunna säkerställa att data finns tillgängliga i tid.

- 2. Punkt 1 b ska inte tillämpas på mikroföretag och små företag.
- 3. Skyldigheten att visa att det offentliga organet inte har kunnat erhålla icke-personuppgifter genom att köpa in dem på marknaden ska inte gälla om den specifika uppgiften av allmänt intresse är framställning av officiell statistik och om inköp av sådana data inte är tillåtet enligt nationell rätt.

Artikel 16

Förhållande till andra skyldigheter att göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan

- 1. Detta kapitel ska inte påverka de skyldigheter som fastställs i unionsrätten eller nationell rätt vad gäller rapportering eller att tillmötesgå begäranden om åtkomst till information eller visa eller kontrollera efterlevnaden av rättsliga skyldigheter.

2. Detta kapitel ska inte tillämpas på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan som bedriver verksamhet som syftar till att förebygga, utreda, upptäcka eller lagföra brott eller administrativa överträdelser eller verkställa straffrättsliga påföljder, eller på tull- eller skatteförvaltning. Detta kapitel påverkar inte tillämplig unionsrätt eller nationell rätt om förebyggande, utredning, upptäckt eller lagföring av brott eller administrativa överträdelser eller verkställighet av straffrättsliga eller administrativa sanktioner, eller för tull- eller skatteförvaltning.

Artikel 17

Begäran om att data ska göras tillgängliga

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som begär data enligt artikel 14 ska
- a) specificera vilka data som krävs, inbegripet de relevanta metadata som är nödvändiga för att tolka och använda dessa data,
 - b) visa att de nödvändiga villkor för att det föreligger ett exceptionellt behov enligt artikel 15 för det ändamål för vilket data begärs är uppfyllda,
 - c) förklara syftet med begäran, den avsedda användningen av begärda data, i tillämpliga fall även av en tredje part i enlighet med punkt 4 i denna artikel, användningens varaktighet, och när så är lämpligt hur behandlingen av personuppgifter ska tillgodose det exceptionella behovet,

- d) om möjligt specificera när data förväntas raderas av alla parter som har åtkomst till dem,
- e) motivera valet av datahållare till vilken begäran riktas,
- f) specificera eventuella andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan och de tredje parter med vilka begärda data förväntas delas,
- g) om personuppgifter begärs, specificera vilka tekniska och organisatoriska åtgärder som är nödvändiga och proportionella för att genomföra dataskyddsprinciperna och de nödvändiga skyddsåtgärderna, såsom pseudonymisering, och huruvida datahållaren kan tillämpa anonymisering innan data görs tillgängliga,
- h) ange den rättsliga bestämmelse som tilldelar det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet den specifika uppgift av allmänt intresse som är relevant för begäran om data,
- i) ange den tidsfrist inom vilken data ska tillgängliggöras och den tidsfrist som avses i artikel 18.2 inom vilken datahållaren får neka eller begära ändring av begäran,
- j) göra sitt yttersta för att undvika att ett tillmötesgående av begäran om data leder till att datahållare blir ansvariga för överträdelser av unionsrätten eller nationell rätt.

2. En begäran om data enligt punkt 1 i denna artikel ska
- a) göras skriftligen och uttryckas på ett klart, koncist och tydligt språk som kan förstås av datahållaren,
 - b) vara specifik avseende den typ av data som begärs och avse data som datahållaren har kontroll över vid tidpunkten för begäran,
 - c) stå i proportion till det exceptionella behovet och vara motiverad, i fråga om detaljnivå och omfattning av begärda data och hur ofta dessa begärda data kommer att tillgås,
 - d) respektera datahållarens legitima mål och innehålla ett åtagande om att säkerställa skyddet av företagshemligheter i enlighet med artikel 19.3 och beakta de kostnader och ansträngningar som krävs för att göra data tillgängliga,
 - e) gälla icke-personuppgifter och, endast om detta har visats vara otillräckligt för att tillgodose det exceptionella behovet av att använda data i enlighet med artikel 15.1 a, begära personuppgifter i pseudonymiserad form och fastställa de tekniska och organisatoriska åtgärder som ska vidtas för att skydda dessa data,
 - f) informera datahållaren om de sanktioner som den behöriga myndighet som utsetts enligt artikel 37 ska ålägga enligt artikel 40 om begäran inte tillmötesgås,

- g) om begäran görs av ett offentligt organ, överförs till den datasamordnare som avses i artikel 37 i den medlemsstat där det begärande offentliga organet är etablerat, som utan oskäligt dröjsmål ska offentliggöra begäran på nätet såvida datasamordnaren inte anser att sådant offentliggörande skulle utgöra en risk för den allmänna säkerheten,
- h) om begäran görs av kommissionen, Europeiska centralbanken eller ett unionsorgan, utan oskäligt dröjsmål göras tillgänglig på nätet,
- i) om personuppgifter begärs, utan oskäligt dröjsmål anmälas till den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 i den medlemsstat där det offentliga organet är etablerat.

Europeiska centralbanken och unionsorgan ska underrätta kommissionen om sina begäranden.

3. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan får inte göra data som erhållits enligt detta kapitel tillgängliga för vidareutnyttjande enligt definitionen i artikel 2.2 i förordning (EU) 2022/868 eller artikel 2.11 i direktiv (EU) 2019/1024. Förordning (EU) 2022/868 och direktiv (EU) 2019/1024 ska inte tillämpas på data som innehas av offentliga organ och som erhållits enligt detta kapitel.

4. Punkt 3 i denna artikel hindrar inte ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan från att utbyta data som erhållits enligt detta kapitel med andra offentliga organ eller kommissionen, Europeiska centralbanken eller unionsorgan, i syfte att fullgöra de uppgifter som avses i artikel 15, enligt vad som anges i begäran i enlighet med punkt 1 f i den här artikeln, eller att göra dessa data tillgängliga för en tredje part om den/det genom ett offentligt tillgängligt avtal har delegerat tekniska inspektioner eller andra funktioner till denna tredje part. Skyldigheterna för offentliga organ enligt artikel 19, särskilt skyddsåtgärder för att bevara konfidentialiteten för företagshemligheter, ska även tillämpas på sådana tredje parter. Om ett offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan överför eller tillgängliggör data enligt den här punkten ska det eller den utan oskäligt dröjsmål underrätta den datahållare från vilken dessa data mottogs.
5. Om datahållaren anser att dess rättigheter enligt detta kapitel har kränkts genom överföringen eller tillgängliggörandet av data, får denne lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.
6. Kommissionen ska utarbeta en mall för begäranden enligt denna artikel.

Artikel 18

Tillmötesgående av begäran om data

1. En datahållare som mottar en begäran om att göra data tillgängliga enligt detta kapitel ska utan oskäligt dröjsmål göra dessa data tillgängliga för det begärande offentliga organet, kommissionen, Europeiska centralbanken eller ett unionsorgan, med beaktande av nödvändiga tekniska, organisatoriska och rättsliga åtgärder.
2. Utan att det påverkar de särskilda behov vad gäller tillgänglighet av data som fastställs i unionsrätten eller nationell rätt får en datahållare avslå eller ansöka om ändring av en begäran om att göra data tillgängliga enligt detta kapitel utan oskäligt dröjsmål och under alla omständigheter senast fem arbetsdagar efter mottagandet av en begäran om data som är nödvändiga för att hantera ett allmänt nödläge och utan oskäligt dröjsmål och, under alla omständigheter, senast 30 arbetsdagar efter mottagandet av en sådan begäran i andra fall av exceptionellt behov, av något av följande skäl:
 - a) Datahållaren har inte kontroll över de data som begärs.
 - b) En liknande begäran för samma ändamål har tidigare lämnats in av ett annat offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan, och datahållaren har inte underrättats om att dessa data har raderats enligt artikel 19.1 c.
 - c) Begäran uppfyller inte villkoren i artikel 17.1 och 17.2.

3. Om datahållaren beslutar sig för att avslå begäran eller ansöka om ändring av den i enlighet med punkt 2 b, ska denne ange identiteten på det offentliga organ eller kommissionen eller Europeiska centralbanken eller det unionsorgan som tidigare lämnat in en begäran för samma ändamål.
4. Om de data som begärs innehåller personuppgifter ska datahållaren anonymisera personuppgifterna på korrekt sätt, såvida det inte för att tillmötesgå begäran om att göra data tillgängliga för ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan krävs att personuppgifterna lämnas ut. I sådana fall ska datahållaren pseudonymisera personuppgifterna.
5. Om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet vill överklaga en datahållares vägran att tillhandahålla begärda data eller om datahållaren vill bestrida begäran och ärendet inte kan lösas genom en lämplig ändring av begäran, ska ärendet hänskjutas till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 19

Skyldigheter för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som tar emot data till följd av en begäran enligt artikel 14 ska
 - a) inte använda dessa data på ett sätt som är oförenligt med det ändamål för vilket de begärdes,

- b) ha genomfört tekniska och organisatoriska åtgärder som bevarar konfidentialiteten och integriteten avseende de data som begärs och säkerheten vid överföring av data, särskilt personuppgifter, och som skyddar de registrerades rättigheter och friheter,
- c) radera dessa data så snart de inte längre är nödvändiga för det angivna ändamålet och utan oskäligt dröjsmål informera datahållaren och enskilda personer eller organisationer som har tagit emot data enligt artikel 21.1 om att de har raderats, såvida det inte krävs att dessa data arkiveras i enlighet med unionsrätt eller nationell rätt om allmänhetens tillgång till handlingar i samband med insynsskyldigheter.

2. Ett offentligt organ, kommissionen, Europeiska centralbanken, ett unionsorgan eller en tredje part som tar emot data enligt detta kapitel får inte

- a) använda data eller insikter om datahållarens ekonomiska situation, tillgångar och produktions- eller driftsmetoder för att utveckla eller förbättra en uppkopplad produkt eller tillhörande tjänst som konkurrerar med datahållarens uppkopplade produkt eller tillhörande tjänst,
- b) dela dessa data med en annan tredje part för något av de ändamål som avses i led a.

3. Röjande av företagshemligheter till ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska endast krävas i den mån det är absolut nödvändigt för att uppnå syftet med en begäran enligt artikel 15. I sådana fall ska datahållaren eller, om det inte rör sig om samma person, innehavaren av en företagshemlighet identifiera de data som skyddas som företagshemligheter, inbegripet relevanta metadata. Det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska före röjandet av företagshemligheter vidta alla nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att bevara konfidentialiteten för företagshemligheterna, när så är lämpligt även användning av standardavtalsvillkor och tekniska standarder samt tillämpning av uppförandekoder.
4. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ansvara för säkerheten för de data som de tar emot.

Artikel 20

Ersättning vid situationer då det föreligger ett exceptionellt behov

1. Andra datahållare än mikroföretag och små företag ska kostnadsfritt tillgängliggöra de data som är nödvändiga för att hantera ett allmänt nödläge enligt artikel 15.1 a. Det offentliga organ, kommissionen, Europeiska centralbanken eller det unionsorgan som har tagit emot dessa data ska ge datahållaren offentligt erkännande på begäran av datahållaren.

2. Datahållaren ska ha rätt till skälig ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15.1 b. Sådan ersättning ska täcka de tekniska och organisatoriska kostnader som uppstår till följd av tillmötesgåendet av begäran, inbegripet, vid behov, kostnaderna för anonymisering, pseudonymisering, aggregering och teknisk anpassning, och en rimlig marginal. På begäran av det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska datahållaren tillhandahålla information om underlaget till kostnadsberäkningen och den rimliga marginalen.
3. Punkt 2 ska också vara tillämplig om mikroföretag och små företag begär ersättning för att göra data tillgängliga.
4. Datahållare ska inte ha rätt till ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15.1 b, om den specifika uppgiften av allmänt intresse är framställning av officiell statistik och om inköp av data inte är tillåten enligt nationell rätt. Medlemsstaterna ska underrätta kommissionen om inköp av data för framställning av officiell statistik inte är tillåtet enligt nationell rätt.
5. Om det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inte godtar den ersättningsnivå som datahållaren begär, får det eller den lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 21

Delning av data som erhållits i samband med ett exceptionellt behov med forskningsorganisationer eller statistikorgan

1. Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska ha rätt att dela data som mottagits enligt detta kapitel
 - a) med enskilda personer eller organisationer i syfte att bedriva vetenskaplig forskning eller analys som är förenlig med det ändamål för vilket data begärdes, eller
 - b) med nationella statistikbyråer och Eurostat för framställning av officiell statistik.
2. Enskilda personer eller organisationer som tar emot data enligt punkt 1 ska agera utan vinstsyfte eller inom ramen för ett uppdrag av allmänt intresse som erkänns i unionsrätten eller nationell rätt. Detta omfattar inte organisationer på vilka kommersiella företag har ett betydande inflytande som sannolikt skulle kunna leda till förmånstillträde till forskningsresultaten.
3. Enskilda personer eller organisationer som tar emot data enligt punkt 1 i denna artikel ska fullgöra samma skyldigheter som dem som är tillämpliga på offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan enligt artiklarna 17.3 och 19.

4. Trots vad som anges i artikel 19.1 c får enskilda personer eller organisationer som tar emot data enligt punkt 1 i den här artikeln behålla de data som mottagits för det ändamål för vilket data begärdes i upp till sex månader efter det att dessa data har raderats av de offentliga organen, kommissionen, Europeiska centralbanken och unionsorgan.
5. Om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan har för avsikt att överföra eller tillgängliggöra data enligt punkt 1 i denna artikel ska det eller den utan oskäligt dröjsmål underrätta den datahållare från vilken dessa data mottogs samt uppgge identitet och kontaktuppgifter för den organisation eller enskilda person som tar emot data, ändamålet med överföringen eller tillgängliggörandet av data, den period under vilken data ska användas och de tekniska skyddsåtgärder och organisatoriska åtgärder som har vidtagits för att skydda dessa data, även om det rör sig om personuppgifter eller företagshemligheter. Om datahållaren inte godtar överföringen eller tillgängliggörandet av data, får denne lämna in ett klagomål till den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.

Artikel 22

Ömsesidigt bistånd och gränsöverskridande samarbete

1. Offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan ska samarbeta och bistå varandra för att genomföra detta kapitel på ett konsekvent sätt.
2. Data som utbyts i samband med begärt bistånd och som tillhandahållits enligt punkt 1 får inte användas på ett sätt som är oförenligt med det ändamål för vilket de begärdes.

3. Om ett offentligt organ avser att begära data från en datahållare som är etablerad i en annan medlemsstat, ska den först underrätta den behöriga myndighet som utsetts enligt artikel 37 i den medlemsstaten om den avsikten. Detta krav ska även gälla för begäranden från kommissionen, Europeiska centralbanken och unionsorgan. Begäran ska granskas av den behöriga myndigheten i den medlemsstat där datahållaren är etablerad.
4. Efter att ha granskat begäran mot bakgrund av kraven enligt artikel 17, ska den relevanta behöriga myndigheten utan oskäligt dröjsmål vidta en av följande åtgärder:
 - a) Överföra begäran till datahållaren och i tillämpliga fall ge det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet råd om det eventuella behovet av att samarbeta med offentliga organ i den medlemsstat där datahållaren är etablerad, i syfte att minska den administrativa bördan för datahållaren när det gäller att tillmötesgå begäran.
 - b) Avslå begäran av vederbörligen motiverade skäl i enlighet med detta kapitel.

Det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska beakta råden från och de skäl som anges av den relevanta behöriga myndigheten enligt första stycket innan ytterligare åtgärder vidtas, såsom en inlämning på nytt av begäran, i tillämpliga fall.

Kapitel VI

Byte av databehandlingstjänster

Artikel 23

Undanröjande av hinder för ett effektivt byte

Leverantörer av databehandlingstjänster ska vidta de åtgärder som föreskrivs i artiklarna 25, 26, 27, 29 och 30 för att göra det möjligt för kunder att byta till en databehandlingstjänst som omfattar samma tjänstetyp och som tillhandahålls av en annan leverantör av databehandlingstjänster, eller till lokal IKT-infrastruktur, eller, i förekommande fall, att använda flera leverantörer av databehandlingstjänster samtidigt. I synnerhet ska leverantörer av databehandlingstjänster inte införa utan i stället undanröja förkommersiella, kommersiella, tekniska, avtalsmässiga och organisatoriska hinder som hindrar kunderna från att

- a) säga upp avtalet om databehandlingstjänsten efter den maximala uppsägningstiden och efter det att bytesprocessen har slutförts med framgång, i enlighet med artikel 25,
- b) ingå nya avtal med en annan leverantör av databehandlingstjänster som täcker samma tjänstetyp,

- c) portera kundens exporterbara data och digitala tillgångar till en annan leverantör av databehandlingstjänster eller till en lokal IKT-infrastruktur, även efter att ha utnyttjat ett gratiserbjudande,
- d) i enlighet med artikel 24 uppnå funktionell likvärdighet i användningen av den nya databehandlingstjänsten i IKT-miljön hos en annan leverantör av databehandlingstjänster som omfattar samma tjänstetyp,
- e) om det är tekniskt möjligt separera de databehandlingstjänster som avses i artikel 30.1 från andra databehandlingstjänster som tillhandahålls av leverantören av databehandlingstjänster.

Artikel 24

Tillämpningsområdet för de tekniska skyldigheterna

Ansvaret för leverantörer av databehandlingstjänster enligt artiklarna 23, 25, 29, 30 och 34 ska endast gälla de tjänster, avtal eller affärsmetoder som tillhandahålls av den ursprungliga leverantören av databehandlingstjänster.

Artikel 25
Avtalsvillkor om byte

1. Kundens rättigheter och leverantörens skyldigheter vad gäller ett byte av leverantör av databehandlingstjänster eller, i tillämpliga fall, till en lokal IKT-infrastruktur ska tydligt anges i ett skriftligt avtal. Leverantören av databehandlingstjänster ska göra detta avtal tillgängligt för kunden före undertecknandet av avtalet på ett sätt som gör det möjligt för kunden att lagra och återge avtalet.
2. Utan att det påverkar tillämpningen av direktiv (EU) 2019/770 ska det avtal som avses i punkt 1 i denna artikel innehålla åtminstone följande:
 - a) Villkor som gör det möjligt för kunden att på begäran byta till en databehandlingstjänst som erbjuds av en annan leverantör av databehandlingstjänster eller att portera alla exporterbara data och digitala tillgångar till en lokal IKT-infrastruktur, utan oskäligt dröjsmål och under alla omständigheter senast efter den maximala övergångsperioden på 30 kalenderdagar, som ska inledas efter den maximala uppsägningstid som avses i led d, under vilken tjänsteavtalet fortfarande är tillämpligt och under vilken leverantören av databehandlingstjänster ska
 - i) ge kunden och tredje parter som kunden har godkänt rimligt bistånd i bytesprocessen,

- ii) iaktta vederbörlig omsorg för att upprätthålla driftskontinuitet och fortsätta att tillhandahålla funktioner eller tjänster enligt avtalet,
 - iii) tillhandahålla tydlig information om kända risker för kontinuiteten i tillhandahållandet av funktioner eller tjänster från den ursprungliga leverantören av databehandlingstjänster,
 - iv) säkerställa att en hög säkerhetsnivå upprätthålls under hela bytesprocessen, särskilt säkerheten för data under överföringen och den fortsatta säkerheten för dessa data under den period för datahämtning som avses i led g, i enlighet med tillämplig unionsrätt eller nationell rätt.
- b) En skyldighet för leverantören av databehandlingstjänster att stödja den utträdesstrategi för kunden som är relevant för de avtalade tjänsterna, bland annat genom att tillhandahålla all relevant information.
- c) Ett villkor som anger att avtalet ska anses vara uppsagt och att kunden ska underrättas om detta i något av följande fall:
- i) I tillämpliga fall, efter ett framgångsrikt slutförande av bytesprocessen.
 - ii) Vid utgången av den maximala uppsägningstid som avses i led d, om kunden inte vill byta utan radera sina exporterbara data och digitala tillgångar när tjänsten upphör.
- d) En maximal uppsägningstid för inledande av bytesprocessen, som inte får överstiga två månader.

- e) En uttömmande specifikation av alla kategorier av data och digitala tillgångar som kan porteras under bytesprocessen, inklusive åtminstone alla exporterbara data.
- f) En uttömmande specifikation av alla kategorier av data som är specifika för att leverantörens databehandlingstjänsten ska fungera internt och som ska undantas från de exporterbara data enligt led e om det finns en risk för överträdelse med avseende på leverantörens företagshemligheter, förutsatt att sådana undantag inte hindrar eller försenar den bytesprocess som föreskrivs i artikel 23.
- g) En minimiperiod för datahämtning på minst 30 kalenderdagar, med början efter det att den övergångsperiod som överenskommits mellan kunden och leverantören av databehandlingstjänster har löpt ut, i enlighet med led a i denna punkt och punkt 4.
- h) Ett villkor som säkerställer fullständig radering av alla exporterbara data och digitala tillgångar som genereras direkt av kunden eller som direkt berör kunden, efter utgången av den period för datahämtning som avses i led g eller efter utgången av en alternativ överenskommen period vid en senare tidpunkt än den dag då den period för datahämtning som avses i led g löper ut, förutsatt att bytesprocessen har slutförts med framgång.
- i) Bytesavgifter som får införas av leverantörer av databehandlingstjänster i enlighet med artikel 29.

3. Det avtal som avses i punkt 1 ska innehålla klausuler enligt vilka kunden får underrätta leverantören av databehandlingstjänster om sitt beslut att vidta en eller flera av följande åtgärder när den maximala uppsägningstid som avses i punkt 2 d löper ut:
 - a) Byta till en annan leverantör av databehandlingstjänster; kunden ska i så fall tillhandahålla nödvändiga uppgifter om den leverantören.
 - b) Byta till en lokal IKT-infrastruktur.
 - c) Radera sina exporterbara data och digitala tillgångar.
4. Om den obligatoriska maximala övergångsperiod som föreskrivs i punkt 2 a är tekniskt ogenomförbar ska leverantören av databehandlingstjänster underrätta kunden inom 14 arbetsdagar efter det att begäran om byte gjorts och vederbörligen motivera varför det är tekniskt ogenomförbart samt ange en alternativ övergångsperiod, som inte får överstiga sju månader. I enlighet med punkt 1 ska driftskontinuitet säkerställas under hela den alternativa övergångsperiod.
5. Utan att det påverkar tillämpningen av punkt 4 ska det avtal som avses i punkt 1 innehålla klausuler som ger kunden rätt att förlänga övergångsperioden en gång med en tidsperiod som kunden anser lämpligare för sina egna ändamål.

Artikel 26

Informationsskyldighet för leverantörer av databehandlingstjänster

Leverantören av databehandlingstjänster ska förse kunden med

- a) information om tillgängliga förfaranden för byte och portering till databehandlingstjänsten, inbegripet information om tillgängliga metoder och format för byten och portering samt tekniska och andra begränsningar som leverantören av databehandlingstjänster känner till,
- b) en hänvisning till ett uppdaterat onlineregister som sköts av leverantören av databehandlingstjänster, med uppgifter om alla datastrukturer och dataformat samt relevanta standarder och öppna interoperabilitetsspecifikationer i vilka de exporterbara data som avses i artikel 25.2 e är tillgängliga.

Artikel 27

Skyldighet att handla i god tro

Alla berörda parter, inbegripet destinationsleverantörer av databehandlingstjänster, ska samarbeta i god tro för att göra bytesprocessen effektiv, möjliggöra snabb överföring av data och bibehålla databehandlingstjänstens kontinuitet.

Artikel 28

Avtalsenliga insynsskyldigheter i fråga om internationell åtkomst och överföring

1. Leverantörer av databehandlingstjänster ska göra följande information tillgänglig på sina webbplatser och hålla den informationen uppdaterad:
 - a) Vilken jurisdiktion som den IKT-infrastruktur som används för databehandling av deras enskilda tjänster tillhör.
 - b) En allmän beskrivning av de tekniska, organisatoriska och avtalsmässiga åtgärder som leverantören av databehandlingstjänster vidtagit för att förhindra internationell statlig åtkomst till eller överföring av icke-personuppgifter som innehas i unionen, om en sådan åtkomst eller överföring skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt.
2. De webbplatser som avses i punkt 1 ska förtecknas i avtal för alla databehandlingstjänster som erbjuds av leverantörer av databehandlingstjänster.

Artikel 29

Gradvist avskaffande av bytesavgifter

1. Från och med den ... [tre år från den dag då denna förordning träder i kraft] ska leverantörer av databehandlingstjänster inte ta ut några bytesavgifter av kunden för bytesprocessen.

2. Från och med den ... [den dag då denna förordning träder i kraft] till och med den ... [tre år från den dag då denna förordning träder i kraft] får leverantörer av databehandlingstjänster ta ut nedsatta bytesavgifter av kunden för bytesprocessen.
3. De nedsatta bytesavgifter som avses i punkt 2 får inte överstiga de kostnader som är direkt kopplade till den berörda bytesprocessen som uppstår för leverantören av databehandlingstjänster.
4. Innan leverantörer av databehandlingstjänster ingår avtal med en kund ska de förse den potentiella kunden med tydlig information om vilka standardavgifter och straffavgifter för förtida uppsägning som kan komma att utkrävas, samt om de nedsatta bytesavgifterna som kan komma att utkrävas under den tidsperiod som avses i punkt 2.
5. I förekommande fall ska leverantörer av databehandlingstjänster tillhandahålla information till en kund om databehandlingstjänster som inbegriper mycket komplexa eller kostsamma byten eller för vilka det är omöjligt att byta utan betydande störningar i data, digitala tillgångar eller tjänstearkitektur.
6. I tillämpliga fall ska leverantörerna av databehandlingstjänster göra den information som avses i punkterna 4 och 5 allmänt tillgänglig för kunderna via en särskild del av sin webbplats eller på något annat lättillgängligt sätt.

7. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 med avseende på att komplettera denna förordning genom att inrätta en övervakningsmekanism som låter kommissionen övervaka de bytesavgifter som tas ut av leverantörer av databehandlingstjänster på marknaden för att säkerställa att avskaffandet och nedsättningen av bytesavgifter enligt punkterna 1 och 2 i den här artikeln kommer att genomföras i enlighet med de tidsfrister som föreskrivs i de punkterna.

Artikel 30

Tekniska aspekter av byte

1. Leverantörer av databehandlingstjänster som avser skalbara och elastiska datorresurser begränsade till infrastrukturella element såsom servrar, nät och de virtuella resurser som krävs för driften av infrastrukturen, men som inte ger åtkomst till de operativa tjänster, den programvara och de applikationer som lagras, på annat sätt behandlas eller används på dessa infrastrukturkomponenter ska, i enlighet med artikel 27, vidta alla rimliga åtgärder som står i deras makt för att underlätta för kunden att, efter att denna har bytt till en tjänst som omfattar samma tjänstetyp, uppnå funktionell likvärdighet vid användningen av den destinationstjänsten för databehandling. Den ursprungliga leverantören av databehandlingstjänster ska underlätta bytesprocessen genom att tillhandahålla kapacitet, adekvat information, dokumentation, tekniskt stöd och, vid behov, nödvändiga verktyg.

2. Andra leverantörer av databehandlingstjänster än de som avses i punkt 1 ska göra öppna gränssnitt tillgängliga i samma utsträckning för alla sina kunder och de berörda destinationsleverantörerna av databehandlingstjänster och kostnadsfritt i syfte att underlätta bytesprocessen. Dessa gränssnitt ska innehålla tillräcklig information om den berörda tjänsten för att möjliggöra utveckling av programvara för kommunikation med tjänsterna, i syfte att åstadkomma dataportabilitet och interoperabilitet.
3. För andra databehandlingstjänster än de som avses i punkt 1 i denna artikel ska leverantörer av databehandlingstjänster säkerställa kompatibilitet med gemensamma specifikationer som bygger på öppna interoperabilitetsspecifikationer eller harmoniserade standarder för interoperabilitet minst tolv månader efter det att hänvisningarna till dessa gemensamma specifikationer eller harmoniserade standarder för interoperabla databehandlingstjänster offentliggjordes i det centrala unionsregistret över standarder för interoperabla databehandlingstjänster efter offentliggörandet av de underliggande genomförandeakterna i *Europeiska unionens officiella tidning* i enlighet med artikel 35.8.
4. Andra leverantörer av databehandlingstjänster än de som avses i punkt 1 i denna artikel ska uppdatera det onlineregister som avses i artikel 26 b i enlighet med sina skyldigheter enligt punkt 3 i den här artikeln.

5. Vid byten mellan tjänster av samma tjänstetyp, för vilka gemensamma specifikationer eller harmoniserade standarder för interoperabla databehandlingstjänster som avses i punkt 3 i denna artikel inte har offentliggjorts i det centrala unionsregistret över standarder för interoperabla databehandlingstjänster i enlighet med artikel 35.8, ska leverantören av databehandlingstjänsterna på kundens begäran exportera alla exporterbara data i ett strukturerat, allmänt använt och maskinläsbart format.
6. Leverantörer av databehandlingstjänster ska inte vara skyldiga att utveckla ny teknik eller nya tjänster, eller att röja eller överföra digitala tillgångar som skyddas genom immateriella rättigheter eller utgör en företagshemlighet till en kund eller en annan leverantör av databehandlingstjänster eller att äventyra kundens eller leverantörens driftssäkerhet och driftintegritet.

Artikel 31

Särskild ordning för vissa databehandlingstjänster

1. De skyldigheter som fastställs i artiklarna 23 d, 29, 30.1 och 30.3 ska inte tillämpas på databehandlingstjänster där de flesta huvudfunktioner har skräddarsyttts för att tillgodose en enskild kunds särskilda behov eller där alla komponenter har utvecklats för en enskild kunds räkning, och om dessa databehandlingstjänster inte erbjuds i stor kommersiell skala via tjänstekatalogen hos leverantören av databehandlingstjänster.

2. De skyldigheter som fastställs i detta kapitel ska inte tillämpas på databehandlingstjänster som tillhandahålls som en icke-produktionsversion för testnings- och utvärderingsändamål och under en begränsad tidsperiod.
3. Innan ett avtal om tillhandahållande av de databehandlingstjänster som avses i denna artikel ingås ska leverantören av databehandlingstjänster informera den potentiella kunden om vilka skyldigheter i detta kapitel som inte är tillämpliga.

Kapitel VII

Olaglig internationell statlig åtkomst till och överföring av icke-personuppgifter

Artikel 32

Internationell statlig åtkomst och överföring

1. Leverantörer av databehandlingstjänster ska vidta alla adekvata tekniska, organisatoriska och rättsliga åtgärder, inbegripet avtal, för att förhindra internationell statlig åtkomst och tredjeländers statliga åtkomst till och överföring av icke-personuppgifter som innehas i unionen, om en sådan överföring eller åtkomst skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt, utan att det påverkar tillämpningen av punkt 2 eller 3.

2. Beslut eller domar från en domstol i ett tredjeland och beslut från en administrativ myndighet i ett tredjeland där det krävs att en leverantör av databehandlingstjänster överför eller ger åtkomst till icke-personuppgifter som omfattas av denna förordning och som innehas i unionen ska endast erkännas eller genomföras på något som helst sätt om de grundar sig på en internationell överenskommelse, såsom ett fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, eller ett sådant avtal mellan det begärande tredjelandet och en medlemsstat.
3. I de fall då, i avsaknad av en internationell överenskommelse som avses i punkt 2, en leverantör av databehandlingstjänster är adressat för ett beslut eller en dom från en domstol i ett tredjeland eller ett beslut från en administrativ myndighet i ett tredjeland om att överföra eller ge åtkomst till icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning och som innehas i unionen, och efterlevnaden av ett sådant beslut skulle riskera att medföra att adressaten bryter mot unionsrätten eller den berörda medlemsstatens nationella rätt, ska tredjelandsmyndigheten motta eller få åtkomst till sådana data endast om
 - a) tredjelandets system kräver att skälen till ett sådant beslut och beslutets proportionalitet ska fastställas och föreskriver att beslutet eller domen är av specifik art, exempelvis genom att det fastställs en tillräckligt stark koppling till vissa misstänkta personer eller till överträdelser,
 - b) adressatens motiverade invändning är föremål för en granskning av en behörig domstol i tredjelandet, och

- c) den behöriga domstol i tredjelandet som utfärdar beslutet eller domen eller granskar en administrativ myndighets beslut enligt det tredjelandets rätt har befogenhet att ta vederbörlig hänsyn till de relevanta rättsliga intressena för leverantören av de data som skyddas av unionsrätten eller den berörda medlemsstatens nationella rätt.

Beslutets eller domens adressat får begära ett yttrande från det relevanta nationella organ eller den relevanta nationella myndighet som har behörighet för internationellt samarbete i rättsliga frågor, för att avgöra om de villkor som anges i första stycket är uppfyllda, särskilt när den anser att beslutet kan avse företagshemligheter och andra kommersiellt känsliga data samt innehåll som skyddas av immateriella rättigheter eller att överföringen kan leda till återidentifiering. Det relevanta nationella organet eller den relevanta nationella myndigheten får samråda med kommissionen. Om adressaten anser att beslutet eller domen kan inkräkta på unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen ska den begära ett yttrande från det relevanta nationella organet eller den relevanta nationella myndigheten för att avgöra om begärda data rör unionens eller dess medlemsstaters nationella säkerhets- eller försvarsintressen. Om adressaten inte har fått något svar inom en månad, eller om yttrandet av ett sådant organ eller en sådan myndighet visar att de villkor som anges i första stycket inte är uppfyllda, får adressaten avslå begäran om överföring eller åtkomst till icke-personuppgifter av dessa skäl.

Europeiska datainnovationsstyrelsen, som avses i artikel 42, ska ge råd till och bistå kommissionen vid utarbetandet av riktlinjer för bedömningen av huruvida de villkor som avses i första stycket i denna punkt är uppfyllda.

4. Om de villkor som fastställs i punkt 2 eller 3 är uppfyllda ska leverantören av databehandlingstjänster tillhandahålla den minsta mängd data som är tillåten som svar på en begäran, på grundval av en rimlig tolkning av den begäran av den leverantör, det relevanta nationella behöriga organ eller den relevanta behöriga nationella myndighet som avses i punkt 3 andra stycket.
5. Leverantören av databehandlingstjänster ska informera kunden om att det finns en begäran från en myndighet i ett tredjeland om att få åtkomst till dess data innan leverantören tillmötesgår den begäran, utom när begäran tjänar brottsbekämpande ändamål och så länge som detta är nödvändigt för att upprätthålla den brottsbekämpande verksamhetens effektivitet.

Kapitel VIII

Interoperabilitet

Artikel 33

Väsentliga krav med avseende på interoperabilitet för data, datadelningsmekanismer och datadelningstjänster samt gemensamma europeiska dataområden

1. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare ska uppfylla följande väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden, som är ändamåls- eller sektorsspecifika eller sektoröverskridande interoperabla ramar för gemensamma standarder och praxisformer för delning eller gemensam behandling av data för bland annat utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ:
 - a) Innehåll i datamängden, användningsbegränsningar, licenser, datainsamlingsmetoder, datakvalitet och osäkerhet i data ska beskrivas tillräckligt, när så är tillämpligt, i ett maskinläsbart format, för att mottagaren ska kunna hitta, få åtkomst till och använda data.
 - b) Datastrukturer, dataformat, vokabulärer, klassificeringssystem, taxonomier och kodförteckningar ska, om sådana finns tillgängliga, beskrivas på ett allmänt tillgängligt och konsekvent sätt.

- c) De tekniska medlen för åtkomst till data, såsom programmeringsgränssnitt, och deras användningsvillkor och tjänstekvalitet ska vara tillräckligt beskrivna för att möjliggöra automatisk åtkomst och överföring av data mellan parter, även kontinuerligt, genom bulknedladdning eller i realtid i ett maskinläsbart format, om detta är tekniskt möjligt och inte hindrar den uppkopplade produktens funktionsduglighet.
- d) De medel som krävs för att möjliggöra interoperabilitet för verktyg för automatiserat genomförande av datadelningsavtal, såsom smarta kontrakt, ska i tillämpliga fall tillhandahållas.

Kraven kan vara av allmän karaktär eller avse specifika sektorer, samtidigt som sambandet med krav som härrör från annan unionsrätt eller nationell rätt beaktas fullt ut.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 i denna förordning med avseende på att komplettera denna förordning genom att ytterligare specificera de väsentliga krav som fastställs i punkt 1 i den här artikeln, med avseende på de krav som till sin natur inte kan ge den avsedda effekten om de inte specificeras närmare i bindande unionsrättsakter och för att korrekt återspegla den tekniska utvecklingen och marknadsutvecklingen.

Kommissionen ska, när den antar delegerade akter, beakta råd från Europeiska datainnovationsstyrelsen i enlighet med artikel 42 c iii.

3. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare i dataområden som uppfyller de harmoniserade standarder eller delar av dem vars hänvisningar är offentliggjorda i *Europeiska unionens officiella tidning* ska förutsättas uppfylla de väsentliga krav som fastställs i punkt 1, i den mån dessa krav omfattas av sådana harmoniserade standarder eller delar av dem.
4. Kommissionen ska enligt artikel 10 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln.
5. Kommissionen får genom genomförandeakter anta gemensamma specifikationer som omfattar något av eller alla de väsentliga krav som fastställs i punkt 1 om följande villkor är uppfyllda:
 - a) Kommissionen har enligt artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln, och
 - i) begäran har inte accepterats,
 - ii) de harmoniserade standarder som avser denna begäran har inte levererats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller
 - iii) de harmoniserade standarderna uppfyller inte begäran, och

- b) ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga krav som fastställs i punkt 1 i denna artikel är offentliggjord i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

6. Innan kommissionen utarbetar ett utkast till genomförandeakt som avses i punkt 5 i denna artikel ska den underrätta den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 5 i den här artikeln är uppfyllda.
7. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 5 ska kommissionen beakta råd från Europeiska datainnovationsstyrelsen och synpunkter från andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.
8. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare i dataområden som uppfyller de gemensamma specifikationer som fastställs genom genomförandeakter som avses i punkt 5 eller delar av dem ska förutsättas överensstämja med de väsentliga krav som fastställs i punkt 1 i den mån dessa krav omfattas av sådana gemensamma specifikationer eller delar av dem.

9. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 5 i denna artikel, eller delar av dem som omfattar samma väsentliga krav som omfattas av den harmoniserade standarden.
10. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkt 1 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.
11. Kommissionen får anta riktlinjer med beaktande av förslaget från Europeiska datainnovationsstyrelsen i enlighet med artikel 30 h i förordning (EU) 2022/868 om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion.

Artikel 34

Interoperabilitet för parallell användning av databehandlingstjänster

1. Kraven i artiklarna 23, 24, 25.2 a ii, 25.2 a iv, 25.2 e, 25.2 f och 30.2–30.5 ska också gälla i tillämpliga delar för leverantörer av databehandlingstjänster för att underlätta interoperabilitet för parallell användning av databehandlingstjänster.
2. När en databehandlingstjänst används parallellt med en annan databehandlingstjänst, får leverantörerna av databehandlingstjänster påföra uttagsavgifter för data, men endast i syfte att vidareföra de kostnader som uppkommit, utan att överskrida dessa kostnader.

Artikel 35

Interoperabilitet för databehandlingstjänster

1. Öppna interoperabilitetsspecifikationer och harmoniserade standarder för interoperabla databehandlingstjänster ska
 - a) om det är tekniskt möjligt åstadkomma interoperabilitet mellan olika databehandlingstjänster som omfattar samma tjänstetyp,
 - b) förbättra portabiliteten för digitala tillgångar mellan olika databehandlingstjänster som omfattar samma tjänstetyp,
 - c) om det är tekniskt möjligt underlätta funktionell likvärdighet mellan olika sådana databehandlingstjänster som avses i artikel 30.1 som omfattar samma tjänstetyp,

- d) inte inverka negativt på säkerhet och integritet för databehandlingstjänster och data,
 - e) vara utformade på ett sådant sätt att det möjliggör tekniska framsteg och införande av nya funktioner och innovation inom databehandlingstjänster.
2. Öppna interoperabilitetsspecifikationer och harmoniserade standarder för interoperabla databehandlingstjänster ska på ett adekvat sätt hantera
- a) aspekterna av interoperabilitet i molnet när det gäller transportinteroperabilitet, syntaktisk interoperabilitet, semantisk datainteroperabilitet, beteendeinteroperabilitet och policyinteroperabilitet,
 - b) aspekterna av dataportabilitet i molnet vad gäller syntaktisk dataportabilitet, semantisk dataportabilitet och portabilitet för datapolicy,
 - c) aspekterna av applikationer i molnet vad gäller syntaktisk applikationsportabilitet, applikationsportabilitet för instruktioner, applikationsportabilitet för metadata, applikationsportabilitet för beteende och applikationsportabilitet för policy.
3. De öppna interoperabilitetsspecifikationerna ska uppfylla kraven i bilaga II till förordning (EU) nr 1025/2012.

4. Efter att ha beaktat relevanta internationella och europeiska standarder och självregleringsinitiativ får kommissionen i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkterna 1 och 2 i den här artikeln.
5. Kommissionen får genom genomförandeakter anta gemensamma specifikationer på grundval av öppna interoperabilitetsspecifikationer som omfattar alla de väsentliga krav som fastställs i punkterna 1 och 2.
6. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 5 i denna artikel ska kommissionen beakta synpunkterna från de relevanta behöriga myndigheter som avses i artikel 37.5 h och andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.
7. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkterna 1 och 2 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.
8. Vid tillämpning av artikel 30.3 ska kommissionen genom genomförandeakter offentliggöra hänvisningar till harmoniserade standarder och gemensamma specifikationer för interoperabla databehandlingstjänster i ett centralt unionsregister över standarder för interoperabla databehandlingstjänster.

9. De genomförandeakter som avses i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

Artikel 36

Väsentliga krav avseende smarta kontrakt för genomförande av datadelningsavtal

1. Säljaren av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data ska säkerställa att dessa smarta kontrakt efterlever följande väsentliga krav:
- a) Robusthet och åtkomstkontroll: Säkerställa att det smarta kontraktet har utformats för att erbjuda åtkomstkontrollmekanismer och en mycket hög grad av robusthet för att undvika funktionsfel och stå emot manipulering från tredje parter sida.
 - b) Säkerhet vid uppsägning och avbrott: Säkerställa att det finns en mekanism för att avsluta det fortsatta genomförandet av transaktioner och att det smarta kontraktet omfattar interna funktioner som kan återställa eller instruera kontraktet att permanent eller tillfälligt avbryta driften, i synnerhet för att undvika framtida oavsiktliga exekveringar.
 - c) Dataarkivering och kontinuitet: Säkerställa, under omständigheter då ett smart kontrakt måste avslutas eller avaktiveras, att det finns en möjlighet att arkivera transaktionsuppgifterna, smart avtalslogik och kod för att föra register över tidigare utförda transaktioner (granskningsbarhet).

- d) Åtkomstkontroll: Säkerställa att ett smart kontrakt skyddas genom strikta mekanismer för åtkomstkontroll vid skikten för kontroll och smarta kontrakt.
 - e) Enhetlighet: Säkerställa enhetlighet med villkoren i det datadelningsavtal som det smarta kontraktet genomför.
2. Säljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data ska utföra en bedömning av överensstämmelse i syfte att uppfylla de väsentliga krav som fastställs i punkt 1 och, när dessa krav är uppfyllda, utfärda en EU-försäkran om överensstämmelse.
3. Genom att utarbeta en EU-försäkran om överensstämmelse ska försäljaren av en applikation som använder smarta kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data vara ansvarig för efterlevnaden av de väsentliga krav som fastställs i punkt 1.
4. Ett smart kontrakt som uppfyller de harmoniserade standarder eller de relevanta delarna av dessa standarder och vars hänvisningar är offentliggjorda i *Europeiska unionens officiella tidning* ska förutsättas uppfylla de väsentliga krav som fastställs i punkt 1, i den mån dessa krav omfattas av sådana harmoniserade standarder eller delar av dem.

5. Kommissionen ska enligt artikel 10 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln.
6. Kommissionen får, genom genomförandeakter, anta gemensamma specifikationer som omfattar något av eller alla de väsentliga krav som fastställs i punkt 1 om följande villkor är uppfyllda:
- a) Kommissionen har enligt artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard som uppfyller de väsentliga krav som fastställs i punkt 1 i den här artikeln, och
 - i) begäran har inte accepterats,
 - ii) de harmoniserade standarder som avser denna begäran har inte levererats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller
 - iii) de harmoniserade standarderna uppfyller inte begäran, och
 - b) ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga krav som fastställs i punkt 1 i denna artikel är offentliggjord i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

7. Innan kommissionen utarbetar ett utkast till den genomförandeakt som avses i punkt 6 i denna artikel ska den underrätta den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 6 i den här artikeln är uppfyllda.
8. Vid utarbetandet av utkastet till den genomförandeakt som avses i punkt 6 ska kommissionen beakta råd från Europeiska datainnovationsstyrelsen och synpunkter från andra relevanta organ eller expertgrupper och vederbörligen samråda med alla berörda parter.
9. Säljaren av ett smart kontrakt eller, i avsaknad av en sådan, den person vars närings- eller yrkesverksamhet inbegriper användning av smarta kontrakt för andra inom ramen för genomförandet av ett avtal eller en del av det om att tillgängliggöra data som uppfyller de gemensamma specifikationer som fastställs genom genomförandeakter som avses i punkt 6 eller delar av dem ska förutsättas överensstämma med de väsentliga krav som fastställs i punkt 1 i den mån dessa krav omfattas av sådana gemensamma specifikationer eller delar av dem.

10. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 6 i denna artikel, eller delar av dem som omfattar samma väsentliga krav som de som omfattas av den harmoniserade standarden.
11. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga krav som fastställs i punkt 1 ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

Kapitel IX

Genomförande och verkställighet

Artikel 37

Behöriga myndigheter och datasamordnare

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska ansvara för tillämpningen och genomförandet av denna förordning (behöriga myndigheter). Medlemsstaterna får inrätta en eller flera nya myndigheter eller förlita sig på befintliga myndigheter.

2. Om en medlemsstat utser mer än en behörig myndighet ska den bland dem utse en datasamordnare för att underlätta samarbetet mellan de behöriga myndigheterna och bistå enheter som omfattas av denna förordning i alla frågor som rör dess tillämpning och efterlevnad. De behöriga myndigheterna ska, vid utövandet av de uppgifter och befogenheter som tilldelats dem enligt punkt 5, samarbeta med varandra.
3. De tillsynsmyndigheter som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 ska ansvara för att övervaka tillämpningen av den här förordningen när det gäller skyddet av personuppgifter. Kapitlen VI och VII i förordning (EU) 2016/679 ska gälla i tillämpliga delar.

Europeiska datatillsynsmannen ska ansvara för att övervaka tillämpningen av denna förordning i den mån den berör kommissionen, Europeiska centralbanken eller unionsorgan. Där det är relevant ska artikel 62 i förordning (EU) 2018/1725 gälla i tillämpliga delar.

Uppgifterna och befogenheterna för de tillsynsmyndigheter som avses i denna punkt ska utövas med avseende på behandling av personuppgifter.

4. Utan att det påverkar tillämpningen av punkt 1 i denna artikel gäller följande:
 - a) När det gäller sektorsspecifika frågor som rör åtkomst till och användning av data i samband med tillämpningen av denna förordning ska sektorsmyndigheternas behörighet respekteras.

- b) Den behöriga myndighet som ansvarar för tillämpningen och kontrollen av efterlevnaden av artiklarna 23–31, 34 och 35 ska ha erfarenhet på området data och elektroniska kommunikationstjänster.
5. Medlemsstaterna ska säkerställa att uppgifterna och befogenheterna för de behöriga myndigheterna är tydligt definierade och omfattar följande:
- a) Öka datakompetensen och medvetenheten bland de användare och enheter som omfattas av denna förordning om deras rättigheter och skyldigheter inom ramen för denna förordning.
 - b) Hantera klagomål som härrör från påstådda överträdelser av denna förordning, inbegripet vad gäller företagshemligheter, och i lämplig utsträckning undersöka föremålet för klagomålen och regelbundet inom rimlig tid informera de klagande, i tillämpliga fall i enlighet med nationell rätt, om hur utredningen fortskrider och om resultatet av den, särskilt om ytterligare utredning eller samordning med en annan behörig myndighet är nödvändig.
 - c) Utföra undersökningar om frågor som rör tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan behörig myndighet eller offentlig myndighet.
 - d) Ålägga effektiva, proportionella och avskräckande ekonomiska sanktioner, som kan inbegripa viten och sanktioner med retroaktiv verkan, eller inleda rättsliga förfaranden för åläggande av böter,

- e) Övervaka den tekniska och relevanta kommersiella utveckling som är relevant för tillgängliggörande och användning av data,
- f) Samarbeta med behöriga myndigheter i andra medlemsstater och, i förekommande fall, med kommissionen eller Europeiska datainnovationsstyrelsen, för att säkerställa en konsekvent och effektiv tillämpning av denna förordning, inbegripet utbyte av all relevant information på elektronisk väg, utan oskäligt dröjsmål, även avseende punkt 10 i denna artikel.
- g) Samarbeta med de relevanta behöriga myndigheter som ansvarar för genomförandet av andra unionsrättsakter eller nationella rättsakter, inbegripet med myndigheter med behörighet på området data och elektroniska kommunikationstjänster, med den tillsynsmyndighet som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 eller med sektorsmyndigheter för att säkerställa att den här förordningen genomdrivs i överensstämmelse med annan unionsrätt och nationell rätt.
- h) Samarbeta med de relevanta behöriga myndigheterna för att säkerställa att artiklarna 23–31, artikel 34 och 35 verkställs i överensstämmelse med annan unionsrätt och självreglering som är tillämplig på leverantörer av databehandlingstjänster.
- i) Säkerställa att bytesavgifter avskaffas i enlighet med artikel 29.
- j) Granska de begäranden om data som gjorts enligt kapitel V.

Om en datasamordnare har utsetts ska denna underlätta det samarbete som avses i första stycket f, g och h och på begäran bistå de behöriga myndigheterna.

6. Datasamordnaren ska, om en sådan behörig myndighet har utsetts,
 - a) fungera som enda kontaktpunkt för alla frågor som rör tillämpningen av denna förordning,
 - b) säkerställa att offentliga organs begäranden om att göra data tillgängliga på grund av ett exceptionellt behov enligt kapitel V finns tillgängliga för allmänheten på nätet och främja frivilliga avtal om datadelning mellan offentliga organ och datahållare,
 - c) årligen informera kommissionen om de avslag som det underrättats om enligt artiklarna 4.2, 4.8 och 5.11.
7. Medlemsstaterna ska meddela kommissionen namnen på de behöriga myndigheterna och deras uppgifter och befogenheter samt, i tillämpliga fall, namnet på datasamordnaren. Kommissionen ska föra ett offentligt register över dessa myndigheter.
8. När de behöriga myndigheterna utför sina uppgifter och utövar sina befogenheter i enlighet med denna förordning ska de vara opartiska och stå fria från all yttre påverkan, direkt eller indirekt, och får varken begära eller ta emot instruktioner i enskilda ärenden från någon annan offentlig myndighet eller någon privat part.
9. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har tillräckliga personalresurser och tekniska resurser och relevant sakkunskap för att de på ett effektivt sätt ska kunna utföra sina uppgifter i enlighet med denna förordning.

10. Enheter som omfattas av tillämpningsområdet för denna förordning ska omfattas av behörigheten för den medlemsstat där de är etablerade. Om enheten är etablerad i fler än en medlemsstat ska den anses omfattas av behörigheten för den medlemsstat där den har sitt huvudsakliga etableringsställe, dvs. där enheten har sitt huvudkontor eller säte från vilket de huvudsakliga finansiella funktionerna och den operativa kontrollen utövas.
11. Varje enhet som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen, och som inte är etablerad i unionen, ska utse en rättslig företrädare i en av medlemsstaterna.
12. För att säkerställa efterlevnaden av denna förordning ska enheter som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen bemyndiga en rättslig företrädare som de behöriga myndigheterna ska vända sig till utöver eller i stället för enheten med avseende på alla frågor som rör denna enhet. Den rättsliga företrädaren ska samarbeta med de behöriga myndigheterna och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och de bestämmelser som införts av enheter som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen för att säkerställa efterlevnaden av denna förordning.

13. En enhet som omfattas av tillämpningsområdet för denna förordning och som gör uppkopplade produkter tillgängliga eller erbjuder tillhörande tjänster i unionen ska anses omfattas av den medlemsstats behörighet där dess rättsliga företrädare finns. Att en sådan enhet utser en rättslig företrädare ska inte påverka denna enhets ansvar eller rättsliga åtgärder som kan vidtas mot denna enhet. Fram till dess att en enhet utser en rättslig företrädare i enlighet med denna artikel ska den i tillämpliga fall omfattas av alla medlemsstaters behörighet med avseende på att säkerställa tillämpningen och efterlevnaden av denna förordning. Varje behörig myndighet får utöva sin behörighet, inbegripet genom att ålägga effektiva, proportionella och avskräckande sanktioner, förutsatt att enheten inte är föremål för verkställighetsförfaranden enligt denna förordning avseende samma sakförhållanden vid en annan behörig myndighet.
14. De behöriga myndigheterna ska ha befogenhet att från användare, datahållare eller datamottagare, eller deras rättsliga företrädare, som omfattas av deras medlemsstats behörighet begära all information som krävs för att kontrollera efterlevnaden av denna förordning. Varje begäran om information ska stå i proportion till den underliggande uppgiftens utförande och innehålla en motivering.
15. Om en behörig myndighet i en medlemsstat begär bistånd eller verkställighetsåtgärder från en behörig myndighet i annan medlemsstat ska den lämna en motiverad begäran. En behörig myndighet ska vid mottagandet av en sådan begäran utan oskäligt dröjsmål lämna ett svar med detaljerade uppgifter om de åtgärder som har vidtagits eller som avses att vidtas.

16. Behöriga myndigheter ska respektera principen om konfidentialitet samt om yrkes- och affärshemligheter och ska skydda personuppgifter i enlighet med unionsrätten eller nationell rätt. All information som utbyts inom ramen för en begäran om bistånd och som tillhandahålls enligt denna artikel får användas endast med avseende på det ärende för vilket den har begärts.

Artikel 38

Rätt att lämna in klagomål

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel ska fysiska och juridiska personer ha rätt att enskilt eller, i förekommande fall, kollektivt lämna in ett klagomål till den relevanta behöriga myndigheten i den medlemsstat där de har sin hemvist, sin arbetsplats eller sin etableringsort, om de anser att deras rättigheter enligt denna förordning har kränkts. Datasamordnaren ska på begäran lämna all nödvändig information till fysiska och juridiska personer så att de kan lämna in klagomål till den relevanta behöriga myndigheten.
2. Den behöriga myndighet till vilken klagomålet har lämnats in ska i enlighet med nationell rätt underrätta klaganden om hur förfarandet fortskrider och om det beslut som fattats.

3. Behöriga myndigheter ska samarbeta för att effektivt och snabbt hantera och avgöra klagomål, bland annat genom att utan oskäligt dröjsmål utbyta all relevant information på elektronisk väg. Detta samarbete ska inte påverka de samarbetsmekanismer som föreskrivs i kapitlen VI och VII i förordning (EU) 2016/679 och i förordning (EU) 2017/2394.

Artikel 39

Rätten till ett effektivt rättsmedel

1. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol ska berörda fysiska och juridiska personer ha rätt till ett effektivt rättsmedel avseende rättsligt bindande beslut som fattats av behöriga myndigheter.
2. Om en behörig myndighet underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.
3. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den behöriga myndighet som rättsmedlen avser är belägen, antingen individuellt eller, i förekommande fall, kollektivt av företrädare för en eller flera fysiska eller juridiska personer.

Artikel 40

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.
2. Senast den ... [20 månader från dagen för denna förordnings ikraftträdande] ska medlemsstaterna till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål anmäla eventuella ändringar som berör dem. Kommissionen ska regelbundet uppdatera och föra ett lättillgängligt offentligt register över dessa åtgärder.
3. Medlemsstaterna ska beakta rekommendationerna från Europeiska datainnovationsstyrelsen och följande icke uttömmande kriterier för åläggande av sanktioner för överträdelser av denna förordning:
 - a) Överträdelsens art, allvar, omfattning och varaktighet.
 - b) Varje åtgärd som den överträdande parten har vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat.
 - c) Eventuella tidigare överträdelser som begåtts av den överträdande parten.
 - d) De ekonomiska fördelar som den överträdande parten har erhållit eller de förluster denna har undvikit genom överträdelsen, i den mån sådana fördelar eller förluster kan fastställas på ett tillförlitligt sätt.

- e) Eventuella andra försvårande eller förmildrande omständigheter som är tillämpliga på ärendet.
 - f) Den överträdande partens årsomsättning i unionen under det föregående räkenskapsåret.
4. För överträdelser av de skyldigheter som fastställs i kapitlen II, III och V i denna förordning får de tillsynsmyndigheter som ansvarar för att övervaka tillämpningen av förordning (EU) 2016/679 inom ramen för sin behörighet påföra administrativa sanktionsavgifter i enlighet med artikel 83 i förordning (EU) 2016/679 på upp till det belopp som avses i artikel 83.5 i den förordningen.
5. För överträdelser av de skyldigheter som fastställs i kapitel V i denna förordning får Europeiska datatillsynsmannen inom ramen för sin behörighet påföra administrativa sanktionsavgifter i enlighet med artikel 66 i förordning (EU) 2018/1725 på upp till det belopp som avses i artikel 66.3 i den förordningen.

Artikel 41

Standardavtalsvillkor och standardavtalsklausuler

Kommissionen ska före den ... [20 månader från dagen för denna förordnings ikraftträdande] utarbeta och rekommendera icke-bindande standardavtalsvillkor för åtkomst till och användning av data, inbegripet villkor om rimlig ersättning och skydd av företagshemligheter, och icke-bindande standardavtalsklausuler för molnavtal för att hjälpa parterna att utarbeta och förhandla fram avtal med rättvisa, rimliga och icke-diskriminerande avtalsenliga rättigheter och skyldigheter.

Artikel 42

Europeiska datainnovationsstyrelsens roll

Europeiska datainnovationsstyrelsen, som inrättats av kommissionen som en expertgrupp enligt artikel 29 i förordning (EU) 2022/868 och i vilken behöriga myndigheter ska vara företrädare, ska stödja en konsekvent tillämpning av den här förordningen genom att

- a) ge råd till och bistå kommissionen när det gäller att utveckla en konsekvent praxis hos behöriga myndigheter avseende efterlevnaden av kapitlen II, III, V och VII,
- b) underlätta samarbete mellan behöriga myndigheter genom kapacitetsuppbyggnad och informationsutbyte, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om efterlevnaden av rättigheterna och skyldigheterna enligt kapitlen II, III och V i gränsöverskridande fall, inbegripet samordning när det gäller fastställande av sanktioner,
- c) ge råd till och bistå kommissionen när det gäller
 - i) huruvida det ska begäras att sådana harmoniserade standarder som avses i artiklarna 33.4, 35.4 och 36.5 utarbetas,
 - ii) utarbetandet av de genomförandeakter som avses i artiklarna 33.5, 35.5, 35.8 och 36.6,
 - iii) utarbetandet av de delegerande akter som avses i artiklarna 29.7 och 33.2, och

- iv) antagandet av de riktlinjer om fastställande av interoperabla ramar för gemensamma standarder och praxisformer för de gemensamma europeiska dataområdenas funktion som avses i artikel 33.11.

Kapitel X

Rätten av sitt eget slag enligt direktiv 96/9/EG

Artikel 43

Databaser som innehåller vissa data

Rätten av sitt eget slag enligt artikel 7 i direktiv 96/9/EG ska inte tillämpas när data erhålls från eller genereras av en uppkopplad produkt eller en tillhörande tjänst som omfattas av denna förordning, särskilt med avseende på artiklarna 4 och 5 i denna förordning.

KAPITEL XI

SLUTBESTÄMMELSER

Artikel 44

Andra unionsrättsakter som reglerar rättigheter och skyldigheter avseende åtkomst till och användning av data

1. De specifika skyldigheterna att göra data tillgängliga mellan företag, mellan företag och konsumenter, och i undantagsfall mellan företag och offentliga organ, i unionsrättsakter som trädde i kraft senast den ... [den dag då denna förordning träder i kraft], och delegerade akter eller genomförandeakter som antagits på grundval av dessa, ska inte påverkas.

2. Denna förordning påverkar inte sådan unionsrätt som, mot bakgrund av behoven inom en sektor, ett gemensamt europeiskt dataområde eller ett område av allmänt intresse, fastställer ytterligare krav, särskilt när det gäller följande:
 - a) Tekniska aspekter på dataåtkomst.
 - b) Begränsningar av datahållares rätt att få åtkomst till eller använda vissa data som tillhandahålls av användarna.
 - c) Aspekter som går utöver åtkomst till och användning av data.
3. Denna förordning, med undantag för kapitel V, påverkar inte tillämpningen av sådan unionsrätt och nationell rätt som föreskriver åtkomst till och godkännande av användning av data för vetenskapliga forskningsändamål.

Artikel 45

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 29.7 och 33.2 ges till kommissionen tills vidare från och med ... [den dag då denna förordning träder i kraft].

3. Den delegering av befogenhet som avses i artiklarna 29.7 och 33.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artikel 29.7 eller artikel 33.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 46
Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats genom förordning (EU) 2022/868. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 47
Ändring av förordning (EU) 2017/2394

I bilagan till förordning (EU) 2017/2394 ska följande punkt läggas till:

- ”29. Europaparlamentets och rådets förordning (EU) 2023/... av den... om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (EUT L ...)+.”

Artikel 48
Ändring av direktiv (EU) 2020/1828

I bilaga I till direktiv (EU) 2020/1828 ska följande punkt läggas till:

- ”68. Europaparlamentets och rådets förordning (EU) 2023/... av den... om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (EUT L ...)+.”

⁺ EUT: Vänligen för in nummer, datum och EUT-hänvisning för den förordning som finns i dokument PE-CONS 49/23 (2022/0047(COD)).

Artikel 49

Utvärdering och översyn

1. Kommissionen ska senast den ... [56 månader från den dag då denna förordning träder i kraft] genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. I utvärderingen ska särskilt följande bedömas:
 - a) Situationer som ska betraktas som situationer då det finns exceptionella behov vid tillämpningen av artikel 15 i denna förordning och tillämpningen av kapitel V i denna förordning i praktiken, särskilt de offentliga organens, kommissionens, Europeiska centralbankens och unionsorganens erfarenheter av tillämpningen av kapitel V i denna förordning, antalet samt resultatet av de förfaranden som inletts hos den behöriga myndigheten enligt artikel 18.5 om tillämpningen av kapitel V i denna förordning, enligt vad som rapporterats av de behöriga myndigheterna, effekterna av andra skyldigheter som fastställs i unionsrätten eller nationell rätt för att tillmötesgå begäranden om åtkomst till information, effekterna av frivilliga mekanismer för datadelning, såsom de som införts av dataaltruismorganisationer som erkänns enligt förordning (EU) 2022/868, på uppnåendet av målen i kapitel V i den här förordningen, och personuppgifternas roll inom ramen för artikel 15 i den här förordningen, inbegripet utvecklingen av integritetsfrämjande teknik.

- b) Denna förordnings inverkan på användningen av data i ekonomin, inbegripet på datainnovation, metoder för monetarisering av data och dataförmedlingstjänster samt på datadelning inom de gemensamma europeiska dataområdena.
- c) Tillgängligheten till och användningen av olika kategorier och typer av data.
- d) Uteslutning av vissa kategorier av företag vad gäller bestämmelserna i artikel 5.
- e) Avsaknaden av all påverkan på immateriella rättigheter.
- f) Inverkan på företagshemligheter, inbegripet skyddet mot att de olagligen anskaffas, utnyttjas och lämnas ut, samt effekterna av den mekanism som gör det möjligt för datahållaren att avslå användarens begäran enligt artiklarna 4.8 och 5.11, med beaktande, i möjligaste mån, av en eventuell översyn av direktiv (EU) 2016/943.
- g) Huruvida den förteckning över oskäligen avtalsvillkor som avses i artikel 13 är uppdaterad mot bakgrund av nya affärsmetoder och den snabba takten i marknadsinnovationen.
- h) Ändringar av avtalspraxis hos leverantörer av databehandlingstjänster och huruvida detta leder till tillräcklig efterlevnad av artikel 25.
- i) Sänkningen av de avgifter som tas ut av leverantörer av databehandlingstjänster för bytesprocessen, i enlighet med det gradvisa avskaffandet av bytesavgifter enligt artikel 29.
- j) Samspelet mellan denna förordning och andra unionsrättsakter av betydelse för dataekonomin.

- k) Förhindrandet av olaglig statlig åtkomst till icke-personuppgifter.
 - l) Effektiviteten hos det system för kontroll av efterlevnad som krävs enligt artikel 37.
 - m) Inverkan av denna förordning på mikroföretag och små och medelstora företag när det gäller deras innovationskapacitet och tillgången till databehandlingstjänster för användare i unionen samt bördan som de nya skyldigheterna innebär.
- 2. Kommissionen ska senast den ... [56 månader från dagen för denna förordnings ikraftträdande] genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. I denna utvärdering ska effekterna av artiklarna 23–31, 34 och 35 bedömas, särskilt när det gäller prissättning och mångfalden av databehandlingstjänster som erbjuds inom unionen, med särskilt fokus på leverantörer som är mikroföretag och små och medelstora företag.
 - 3. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta de rapporter som avses i punkterna 1 och 2.
 - 4. På grundval av de rapporter som avses i punkterna 1 och 2 kan kommissionen om så är lämpligt lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet i syfte att ändra denna förordning.

Artikel 50

Ikraftträdande och tillämpning

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

Den ska tillämpas från och med den ... [20 månader från dagen för denna förordnings ikraftträdande].

De skyldigheter som följer av artikel 3.1 ska tillämpas på de uppkopplade produkter och de tillhörande tjänster som släpps ut på marknaden efter den ... [32 månader från dagen för denna förordnings ikraftträdande].

Kapitel III ska endast tillämpas på skyldigheter att göra data tillgängliga enligt unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten som träder i kraft efter den ... [20 månader från den dag då denna förordnings ikraftträdande].

Kapitel IV ska tillämpas på avtal som ingås efter den ... [20 månader från dagen för denna förordnings ikraftträdande].

Kapitel IV ska tillämpas från och med den ... [44 månader från dagen för denna förordnings ikraftträdande] på avtal som ingåtts den ... [20 månader från dagen för denna förordnings ikraftträdande] eller tidigare, under förutsättning att de

- a) har ingåtts på obestämd tid, eller
- b) löper ut minst 10 år efter den ... [den dag då denna förordning träder i kraft].

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

Utfärdad i ... den ...

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande
