



Fremsat den 8. oktober 2025 af ministeren for digitalisering (Caroline Stage Olsen)

Forslag

til

Lov om supplerende bestemmelser til forordningen om harmoniserende regler om fair adgang til og anvendelse af data (datadelingsloven)¹⁾

§ 1. Loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair adgang til og anvendelse af data (dataforordningen), jf. bilag 1.

§ 2. Digitaliseringsstyrelsen er kompetent myndighed i overensstemmelse med artikel 37, stk. 1, i dataforordningen.

Stk. 2. Digitaliseringsstyrelsen påser overholdelsen af dataforordningen, jf. artikel 37, stk. 1, i dataforordningen, og varetager de opgaver, der er oplistet i dataforordningens artikel 37, stk. 5 og 6.

Stk. 3. Ministeren for digitalisering kan fastsætte nærmere regler om indgivelse af klager efter dataforordningen, herunder formkrav til sådanne klager.

§ 3. Ministeren for digitalisering kan fastsætte nærmere regler om certificering af tvistbilæggesorganer i henhold til artikel 10 i dataforordningen. Ministeren for digitalisering kan derudover fastsætte sådanne regler på andre ministres ressortområder efter aftale med vedkommende minister.

§ 4. Digitaliseringsstyrelsen skal ved udførelsen af sine opgaver og udøvelsen af sine beføjelser i henhold til dataforordningen og denne lov være upartisk og fri for udefra kommende indflydelse, det være sig direkte eller indirekte, og må hverken søge eller modtage instrukser med henblik på enkeltsager fra nogen anden offentlig myndighed eller nogen privat part i overensstemmelse med artikel 37, stk. 8, i dataforordningen.

Stk. 2. Digitaliseringsstyrelsens afgørelser efter dataforordningen og denne lov kan ikke indbringes for anden administrativ myndighed.

§ 5. Digitaliseringsstyrelsen kan fra fysiske og juridiske personer omfattet af dataforordningen samt retlige repræsentanter omfattet af artikel 37, stk. 11, i dataforordningen, anmode om alle oplysninger, som er nødvendige for Digitaliseringsstyrelsens tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under Digitaliseringsstyrelsens kompetence.

§ 6. Digitaliseringsstyrelsen kan videregive oplysninger til Europa-Kommissionen og andre kompetente myndigheder i Den Europæiske Union, i det omfang det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov, dataforordningen eller den pågældende medlemsstats datadelingslovgivning.

§ 7. Digitaliseringsstyrelsen kan udtale kritik af fysiske og juridiske personer omfattet af dataforordningen for overtrædelser af dataforordningen eller denne lov.

§ 8. Digitaliseringsstyrelsen kan offentliggøre sine udtalelser efter § 7 og afgørelser efter § 9 om overtrædelser af dataforordningen eller denne lov.

§ 9. Digitaliseringsstyrelsen kan udstede påbud til fysiske og juridiske personer omfattet af dataforordningen med henblik på at sikre overholdelsen af forpligtelser i medfør af dataforordningen.

§ 10. Medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der uagtsomt eller forsætligt:

- 1) Overtræder dataforordningens artikel 3, artikel 4, stk. 1, 2, 4-8, 10, 11, 13 eller 14, artikel 5, stk. 1, 3-6 eller 9-11, artikel 6, stk. 1 eller 2, artikel 8, stk. 4, artikel 11,

¹⁾ I lovforslaget er der medtaget visse bestemmelser fra Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair adgang til og anvendelse af data og om ændring af forordning (EU) 2017/2394 og direktiv (EU) 2020/1828 (dataforordningen), EU-Tidende 2023, L af 13. december 2023. Ifølge artikel 288 i EUF-Traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven og gengivelsen af forordningen i lovens bilag er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

14, 23, 25-28, artikel 29, stk. 1, 3, 5 eller 6, artikel 30, stk. 1-5, artikel 31, stk. 3, eller artikel 32, stk. 1, 4 eller 5.

- 2) Undlader at efterkomme Digitaliseringsstyrelsens krav efter § 5 eller i forbindelse med sådanne krav afgiver ukorrekte, ufuldstændige eller vildledende oplysninger eller fortier oplysninger.
- 3) Undlader at efterkomme et påbud udstedt efter § 9.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 3. Forældelsesfristen for overtrædelse af dataforordningen eller denne lov er 5 år.

§ 11. Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

§ 12. Loven gælder ikke for Færøerne og Grønland.

Bilag 1**EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2023/2854 af 13. december 2023
om harmoniserede regler om fair adgang til og anvendelse af data og om ændring af forordning
(EU) 2017/2394 og direktiv (EU) 2020/1828 (dataforordningen)****(EØS-relevant tekst)**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Den Europæiske Centralbank ⁽¹⁾,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ⁽²⁾,

under henvisning til udtalelse fra Regionsudvalget ⁽³⁾,

efter den almindelige lovgivningsprocedure ⁽⁴⁾, og

ud fra følgende betragtninger:

- 1) I de seneste år har datadrevne teknologier haft omskabende virkning på alle sektorer i økonomien. Navnlig udbredelsen af produkter, der er forbundet med internettet, har øget mængden og den potentielle værdi af data for forbrugere, virksomheder og samfundet. Interoperable data af høj kvalitet fra forskellige områder øger konkurrenceevnen og innovationen og sikrer bæredygtig økonomisk vækst. De samme data kan anvendes og videreanvendes til forskellige formål og i ubegrænset omfang, uden at kvalitet eller omfang forringes.
- 2) Hindringer for deling af data vanskeliggør en optimal datafordeling til gavn for samfundet. Disse hindringer omfatter manglende incitamenter for dataindehavere til frivilligt at indgå aftaler om data-deling, usikkerhed om rettigheder og forpligtelser vedrørende data, omkostningerne ved indgåelse af aftaler og gennemførelse af tekniske grænseflader, den høje grad af fragmentering af oplysninger i datasiloer, ringe metadataforvaltning, manglende standarder for semantisk og teknisk interoperabilitet, flaskehalse, der hindrer dataadgang, en mangel på fælles praksis for datadeling samt misbruget af aftalemæssige skævheder for så vidt angår adgang til og anvendelse af data.
- 3) I de sektorer, der er kendetegnet ved tilstedeværelsen af mikrovirksomheder, små virksomheder og mellemstore virksomheder som defineret i artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF ⁽⁵⁾(SMV'er), mangler der ofte digital kapacitet og digitale færdigheder til at indsamle, analysere og anvende data, og adgangen er ofte begrænset, hvor en enkelt aktør besidder dataene i

systemet, eller som følge af manglende interoperabilitet mellem data, mellem datatjenester eller på tværs af grænserne.

- 4) For at imødekomme den digitale økonomis behov og fjerne hindringer for et velfungerende indre marked for data er det nødvendigt at fastlægge en harmoniseret ramme, der præciserer, hvem der har ret til at anvende produktdata eller relaterede tjenstedata, på hvilke betingelser og på hvilket grundlag. Medlemsstaterne bør derfor ikke vedtage eller opretholde yderligere nationale krav med hensyn til spørgsmål, der falder ind under denne forordnings anvendelsesområde, medmindre det udtrykkeligt er fastsat i denne forordning, da dette vil påvirke dens direkte og ensartede anvendelse. Desuden bør tiltag på EU-plan ikke berøre pligter og tilsagn, som er indeholdt i internationale handelsaftaler indgået af Unionen.
- 5) Ved denne forordning sikres det, at brugere af et forbundet produkt eller en relateret tjeneste i Unionen rettidigt kan få adgang til de data, der genereres ved brugen af det pågældende forbundne produkt eller den pågældende relaterede tjeneste, og at brugerne kan anvende dataene, bl.a. ved at dele dem med tredjeparter efter eget valg. Dataindehavere pålægges en forpligtelse til stille data til rådighed for brugere og tredjeparter efter brugerens valg under visse omstændigheder. Ved denne forordning sikres det også, at dataindehavere stiller data til rådighed for datamodtagere i Unionen på fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser og på en gennemsigtig måde. Privatretlige regler er vigtige i den overordnede ramme for datadeling. Denne forordning tilpasser derfor aftaleretlige regler og forhindrer udnyttelse af aftalemæssige skævheder, der hindrer fair adgang til og anvendelse af data. Ved denne forordning sikres det også, at dataindehavere stiller de data, der er nødvendige for udførelsen af en specifik opgave i offentlighedens interesse, til rådighed for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer, hvis der er et ekstraordinært behov herfor. Desuden har denne forordning til formål at gøre det lettere at skifte mellem databehandlingstjenester og at forbedre interoperabiliteten af data og datadelingsmekanismer og -tjenester i Unionen. Denne forordning bør ikke fortolkes således, at der ved den anerkendes eller tillægges en ny ret for dataindehaverne til at anvende data, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste.
- 6) Datagenerering er resultatet af handlinger foretaget af mindst to aktører, navnlig designeren eller producenten af et forbundet produkt, som i mange tilfælde også kan være en udbyder af relaterede tjenester, og brugeren af dette forbundne produkt eller denne relaterede tjeneste. Det giver anledning til spørgsmål om retfærdighed i den digitale økonomi, da de data, der registreres af forbundne produkter eller relaterede tjenester, er et vigtigt input i eftersalgsservice, accessoriske tjenesteydelser og andre tjenester. For at kunne udnytte de vigtige økonomiske fordele ved data, herunder ved datadeling på grundlag af frivillige aftaler og udvikling af datadrevet værdiskabelse fra EU-virksomheders side, er en generel tilgang til tildeling af rettigheder vedrørende adgang til og brug af data at foretrække frem for eksklusive adgangs- og brugsrettigheder. Denne forordning indeholder horisontelle regler, som vil kunne følges af EU-ret eller national ret, som imødegår de særlige situationer i de relevante sektorer.
- 7) Den grundlæggende ret til beskyttelse af personoplysninger er navnlig sikret ved Europa-Parlamentets og Rådets forordning (EU) 2016/679 ⁽⁶⁾ og (EU) 2018/1725 ⁽⁷⁾. Europa-Parlamentets og Rådets direktiv 2002/58/EF ⁽⁸⁾ beskytter desuden privatlivets fred og kommunikationshemmeligheden, herunder i form af betingelser for enhver form for personoplysninger og andre data end personoplysninger, der er lagret i og tilgås fra terminaludstyr. Disse lovgivningsmæssige EU-retsakter danner grundlaget for bæredygtig og ansvarlig databehandling, herunder når datasæt omfatter en blanding af personoplysninger og andre data end personoplysninger. Nærværende forordning supplerer, og berører ikke, EU-retten om beskyttelse af personoplysninger og af privatlivets fred, navnlig forordning

(EU) 2016/679 og (EU) 2018/1725 og direktiv 2002/58/EF. Ingen bestemmelse i nærværende forordning bør anvendes eller fortolkes på en sådan måde, at retten til beskyttelse af personoplysninger, retten til privatlivets fred eller kommunikationshemmeligheden mindskes eller begrænses. Enhver behandling af personoplysninger i henhold til nærværende forordning bør overholde EU-retten om databeskyttelse, herunder kravet om et gyldigt retsgrundlag for behandling i henhold til artikel 6 i forordning (EU) 2016/679 og, hvor det er relevant, betingelserne i artikel 9 i nævnte forordning og i artikel 5, stk. 3, i direktiv 2002/58/EF. Nærværende forordning udgør ikke et retsgrundlag for indsamling eller generering af personoplysninger fra dataindehaverens side. Nærværende forordning pålægger dataindehavere en forpligtelse til at stille personoplysninger til rådighed for brugere eller tredjeparter efter en brugers valg på anmodning fra denne bruger. En sådan adgang bør gives til personoplysninger, der behandles af dataindehaveren på grundlag af et af de retsgrundlag, der er omhandlet i artikel 6 i forordning (EU) 2016/679. Når brugeren ikke er en registreret, skaber nærværende forordning ikke et retsgrundlag for at give adgang til personoplysninger eller for at stille personoplysninger til rådighed for en tredjepart og bør ikke forstås således, at den giver dataindehaveren nogen ny ret til at anvende personoplysninger, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste. I disse tilfælde kan det være i brugerens interesse at lette opfyldelsen af kravene i artikel 6 i forordning (EU) 2016/679. Da nærværende forordning ikke bør påvirke registreredes databeskyttelsesrettigheder i negativ retning, kan dataindehaveren imødekomme anmodninger i disse tilfælde, bl.a. ved at anonymisere personoplysninger eller, hvis de let tilgængelige data indeholder personoplysninger om adskillige registrerede, ved kun at overføre personoplysninger vedrørende brugeren.

- 8) Principperne om dataminimering og databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er afgørende, når behandlingen indebærer betydelige risici for fysiske personers grundlæggende rettigheder. Under hensyntagen til det aktuelle tekniske niveau bør alle parter i en datadeling, herunder datadeling inden for denne forordnings anvendelsesområde, gennemføre tekniske og organisatoriske foranstaltninger for at beskytte disse rettigheder. Sådanne foranstaltninger omfatter ikke kun pseudonymisering og kryptering, men også anvendelse af stadig mere tilgængelig teknologi, der gør det muligt at overføre algoritmer til data og opnå værdifuld indsigt uden overførsel mellem parterne eller unødvendig kopiering af de rå eller strukturerede data.
- 9) Medmindre andet er fastsat i denne forordning, berører den ikke national aftaleret, herunder regler om indgåelse, gyldighed eller virkning af aftaler eller konsekvenserne af en aftales opsigelse. Denne forordning supplerer, og berører ikke, EU-ret, der har til formål at fremme forbrugernes interesser og sikre et højt forbrugerbeskyttelsesniveau og at beskytte forbrugernes sundhed, sikkerhed og økonomiske interesser, navnlig Rådets direktiv 93/13/EØF ⁽⁹⁾ og Europa-Parlamentets og Rådets direktiv 2005/29/EF ⁽¹⁰⁾ og 2011/83/EU ⁽¹¹⁾.
- 10) Denne forordning berører ikke EU-retsakter og nationale retsakter, der indeholder bestemmelser om deling af, adgang til og anvendelse af data med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrkelse af strafferetlige sanktioner eller til told- og skatteformål, uanset det retsgrundlag i traktaten om Den Europæiske Unions funktionsmåde (TEUF), som sådanne EU-retsakter er vedtaget på grundlag af, samt internationalt samarbejde på dette område, navnlig på grundlag af Europarådets konvention om IT-kriminalitet (ETS nr. 185), udfærdiget i Budapest den 23. november 2001. Sådanne retsakter omfatter Europa-Parlamentets og Rådets forordning (EU) 2021/784 ⁽¹²⁾, (EU) 2022/2065 ⁽¹³⁾ og (EU) 2023/1543 ⁽¹⁴⁾ og Europa-Parlamentets og Rådets direktiv (EU) 2023/1544 ⁽¹⁵⁾. Nærværende forordning finder ikke anvendelse på indsamling eller deling af, adgang til eller behandling af data i henhold til Europa-Parlamentets og Rådets forordning (EU) 2015/847 ⁽¹⁶⁾ og Europa-Parlamentets og Rådets direktiv (EU) 2015/849

(¹⁷). Nærværende forordning finder ikke anvendelse på områder, der falder uden for EU-retten, og berører under alle omstændigheder ikke medlemsstaternes beføjelser vedrørende offentlig sikkerhed, forsvar eller national sikkerhed, told- og skatteforvaltning eller borgernes sundhed og sikkerhed, uanset hvilken typeenhed medlemsstaterne har bemyndiget til at udføre opgaver i forbindelse med disse kompetencer.

- 11) EU-ret, hvorved der er fastsat krav vedrørende den fysiske udformning af og datakrav til produkter, der skal bringes i omsætning på EU-markedet, bør ikke berøres, medmindre det udtrykkeligt er fastsat i denne forordning.
- 12) Denne forordning supplerer, og berører ikke, EU-ret, der har til formål at fastsætte tilgængelighedskrav for visse produkter og tjenester, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2019/882 (¹⁸).
- 13) Denne forordning berører ikke EU-retsakter og nationale retsakter til beskyttelse af intellektuelle ejendomsrettigheder, herunder Europa-Parlamentets og Rådets direktiv 2001/29/EF (¹⁹), 2004/48/EF (²⁰) og (EU) 2019/790 (²¹).
- 14) Forbundne produkter, der ved hjælp af deres komponenter eller operativsystemer opnår, genererer eller indsamler data vedrørende deres ydeevne, anvendelse eller omgivelser, og som er i stand til at formidle disse data via en elektronisk kommunikationstjeneste, en fysisk forbindelse eller adgang på en enhed, som ofte kaldes tingenes internet, bør være omfattet af denne forordnings anvendelsesområde med undtagelse af prototyper. Eksempler på sådanne elektroniske kommunikationstjenester omfatter navnlig landbaserede telefonnet, kabel-TV-net, satellitbaserede net og nærfeltskommunikationsnet. Forbundne produkter findes i alle aspekter af økonomien og samfundet, herunder i privat, civil eller kommerciel infrastruktur, køretøjer, udstyr til sundheds- og livsstilsektoren, skibe, luftfartøjer, husholdningsudstyr og forbrugsvarer, medicinske og sundhedsmæssige redskaber eller landbrugs- og industrimaskiner. Producenters valg af udformning og, hvor det er relevant, EU-ret eller national ret, som imødegår sektorspecifikke behov og mål, og kompetente myndigheders relevante afgørelser bør bestemme, hvilke data et forbundet produkt kan stille til rådighed.
- 15) Dataene repræsenterer en digitalisering af brugerhandlinger og -begivenheder og bør derfor være tilgængelige for brugeren. Reglerne for adgang til og anvendelse af data fra forbundne produkter og relaterede tjenester i henhold til denne forordning vedrører både produktdata og relaterede tjenstedata. Ved produktdata forstås data, der er genereret ved brug af et forbundet produkt, som producenten har udformet til at kunne hentes fra det forbundne produkt af en bruger, dataindehaver eller en tredjepart, herunder, hvis det er relevant, producenten. Ved relaterede tjenstedata forstås data, som også repræsenterer digitaliseringen af brugerhandlinger eller -begivenheder i forbindelse med det forbundne produkt, som genereres under udbyderens levering af en relateret tjeneste. Data, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste, bør forstås således, at de omfatter data, som bevidst er registreret, eller data, der indirekte er et resultat af brugerens handling, såsom data om det forbundne produkts omgivelser eller interaktioner. Dette bør omfatte data om brugen af et forbundet produkt, der er genereret af en brugergrænseflade eller via en relateret tjeneste, og bør ikke være begrænset til oplysningerne om, at en sådan brug har fundet sted, men bør omfatte alle data, som det forbundne produkt genererer som følge af en sådan brug, såsom data, der er genereret automatisk af sensorer, og data, der er registreret af integrerede applikationer, herunder applikationer, der angiver hardwarestatus og funktionsfejl. Dette bør også omfatte data, der er genereret af det forbundne produkt eller den relaterede tjeneste i perioder uden handling fra brugerens side, f.eks. når brugeren vælger ikke at anvende et forbundet produkt i en given periode og i stedet holde det i standbytilstand eller endda slukket, da et forbundet produkts

eller dets komponenters, f.eks. dets batteriers, status kan variere, når det forbundne produkt er i standbytilstand eller er slukket. Data, som ikke ændres væsentligt, dvs. data i ubearbejdet form, også kendt som kildedata eller primære data, hvilket henviser til datapunkter, der er genereret automatisk uden yderligere behandling, samt data, der er blevet forbehandlet med henblik på at gøre dem forståelige og anvendelige forud for yderligere behandling og analyse, falder inden for denne forordnings anvendelsesområde. Sådanne data omfatter data indsamlet fra en enkelt sensor eller en forbundet gruppe af sensorer med henblik på at gøre de indsamlede data forståelige for bredere brugstilfælde ved at bestemme en fysisk mængde eller kvalitet eller ændringen i en fysisk mængde såsom temperatur, tryk, strømningshastighed, lyd, pH-værdi, væskenniveau, position, acceleration eller hastighed. Udtrykket »forbehandlede data« bør ikke fortolkes på en sådan måde, at dataindehaveren forpligtes til at foretage betydelige investeringer i rensning og transformation af dataene. De data, som skal stilles til rådighed, bør omfatte de relevante metadata, herunder deres grundlæggende kontekst og tidsstempel, til at gøre dataene anvendelige kombineret med andre data såsom data sorteret og klassificeret sammen med andre datapunkter vedrørende dem, eller omformateret til et almindeligt anvendt format. Sådanne data er potentielt værdifulde for brugeren og støtter innovation og udviklingen af digitale tjenester og andre tjenester for at beskytte miljøet, sundheden og den cirkulære økonomi, herunder ved at lette vedligeholdelse og reparation af de pågældende forbundne produkter. Derimod bør oplysninger, der udledes eller afledes af sådanne data, og som er resultatet af yderligere investeringer i tildeling af værdier eller indsigt fra dataene, navnlig ved hjælp af proprietære komplekse algoritmer, herunder algoritmer, der er en del af proprietær software, ikke anses for at falde ind under denne forordnings anvendelsesområde og bør derfor ikke være underlagt en dataindehavers forpligtelse til at stille dem til rådighed for en bruger eller datamodtager, medmindre andet er aftalt mellem brugeren og dataindehaveren. Sådanne data kan navnlig omfatte oplysninger, der afledes ved sensorintegration, hvor data udledes eller afledes af flere sensorer, indsamlet i det forbundne produkt, ved hjælp af proprietære komplekse algoritmer, og som kunne være omfattet af intellektuelle ejendomsrettigheder.

- 16) Denne forordning gør det muligt for brugere af forbundne produkter at drage fordel af eftersalgsservice, accessoriske tjenesteydelser og andre tjenester baseret på data indsamlet af sensorer, der er integreret i sådanne produkter, idet indsamlingen af disse data er af potentiel værdi med hensyn til at forbedre de forbundne produkters ydeevne. Det er vigtigt at foretage en afgrænsning mellem, på den ene side, markeder for levering af sådanne sensorudstyrede forbundne produkter og relaterede tjenester og, på den anden side, markeder for ikke-relateret software og indhold såsom tekstindhold, lydindhold eller audiovisuelt indhold, der ofte er omfattet af intellektuelle ejendomsrettigheder, på den anden side. Som følge heraf bør data, som sådanne sensorudstyrede forbundne produkter genererer, når brugeren optager, overfører, viser eller afspiller indhold, samt selve indholdet, som ofte er omfattet af intellektuelle ejendomsrettigheder, bl.a. til brug for en onlinetjeneste, ikke være omfattet af denne forordning. Denne forordning bør heller ikke omfatte data, der er opnået, genereret eller tilgået fra det forbundne produkt, eller som er overført til det med henblik på lagring eller andre behandlingsaktiviteter på vegne af andre parter, som ikke er brugeren, hvilket kan være tilfældet med servere eller cloudinfrastruktur, der drives af deres ejere udelukkende på vegne af tredjeparter, bl.a. til brug for en onlinetjeneste.
- 17) Det er nødvendigt at fastsætte regler vedrørende produkter, som er forbundet med en relateret tjeneste på købs-, leje- eller leasingtidspunktet på en sådan måde, at dens fravær ville forhindre det forbundne produkt i at udføre en eller flere af sine funktioner, eller som efterfølgende forbindes med produktet af producenten eller en tredjepart med henblik på at supplere eller tilpasse det forbundne produkts funktionalitet. Sådanne relaterede tjenester omfatter udveksling af data mellem det forbundne produkt og tjenesteudbyderen og bør forstås som værende udtrykkeligt knyttet til

den måde, hvorpå det forbundne produkts funktioner fungerer, såsom tjenester, der i givet fald overfører kommandoer til det forbundne produkt, som er i stand til at påvirke dets handlinger eller opførsel. Tjenester, der ikke påvirker den måde, hvorpå det forbundne produkt fungerer, og som ikke indebærer, at tjenesteudbyderen overfører data eller kommandoer til det forbundne produkt, bør ikke betragtes som relaterede tjenester. Sådanne tjenester kan f.eks. omfatte hjælperådgivning, analyse eller finansielle tjenesteydelser eller regelmæssig reparation og vedligeholdelse. Relaterede tjenester kan tilbydes som en del af købs-, leje- eller leasingaftalen. Sådanne relaterede tjenester kan også leveres i forbindelse med produkter af samme type, og brugere kan med rimelighed forvente leveringen i betragtning af det forbundne produkts karakter og eventuelle offentlige udsagn fremsat af eller på vegne af sælger, udlejer, leasinggiver eller andre personer i forudgående led i transaktionskæden, herunder producenten. Disse relaterede tjenester kan selv generere data af værdi for brugeren uafhængigt af det forbundne produkts kapacitet til at indsamle data. Denne forordning bør også finde anvendelse på relaterede tjenester, der ikke leveres af sælger, udlejer eller leasinggiver selv, men som leveres af en tredjepart. I tilfælde af tvivl om, hvorvidt tjenesten leveres som en del af købs-, leje- eller leasingaftalen, bør denne forordning finde anvendelse. Hverken strømforsyningen eller tilvejebringelsen af konnektivitet skal fortolkes som relaterede tjenester i henhold til denne forordning.

- 18) Brugeren af et forbundet produkt bør forstås som en fysisk eller juridisk person såsom en virksomhed, en forbruger eller en offentlig myndighed, der ejer et forbundet produkt, har fået visse midlertidige rettigheder, f.eks. gennem en leje- eller leasingaftale, til at få adgang til eller anvende data, der er opnået fra det forbundne produkt, eller modtager relaterede tjenester med henblik på det forbundne produkt. Disse adgangsrettigheder bør på ingen måde ændre eller gribe ind i rettighederne for registrerede, som kan interagere med et forbundet produkt eller en relateret tjeneste med hensyn til personoplysninger, der er genereret af det forbundne produkt eller under leveringen af den relaterede tjeneste. Brugeren bærer de risici og nyder godt af de fordele, der er forbundet med at bruge det forbundne produkt, og bør også have adgang til de data, det genererer. Brugeren bør derfor have ret til at drage fordel af de data, der er genereret af det forbundne produkt og enhver relateret tjeneste. En ejer, udlejer eller leasingtager bør også anses for at være en bruger, herunder når flere enheder kan anses for at være brugere. I forbindelse med flere brugere kan hver bruger bidrage på forskellig vis til datagenereringen og have en interesse i flere former for anvendelse såsom forvaltning af en bilpark for en leasingvirksomhed eller mobilitetsløsninger for enkeltpersoner, der benytter en bildelingstjeneste.
- 19) Ved datakompetence forstås færdigheder, viden og forståelse, der gør det muligt for brugere, forbrugere og virksomheder, navnlig SMV'er, der falder ind under denne forordnings anvendelsesområde, at få kendskab til den potentielle værdi af de data, som de har genereret, producerer og deler, og som de er motiverede til at tilbyde og give adgang til i overensstemmelse med relevante retsregler. Datakompetence bør være mere end blot læring om værktøjer og teknologier og bør sigte mod at give borgere og virksomheder evne og myndighed til at drage fordel af et inklusivt og retfærdigt datamarked. Udbredelsen af foranstaltninger vedrørende datakompetence og indførelsen af passende opfølgende tiltag kan bidrage til at forbedre arbejdsvilkårene og i sidste ende understøtte dataøkonomiens konsoliderings- og innovationssti i Unionen. De kompetente myndigheder bør fremme værktøjer og vedtage foranstaltninger til at fremme datakompetence blandt brugere og enheder, der falder ind under denne forordnings anvendelsesområde, og et kendskab til deres rettigheder og forpligtelser i henhold til denne forordning.
- 20) I praksis er ikke alle data, der genereres af forbundne produkter eller relaterede tjenester, let tilgængelige for brugeren, og der er ofte begrænsede muligheder med hensyn til portabilitet af data

genereret af produkter, der er forbundet med internettet. Brugeren er ude af stand til at opnå de data, der er nødvendige for at gøre brug af leverandører af reparationstjenester og andre tjenester, og virksomheder er ude af stand til at tilbyde innovative, bekvemme og mere effektive tjenester. I mange sektorer kan producenterne gennem deres kontrol over de forbundne produkters eller de relaterede tjenesters tekniske udformning bestemme, hvilke data der genereres, og hvordan de kan tilgås, selv om de ikke har nogen juridisk ret til de pågældende data. Det er derfor nødvendigt at sikre, at forbundne produkter udformes og fremstilles, og at relaterede tjenester udformes og leveres, på en sådan måde, at produktdata og relaterede tjenestedata, herunder de tilhørende metadata, der er nødvendige for at fortolke og anvende disse data, herunder med henblik på at hente, anvende eller dele dem, altid er let og sikkert tilgængelige for en bruger gratis og i et fyldestgørende, struktureret, almindeligt anvendt og maskinlæsbart format. Produktdata og relaterede tjenestedata, som en dataindehaver lovligt opnår eller lovligt kan opnå fra det forbundne produkt eller den relaterede tjeneste såsom gennem det forbundne produkts udformning, dataindehaverens aftale med brugeren om levering af relaterede tjenester og dennes tekniske midler til dataadgang uden en uforholdsmæssig stor indsats, benævnes »let tilgængelige data«. Let tilgængelige data omfatter ikke data, der er genereret via brugen af et forbundet produkt, hvor det forbundne produkts udformning ikke kræver, at sådanne data skal lagres eller overføres uden for den komponent, som de er genereret i, eller det forbundte produkt som helhed. Denne forordning bør derfor ikke forstås således, at den pålægger en forpligtelse til at lagre data på et forbundet produkts centrale databehandlingsenhed. Fravær af en sådan forpligtelse bør ikke forhindre producenten eller dataindehaveren i frivilligt at indgå aftale med brugeren om at foretage sådanne tilpasninger. Denne forordnings udformningsforpligtelser berører heller ikke princippet om dataminimering, der er fastsat i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679, og bør ikke forstås således, at de pålægger en forpligtelse til at udforme forbundne produkter og relaterede tjenester på en sådan måde, at de lagrer eller på anden måde behandler andre personoplysninger end de personoplysninger, der er nødvendige i forbindelse med at opfylde de formål, hvortil de behandles. Der vil kunne indføres EU-ret eller national ret for at skitsere yderligere særlige forhold såsom minimumsniveauet af produktdata, der bør være tilgængelige fra forbundne produkter eller relaterede tjenester, eftersom sådanne data kan være afgørende for disse forbundne produkters eller relaterede tjenesters effektive funktion, reparation eller vedligeholdelse. Hvis efterfølgende opdateringer eller ændringer af et forbundet produkt eller en relateret tjeneste foretaget af producenten eller en anden part fører til yderligere tilgængelige data eller en begrænsning af oprindeligt tilgængelige data, bør de pågældende ændringer meddeles brugeren i forbindelse med opdateringen eller ændringen.

- 21) Hvis flere personer eller enheder betragtes som brugere, f.eks. i tilfælde af fælles ejerskab, eller hvis en ejer, udlejer eller leasingtager deler rettigheder til dataadgang eller -anvendelse, bør udformningen af det forbundne produkt, den relaterede tjeneste eller den relevante grænseflade gøre det muligt for hver bruger at få adgang til de data, de genererer. Typisk kræves det, at brugere af forbundne produkter, der genererer data, opretter en brugerkonto. En sådan brugerkonto gør det muligt for en dataindehaver, som kan være producenten, at identificere brugeren. Den kan også anvendes som et kommunikationsmiddel og til at indgive og behandle anmodninger om dataadgang. Hvis flere producenter eller udbydere af relaterede tjenester har solgt, udlejet eller leaset forbundne produkter eller leveret relaterede tjenester, der er integreret, til den samme bruger, bør brugeren henvende sig til hver af de parter, som brugeren har en aftale med. Producenter eller designere af et forbundet produkt, der typisk anvendes af flere personer, bør indføre de nødvendige mekanismer, der gør det muligt for individuelle personer at have særskilte brugerkonti i de tilfælde, hvor det er relevant, eller for flere personer at benytte den samme brugerkonto. Kontoløsninger bør gøre det muligt for brugerne at slette deres konti og de data, der vedrører dem, og kunne give brugerne mulighed for at

bringe dataadgangen, -anvendelsen eller -delingen til ophør eller indgive anmodninger med henblik herpå, navnlig under hensyntagen til situationer, hvor ejerskabet eller anvendelsen af det forbundne produkt ændres. Brugeren bør få adgang på grundlag af en simpel anmodningsmekanisme, hvor udførelsen sker automatisk, og hvor der ikke kræves undersøgelse eller godkendelse fra producentens eller dataindehaverens side. Det betyder, at dataene kun bør stilles til rådighed, når brugeren rent faktisk ønsker adgang. Hvis det ikke er muligt at udføre anmodningen om dataadgang automatisk, f.eks. via en brugerkonto eller en ledsagende mobilapplikation leveret sammen med det forbundne produkt eller den relaterede tjeneste, bør producenten oplyse brugeren om, hvordan der kan opnås adgang til dataene.

- 22) Forbundne produkter kan være udformet således, at visse data er direkte tilgængelige fra datalagring på enheden eller fra en fjernserver, som dataene videresendes til. Adgang til datalagring på enheden kan gøres mulig via kabelbaserede eller trådløse lokale net, der er forbundet med en offentligt tilgængelig elektronisk kommunikationstjeneste eller et offentligt tilgængeligt mobilnet. Serveren kan være producentens egen lokale serverkapacitet eller en tredjeparts eller cloudtjenesteudbyders. Databehandlere som defineret i artikel 4, nr. 8), i forordning (EU) 2016/679 anses ikke for at fungere som dataindehavere. Den dataansvarlige som defineret i artikel 4, nr. 7), i forordning (EU) 2016/679 kan dog specifikt give dem til opgave at stille data til rådighed. Forbundne produkter kan være udformet med henblik på at gøre det muligt for brugeren eller en tredjepart at behandle dataene i det forbundne produkt, i en databehandlingsinstans fra producenten eller i et informations- og kommunikationsteknologimiljø (IKT-miljø), der er valgt af brugeren eller tredjeparten.
- 23) Virtuelle assistenter spiller en stadig større rolle i digitaliseringen af forbrugermiljøer og professionelle miljøer og fungerer som en brugervenlig grænseflade til at afspille indhold, få adgang til oplysninger eller aktivere produkter, der er forbundet med internettet. Virtuelle assistenter kan fungere som en fælles portal i f.eks. et intelligent hjemmemiljø og registrere betydelige mængder relevante data om, hvordan brugerne interagerer med produkter, der er forbundet med internettet, også produkter fremstillet af andre parter, og kan overflødig gøre brugen af grænseflader leveret af producenten såsom touchscreens eller smartphoneapplikationer. Brugeren ønsker måske at stille disse data til rådighed for tredjepartsproducenter og drage fordel af nye intelligente tjenester. Virtuelle assistenter bør være omfattet af dataadgangsrettighederne fastsat i denne forordning. Data, der genereres, når en bruger interagerer med et forbundet produkt via en virtuel assistent, der er leveret af en anden enhed end producenten af det forbundne produkt, bør også være omfattet af dataadgangsrettighederne fastsat i denne forordning. Det er imidlertid kun de data, der stammer fra interaktionen mellem brugeren og et forbundet produkt eller en relateret tjeneste via den virtuelle assistent, der bør være omfattet af denne forordning. Data, der er produceret af den virtuelle assistent, og som ikke vedrører anvendelsen af et forbundet produkt eller en relateret tjeneste, er ikke omfattet af denne forordning.
- 24) Inden der indgås en aftale om køb, leje eller leasing af et forbundet produkt, bør sælgeren, udlejeren eller leasinggiveren, som kan være producenten, på en klar og forståelig måde give brugeren oplysninger om de produktdata, som det forbundne produkt er i stand til at generere, herunder typen, formatet og den anslåede mængde af de pågældende data. Dette kan omfatte oplysninger om datastrukturer, dataformater, ordlister, klassifikationsordninger, taksonomier og kodelister, hvis sådanne foreligger, samt klare og tilstrækkelige oplysninger, der er relevante for udøvelsen af brugerens rettigheder, om, hvordan dataene kan lagres, hentes eller tilgås, herunder anvendelsesbetingelser og tjenestekvalitet for programmeringsgrænseflader for applikationer eller i givet fald levering af softwareudviklingssæt. Denne forpligtelse sikrer gennemsigtighed for så vidt angår de genererede produktdata og fremmer let adgang for brugeren. Oplysningspligten kan f.eks. opfyldes ved at have en stabil URL- adresse på internettet, som kan distribueres som et weblink eller en QR-kode

og fører til de relevante oplysninger, som sælgeren, udlejeren eller leasinggiveren, som kan være producenten, kan give brugeren, inden der indgås en aftale om køb, leje eller leasing af et forbundet produkt. Det er under alle omstændigheder nødvendigt at gøre det muligt for brugeren at lagre oplysningerne på en måde, der muliggør senere adgang, og som giver mulighed for uændret gengivelse af de lagrede oplysninger. Dataindehaveren kan ikke forventes at lagre dataene på ubestemt tid i betragtning af de behov, som brugeren af det forbundne produkt har, men bør gennemføre en rimelig dataopbevaringspolitik, i givet fald i overensstemmelse med princippet om opbevaringsbegrænsning i henhold til artikel 5, stk. 1, litra e), i forordning (EU) 2016/679, der giver mulighed for en effektiv anvendelse af dataadgangsrettighederne i henhold til nærværende forordning. Oplysningspligten berører ikke den dataansvarliges forpligtelse til at oplyse den registrerede i henhold til artikel 12, 13 og 14 i forordning (EU) 2016/679. Forpligtelsen til at give oplysninger, inden der indgås en aftale om levering af en relateret tjeneste, bør påhvile den potentielle dataindehaver, uanset om dataindehaveren indgår en aftale om køb, leje eller leasing af et forbundet produkt. Hvis oplysningerne ændres i løbet af det forbundne produkts levetid eller aftaleperioden for den relaterede tjeneste, herunder når det formål, som de pågældende data skal anvendes til, ændres fra det oprindeligt angivne formål, bør de også gives til brugeren.

- 25) Denne forordning bør ikke forstås således, at dataindehaverne tillægges nogen ny ret til at anvende produktdata eller relaterede tjenstedata. Hvis producenten af et forbundet produkt er dataindehaver, bør grundlaget for producentens anvendelse af andre data end personoplysninger være en aftale mellem producenten og brugeren. En sådan aftale kan være en del af en aftale om levering af den relaterede tjeneste, som kan leveres sammen med købs-, leje- eller leasingaftalen vedrørende det forbundne produkt. Ethvert aftalevilkår, der fastsætter, at dataindehaveren kan anvende produktdata eller relaterede tjenstedata, bør være gennemskeligt for brugeren, herunder med hensyn til de formål, som dataindehaveren har til hensigt at anvende dataene til. Sådanne formål kan omfatte forbedring af det forbundne produkts eller de relaterede tjenesters funktion, udvikling af nye produkter eller tjenester eller aggregering af data med henblik på at stille de deraf følgende afledte data til rådighed for tredjeparter, forudsat at sådanne afledte data ikke gør det muligt at identificere specifikke data, der overføres til dataindehaveren fra det forbundne produkt, eller gør det muligt for en tredjepart at aflede de pågældende data af datasættet. Enhver ændring af aftalen bør afhænge af brugerens informerede samtykke. Denne forordning forhindrer ikke parter i at indgå aftale om aftalevilkår, hvis virkning er at udelukke eller begrænse dataindehaverens anvendelse af andre data end personoplysninger eller visse kategorier af andre data end personoplysninger. Den forhindrer heller ikke parter i at indgå aftale om at stille produktdata eller relaterede tjenstedata direkte eller indirekte til rådighed, herunder i givet fald via en anden dataindehaver. Denne forordning forhindrer heller ikke sektorspecifikke reguleringskrav i henhold til EU-ret eller national ret, der er forenelig med EU-retten, som af veldefinerede hensyn til den offentlige orden udelukker eller begrænser dataindehaverens anvendelse af visse sådanne data. Denne forordning er ikke til hinder for, at brugere i forbindelse med relationer mellem virksomheder stiller data til rådighed for tredjeparter eller dataindehavere i henhold til et lovligt aftalevilkår, herunder ved at aftale at begrænse eller indskrænke yderligere deling af sådanne data, eller bliver godtgjort forholdsmæssigt, f.eks. for at give afkald på deres ret til at anvende eller dele de pågældende data. Selv om begrebet »dataindehaver« generelt ikke omfatter offentlige myndigheder, kan det dog omfatte offentlige virksomheder.
- 26) For at fremme udviklingen af likvide, retfærdige og effektive markeder for andre data end personoplysninger bør brugere af forbundne produkter være i stand til at dele data med andre, herunder til kommercielle formål, med en minimal juridisk og teknisk indsats. Det er i øjeblikket ofte vanskeligt for virksomheder at begrunde de personale- eller databehandlingsomkostninger, der er nødvendige for at udarbejde datasæt eller dataprodukter med andre data end personoplysninger og tilbyde dem

til potentielle modparter via dataformidlingstjenester, herunder datamarkeder. En væsentlig hindring for virksomhedernes deling af andre data end personoplysninger skyldes derfor den manglende forudsigelighed med hensyn til det økonomiske udbytte af at investere i kurateringen og tilrådighedsstillelsen af datasæt eller dataprodukter. For at gøre det muligt at skabe likvide, fair og effektive markeder for andre data end personoplysninger i Unionen skal det præciseres, hvilken part der har ret til at tilbyde sådanne data på et marked. Brugere bør derfor have ret til at dele andre data end personoplysninger med datamodtagere til kommercielle og ikkekommercielle formål. En sådan datadeling kan udføres direkte af brugeren, efter anmodning fra brugeren via en dataindehaver eller gennem dataformidlingstjenester. Dataformidlingstjenester som reguleret ved Europa-Parlamentets og Rådets forordning (EU) 2022/868 ⁽²²⁾ kan fremme en dataøkonomi ved at etablere kommercielle forbindelser mellem brugere, datamodtagere og tredjeparter og kan støtte brugerne i udøvelsen af deres ret til at anvende data såsom ved at sikre anonymisering af personoplysninger eller aggregering af adgangen til data fra flere individuelle brugere. Hvis data er udelukket fra en dataindehavers forpligtelse til at stille dem til rådighed for brugere eller tredjeparter, kan omfanget af sådanne data præciseres i aftalen mellem brugeren og dataindehaveren om levering af en relateret tjeneste, således at brugerne let kan afgøre, hvilke data der er til rådighed for dem med henblik på deling med datamodtagere eller tredjeparter. Dataindehavere bør ikke stille andre produktdata end personoplysninger til rådighed for tredjeparter til andre kommercielle eller ikkekommercielle formål end opfyldelsen af deres aftale med brugeren, uden at det berører retlige krav i henhold til EU-retten eller national ret om, at en dataindehaver skal stille data til rådighed. Hvor det er relevant, bør dataindehavere kontraktligt forpligte tredjeparter til ikke at dele data, som de har modtaget fra dem, med andre.

- 27) I de sektorer, der er kendetegnet ved koncentration af et lille antal producenter, der leverer forbundne produkter til slutbrugere, har brugerne måske kun begrænsede muligheder for dataadgang, -anvendelse og -deling. Under sådanne omstændigheder kan kontraktlige aftaler være utilstrækkelige til at nå målet om brugerindflydelse, hvilket gør det vanskeligt for brugerne at opnå værdi af de data, der er genereret af det forbundne produkt, de køber, lejer eller leaser. Der er derfor et begrænset potentiale for, at innovative mindre virksomheder kan tilbyde databaserede løsninger på en konkurrencedygtig måde, og en begrænset mulighed for en mangfoldig dataøkonomi i Unionen. Denne forordning bør derfor bygge på den seneste udvikling i specifikke sektorer såsom adfærdskodeksen for deling af landbrugsdata ved aftale. EU-ret eller national ret kan vedtages for at imødekomme sektorspecifikke behov og mål. Dataindehavere bør endvidere ikke anvende let tilgængelige andre data end personoplysninger til at opnå indsigt i brugerens økonomiske situation, aktiver eller produktionsmetoder eller i brugerens anvendelse på anden vis, som kan underminere den pågældende brugers forretningsmæssige stilling på de markeder, hvor vedkommende er aktiv. Dette kan omfatte anvendelse til skade for brugeren af viden om en virksomheds eller en bedrifts overordnede resultater i kontraktforhandlinger med brugeren om den potentielle erhvervelse af brugerens produkter eller landbrugsprodukter eller anvendelse af sådanne oplysninger i større databaser vedrørende bestemte markeder samlet set, f.eks. databaser over høstudbyttet i den kommende høstsæson, da en sådan anvendelse indirekte kan påvirke brugeren negativt. Brugeren bør have den nødvendige tekniske grænseflade til rådighed til at kunne forvalte tilladelser, helst med detaljerede valgmuligheder, f.eks. »Tillad én gang« eller »Tillad, mens du bruger denne app eller tjeneste«, herunder muligheden for at trække sådanne tilladelser tilbage.
- 28) I aftaler mellem en dataindehaver og en forbruger som bruger af et forbundet produkt eller en relateret tjeneste, der genererer data, finder Unionens forbrugerret, særlig direktiv 93/13/EØF og 2005/29/EF, anvendelse for at sikre, at forbrugeren ikke er underlagt urimelige aftalevilkår. Med henblik på denne forordning bør urimelige aftalevilkår, der ensidigt pålægges en virksomhed, ikke være bindende for den pågældende virksomhed.

- 29) Dataindehavere kan kræve en hensigtsmæssig brugeridentifikation for at kontrollere en brugers ret til at få adgang til dataene. Hvis personoplysninger behandles af en databehandler på vegne af den dataansvarlige, bør dataindehavere sørge for, at anmodningen om adgang modtages og behandles af databehandleren.
- 30) Brugeren bør frit kunne anvende dataene til et hvilket som helst lovligt formål. Dette omfatter levering af de data, som brugeren har modtaget under udøvelsen af sine rettigheder i henhold til denne forordning, til en tredjepart, der udbyder eftersalgsservice, som kan være i konkurrence med en tjeneste, der leveres af en dataindehaver, eller instruks til dataindehaveren om at gøre dette. Anmodningen bør indgives af brugeren eller af en autoriseret tredjepart, der handler på en brugers vegne, herunder en udbyder af en autoriseret dataformidlingstjeneste. Dataindehavere bør sikre, at de data, der stilles til rådighed for tredjepart, er lige så nøjagtige, fuldstændige, pålidelige, relevante og ajourførte som de data, som dataindehaveren selv kan få adgang til eller har ret til at få adgang til i forbindelse med brugen af det forbundne produkt eller den relaterede tjeneste. Alle intellektuelle ejendomsrettigheder bør respekteres i forbindelse med behandlingen af dataene. Det er vigtigt at bevare incitamenterne til at investere i produkter med funktionaliteter baseret på anvendelsen af data fra sensorer, der er indbygget i de pågældende produkter.
- 31) Europa-Parlamentets og Rådets direktiv (EU) 2016/943 ⁽²³⁾ fastsætter, at erhvervelse, brug eller videregivelse af en forretningshemmelighed bl.a. betragtes som lovlig, hvis EU-retten eller national ret kræver eller tillader en sådan erhvervelse, brug eller videregivelse. Selv om denne forordning kræver, at dataindehavere videregiver visse data til brugere eller tredjeparter efter en brugers eget valg, selv når de pågældende data opfylder betingelserne for beskyttelse som forretningshemmeligheder, bør den fortolkes på en sådan måde, at den beskyttelse, der ydes forretningshemmeligheder i henhold til direktiv (EU) 2016/943, bevares. I denne forbindelse bør dataindehavere være i stand til at kræve, at brugere eller tredjeparter efter en brugers eget valg, skal beskytte fortroligheden af data, der betragtes som forretningshemmeligheder. Dataindehavere bør derfor identificere forretningshemmeligheder forud for videregivelsen og have mulighed for at aftale nødvendige foranstaltninger med brugere eller tredjeparter efter en brugers eget valg for at beskytte deres fortrolighed, herunder ved brug af en model for aftalevilkår, fortrolighedsaftaler, strenge adgangsprotokoller, tekniske standarder og anvendelse af adfærdskodekser. Ud over anvendelsen af den model for aftalevilkår, der skal udarbejdes og anbefales af Kommissionen, kan udarbejdelsen af adfærdskodekser og tekniske standarder vedrørende beskyttelse af forretningshemmeligheder i forbindelse med behandlingen af dataene bidrage til at nå målet med denne forordning og bør fremmes. Hvis der ikke foreligger nogen aftale om de nødvendige foranstaltninger, eller hvis en bruger eller tredjeparter efter brugerens eget valg undlader at gennemføre de aftalte foranstaltninger eller bringer fortroligheden af forretningshemmelighederne i fare, bør dataindehaveren kunne tilbageholde eller suspendere delingen af data, der er identificeret som forretningshemmeligheder. I sådanne tilfælde bør dataindehaveren uden unødigt ophold meddele brugeren eller tredjeparten beslutningen skriftligt og underrette den kompetente myndighed i den medlemsstat, hvor dataindehaveren er etableret, om, at vedkommende har tilbageholdt eller suspenderet datadeling, og udpege de foranstaltninger, der ikke er aftalt eller gennemført, og, hvis det er relevant, de forretningshemmeligheder, hvis fortrolighed er bragt i fare. Dataindehavere kan i princippet ikke afslå en anmodning om dataadgang i henhold til denne forordning udelukkende med den begrundelse, at visse data anses som en forretningshemmelighed, eftersom dette ville undergrave de tilsigtede virkninger med denne forordning. Under særlige omstændigheder bør en dataindehaver, der er en forretningshemmelighedshaver, dog fra sag til sag kunne afslå en anmodning om de pågældende specifikke data, hvis vedkommende er i stand til at påvise over for brugeren eller tredjeparten, at videregivelsen af forretningshemmeligheden på trods af tekniske og organisatoriske foranstaltninger truffet af brugeren eller af tredjeparten højst

sandsynligt vil medføre alvorlig økonomisk skade. Alvorlig økonomisk skade indebærer alvorlig og uoprettelig økonomisk tab. Dataindehaveren bør uden unødigt ophold og skriftligt behørigt begrunde sit afslag over for brugeren eller tredjeparten og underrette den kompetente myndighed. En sådan begrundelse bør baseres på objektive forhold, som påviser den konkrete risiko for alvorlig økonomisk skade, der forventes at opstå som følge af en specifik videregivelse af data, og årsagerne til, at de foranstaltninger, der er truffet for at beskytte de ønskede data, ikke anses for at være tilstrækkelige. Der kan i denne forbindelse tages hensyn til en mulig negativ indvirkning på cybersikkerheden. Uden at det berører retten til prøvelse ved en medlemsstats domstol eller ret, hvor brugeren eller en tredjepart ønsker at anfægte dataindehaverens beslutning om at afslå eller om at tilbageholde eller suspendere datadeling, kan brugeren eller tredjeparten indgive en klage til den kompetente myndighed, som uden unødigt ophold bør beslutte, om og på hvilke betingelser datadeling bør påbegyndes eller genoptages, eller kan aftale med dataindehaveren at indbringe sagen for et tvistbilæggelsesorgan. Undtagelserne fra dataadgangsrettighederne i denne forordning bør under ingen omstændigheder begrænse registreredes indsichtsret og ret til dataportabilitet i henhold til forordning (EU) 2016/679.

- 32) Formålet med denne forordning er ikke kun fremme af udviklingen af nye, innovative forbundne produkter og relaterede tjenester og stimulering af innovationen på eftermarkederne, men også stimulering af udviklingen af helt nye tjenester, der gør brug af de pågældende data, bl.a. på grundlag af data fra en række forbundne produkter eller relaterede tjenester. Samtidig sigter denne forordning mod at undgå at underminere investeringsincitamentene for den type forbundet produkt, som dataene stammer fra, f.eks. hvis dataene anvendes til at udvikle et konkurrerende forbundet produkt, som brugerne betragter som indbyrdes udskifteligt og substituerbart, navnlig på grundlag af det forbundne produkts egenskaber, pris og påtænkte anvendelse. Denne forordning indeholder intet forbud mod udvikling af en relateret tjeneste ved hjælp af data, der er opnået i henhold til denne forordning, da dette ville have en uønsket afskrækkende virkning på innovation. Et forbud mod anvendelse af data, der tilgås i henhold til denne forordning, til udvikling af et konkurrerende forbundet produkt beskytter dataindehavernes innovationsindsats. Hvorvidt et forbundet produkt konkurrerer med det forbundne produkt, som dataene stammer fra, afhænger af, om de to forbundne produkter konkurrerer på det samme produktmarked. Dette skal fastslås på grundlag af de i EU-konkurrenceretten fastlagte principper for afgrænsning af det relevante produktmarked. Lovlige formål med anvendelsen af dataene kan dog omfatte reverse engineering, forudsat at den opfylder kravene i denne forordning og i EU-retten eller national ret. Dette kan være tilfældet med henblik på reparation af et forbundet produkt eller forlængelse af dets levetid eller levering af eftersalgsservice for forbundne produkter.
- 33) En tredjepart, som data stilles til rådighed for, kan være en fysisk eller juridisk person såsom en forbruger, en virksomhed, en forskningsinstitution, en nonprofitorganisation eller en enhed, der handler i erhvervsøjemed. Når en dataindehaver stiller data til rådighed for tredjepart, bør dataindehaveren ikke misbruge sin stilling til at opnå en konkurrencemæssig fordel på markeder, hvor dataindehaveren og tredjeparten kan være i direkte konkurrence. Dataindehaveren bør derfor ikke anvende let tilgængelige data til at opnå indsigt i tredjepartens økonomiske situation, aktiver eller produktionsmetoder eller anvendelse på anden vis, som kunne underminere tredjepartens forretningsmæssige stilling på de markeder, hvor tredjeparten er aktiv. Brugeren bør kunne dele andre data end personoplysninger med tredjeparter til kommercielle formål. Efter aftale med brugeren og med forbehold af denne forordnings bestemmelser bør tredjeparter kunne overføre de dataadgangsrettigheder, som brugeren har tildelt andre tredjeparter, herunder mod godtgørelse. Formidlere af data mellem virksomheder og systemer til forvaltning af personoplysninger (PIMS), benævnt dataformidlingstjenester i forordning (EU) 2022/868, kan hjælpe brugere eller tredjeparter med at

etablere kommercielle forbindelser med et ubestemt antal potentielle modparter til ethvert lovligt formål, der falder ind under nærværende forordnings anvendelsesområde. De kan spille en afgørende rolle med hensyn til at aggregere adgang til data, således at analyser af big data eller maskinlæring bliver lettere, forudsat at brugere fortsat har fuld kontrol over, om de vil give deres data til en sådan aggregering, og på hvilke kommercielle vilkår deres data skal anvendes.

- 34) Brugen af et forbundet produkt eller en relateret tjeneste kan, navnlig når brugeren er en fysisk person, generere data, der vedrører den registrerede. Behandlingen af sådanne data er underlagt reglerne i forordning (EU) 2016/679, herunder i tilfælde, hvor personoplysninger og andre data end personoplysninger i et datasæt er uløseligt forbundet. Den registrerede kan være brugeren eller en anden fysisk person. Kun en dataansvarlig eller en registreret kan anmode om personoplysninger. En bruger, der er den registrerede, har under visse omstændigheder i henhold til forordning (EU) 2016/679 ret til at få adgang til personoplysninger om sig selv, og disse rettigheder berøres ikke af nærværende forordning. I henhold til nærværende forordning har en bruger, der er en fysisk person, yderligere ret til at få adgang til alle data, der er genereret af anvendelsen af et forbundet produkt, hvad enten der er tale om personoplysninger eller andre data end personoplysninger. I andre tilfælde end fælles husholdningsbrug af det forbundne produkt skal brugeren, hvis denne ikke er den registrerede, men en virksomhed, herunder en enkeltmandsvirksomhed, betragtes som dataansvarlig. En sådan bruger, der som dataansvarlig har til hensigt at anmode om personoplysninger, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste, skal derfor have et retsgrundlag for behandlingen af oplysningerne som krævet i henhold til artikel 6, stk. 1, i forordning (EU) 2016/679, såsom den registreredes samtykke eller opfyldelse af en aftale, som den registrerede er part i. En sådan bruger bør sikre sig, at den registrerede er behørigt oplyst om de specifikke, eksplicitte og legitime formål med behandlingen af oplysningerne, og om hvordan den registrerede kan udøve sine rettigheder effektivt. Hvis dataindehaveren og brugeren er fælles dataansvarlige som omhandlet i artikel 26 i forordning (EU) 2016/679, er de forpligtet til på gennemsigtig måde ved hjælp af en ordning mellem dem at fastlægge deres relevante ansvar for overholdelse af nævnte forordning. Det bør forstås, at en sådan bruger, når dataene er blevet stillet rådighed, kan blive dataindehaver, hvis den pågældende bruger opfylder kriterierne i nærværende forordning og dermed bliver omfattet af forpligtelsen til at stille data til rådighed i henhold til nærværende forordning.
- 35) Produktdata eller relaterede tjenstedata bør kun stilles til rådighed for en tredjepart efter anmodning fra brugeren. Denne forordning supplerer i overensstemmelse hermed den registreredes ret, der er fastsat i artikel 20 i forordning (EU) 2016/679, til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format samt til at portere disse oplysninger til en anden dataansvarlig, hvis disse oplysninger behandles automatisk på grundlag af artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), eller en aftale i henhold til nævnte forordnings artikel 6, stk. 1, litra b). Registrerede har også ret til at få overført personoplysningerne direkte fra en dataansvarlig til en anden, dog kun hvis det er teknisk muligt. I artikel 20 i forordning (EU) 2016/679 præciseres det, at nævnte artikel vedrører personoplysninger fra den registrerede, men det præciseres ikke, om dette kræver en aktiv adfærd fra den registreredes side, eller om artiklen også finder anvendelse i situationer, hvor et forbundet produkt eller en relateret tjeneste gennem sin udformning observerer den registreredes adfærd eller genererer andre oplysninger vedrørende den registrerede på passiv vis. De rettigheder, der er fastsat i nærværende forordning, supplerer retten til at modtage og portere personoplysninger i henhold til artikel 20 i forordning (EU) 2016/679 på et antal måder. Nærværende forordning giver brugerne ret til at tilgå produktdata eller relaterede tjenstedata og stille dem til rådighed for en tredjepart, uanset om der er tale om personoplysninger, uanset om der er tale om data, der er leveret aktivt eller genereret passivt, og uanset retsgrundlaget for behandlingen. Til forskel fra artikel 20 i forordning (EU) 2016/679 foreskriver og sikrer nærværende forordning

den tekniske gennemførlighed af tredjeparters adgang til alle de typer data, der falder ind under nærværende forordnings anvendelsesområde, uanset om der er tale om personoplysninger eller andre data end personoplysninger, hvorved det sikres, at tekniske hindringer ikke længere vanskeliggør eller står i vejen for adgangen til sådanne data. Ved nærværende forordning gives dataindehavere mulighed for at fastsætte rimelig godtgørelse, der skal betales af tredjepart, men ikke af brugeren, for omkostninger ved at give direkte adgang til de data, der er genereret af brugerens forbundne produkt. Hvis en dataindehaver og en tredjepart ikke kan nå til enighed om vilkårene for en sådan direkte adgang, bør den registrerede på ingen måde forhindres i at udøve de rettigheder, der er fastsat i forordning (EU) 2016/679, herunder retten til dataportabilitet, ved at gøre brug af retsmidler i overensstemmelse med nævnte forordning. Det skal i denne forbindelse forstås, at en aftale i overensstemmelse med forordning (EU) 2016/679 ikke tillader dataindehaverens eller tredjepartens behandling af særlige kategorier af personoplysninger.

- 36) Adgang til data, der er lagret i og tilgås fra terminaludstyr, er omfattet af direktiv 2002/58/EF og kræver abonnentens eller brugerens samtykke som omhandlet i nævnte direktiv, medmindre det er strengt nødvendigt for leveringen af en informationssamfundstjeneste, som brugeren eller abonnenten udtrykkeligt har anmodet om, eller udelukkende med det formål at overføre kommunikation. Med direktiv 2002/58/EF beskyttes integriteten af en brugers terminaludstyr i forbindelse med anvendelsen af behandlings- og opbevaringsfunktioner og indsamlingen af oplysninger. Udstyr vedrørende tingenes internet betragtes som terminaludstyr, hvis det er direkte eller indirekte forbundet med et offentligt kommunikationsnet.
- 37) For at forhindre, at brugerne udnyttes, bør tredjeparter, for hvem der er stillet data til rådighed efter anmodning fra brugeren, kun behandle de pågældende data til de formål, der er aftalt med brugeren, og kun dele dem med en anden tredjepart med brugerens samtykke til en sådan datadeling.
- 38) I overensstemmelse med princippet om dataminimering bør tredjeparter kun få adgang til oplysninger, der er nødvendige for leveringen af den tjeneste, som brugeren har anmodet om. Efter at have fået adgang til dataene bør tredjeparten behandle dem til de formål, der er aftalt med brugeren, uden indblanding fra dataindehaverens side. Det bør være lige så let for brugeren at afvise eller afbryde tredjepartens adgang til dataene, som det er for brugeren at give tilladelse til adgang. Hverken tredjeparter eller dataindehavere bør gøre brugernes udøvelse af valg eller rettigheder unødigt vanskelig, herunder ved at tilbyde brugeren valgmuligheder på en ikkeneutral måde eller ved at tvinge, vildlede eller manipulere brugeren eller undergrave eller begrænse brugerens autonomi, beslutningstagning eller valgmuligheder, herunder ved hjælp af en digital brugergrænseflade eller en del heraf. I denne forbindelse bør tredjeparter eller dataindehavere ikke benytte sig af såkaldte »mørke mønstre« i udformningen af deres digitale grænseflader. Mørke mønstre er designteknikker, der presser eller vildleder forbrugere til at træffe beslutninger, der har negative konsekvenser for dem. Disse manipulerende teknikker kan bruges til at påvirke brugerne, navnlig sårbare forbrugere, til at udvise uønsket adfærd, til at vildlede dem ved at tilskynde dem til at træffe beslutninger om at videregive data eller til på urimelig vis at skævvride tjenestebrugernes beslutningstagning på en sådan måde, at det undergraver eller forringer deres autonomi, beslutningstagning og valgmuligheder. Almindelig og legitim handelspraksis, der overholder EU-retten, bør ikke i sig selv betragtes som mørke mønstre. Tredjeparter og dataindehavere bør overholde deres forpligtelser i henhold til den relevante EU-ret, navnlig kravene i Europa- Parlamentets og Rådets direktiv 98/6/EF ⁽²⁴⁾ og 2000/31/EF ⁽²⁵⁾ samt i direktiv 2005/29/EF og 2011/83/EU.
- 39) Tredjeparter bør også afholde sig fra at anvende data, der er omfattet af denne forordnings anvendelsesområde, til at profilere enkeltpersoner, medmindre sådanne behandlingsaktiviteter er strengt

nødvendige for at levere den tjeneste, som brugeren har anmodet om, herunder i forbindelse med automatiske afgørelser. Kravet om, at data slettes, når de ikke længere er nødvendige til det formål, der er aftalt med brugeren, medmindre andet er aftalt for andre data end personoplysninger, supplerer den registreredes ret til sletning i henhold til artikel 17 i forordning (EU) 2016/679. Hvis en tredjepart er udbyder af en dataformidlingstjeneste, finder foranstaltningerne til beskyttelse af den registrerede i forordning (EU) 2022/868 anvendelse. Tredjeparten kan anvende dataene til at udvikle et nyt og innovativt forbundet produkt eller en ny og innovativ relateret tjeneste, men ikke til at udvikle et konkurrerende forbundet produkt.

- 40) Opstartsvirksomheder, små virksomheder, virksomheder, der er mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, og virksomheder fra traditionelle sektorer med mindre udviklet digital kapacitet har svært ved at få adgang til relevante data. Denne forordning har til formål at lette adgangen til data for disse enheder, samtidig med at de tilsvarende forpligtelser er så forholdsmæssige som muligt for at undgå overdreven regulering. Samtidig er der dukket et lille antal meget store virksomheder op, som har opnået betydelig økonomisk magt i den digitale økonomi gennem akkumulering og aggregering af enorme mængder data, og som har den teknologiske infrastruktur til at udnytte dataene kommercielt. Disse meget store virksomheder omfatter virksomheder, der udbyder centrale platformstjenester, som kontrollerer hele platformsøkosystemer i den digitale økonomi, og som eksisterende eller nye markedsaktører ikke er i stand til at udfordre eller konkurrere med. Europa- Parlamentets og Rådets forordning (EU) 2022/1925 ⁽²⁶⁾ har til formål at afhjælpe disse ineffektiviteter og ubalancer ved at give Kommissionen mulighed for at udpege en virksomhed som en »gatekeeper« og pålægge sådanne gatekeepere en række forpligtelser, bl.a. et forbud mod at kombinere visse data uden samtykke og en forpligtelse til at sikre en effektiv ret til dataportabilitet i overensstemmelse med artikel 20 i forordning (EU) 2016/679. I overensstemmelse med forordning (EU) 2022/1925 og i betragtning af disse virksomheders enestående evne til at erhverve data er det ikke nødvendigt for at nå målet med nærværende forordning at lade retten til dataadgang omfatte gatekeepere, og det ville derfor være uforholdsmæssigt for de dataindehavere, der er underlagt sådanne forpligtelser. En sådan medtagelse vil sandsynligvis også begrænse fordelene ved nærværende forordning for SMV'er i forbindelse med en retfærdig fordeling af dataværdien på tværs af markedsaktørerne. Det betyder, at en virksomhed, der udbyder centrale platformstjenester, og som er udpeget som gatekeeper, ikke kan anmode om eller få adgang til brugerdata, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste eller genereret af en virtuel assistent i henhold til nærværende forordning. Ydermere må tredjeparter, for hvem der er stillet data til rådighed efter anmodning fra brugeren, ikke stille dataene til rådighed for en gatekeeper. F.eks. må tredjeparten ikke give tjenesteleveringen i underentreprise til en gatekeeper. Dette forhindrer dog ikke tredjeparten i at anvende databehandlingstjenester, der udbydes af en gatekeeper. Det forhindrer heller ikke disse virksomheder i at opnå og anvende de samme data på andre lovlige måder. Adgangsrettighederne i nærværende forordning bidrager til et større udvalg af tjenester for forbrugerne. Da frivillige aftaler mellem gatekeepere og dataindehavere ikke berøres, vil begrænsningen af at give gatekeepere adgang ikke udelukke dem fra markedet eller forhindre dem i at udbyde deres tjenester.
- 41) I betragtning af det nuværende teknologiske niveau vil det være alt for byrdefuldt for mikrovirksomheder og små virksomheder at pålægge yderligere designforpligtelser vedrørende forbundne produkter, der fremstilles eller udformes, eller de relaterede tjenester, der leveres, af dem. Det er imidlertid ikke tilfældet, hvor en mikrovirksomhed eller en lille virksomhed har en partnervirksomhed eller en tilknyttet virksomhed som omhandlet i artikel 3 i bilaget til henstilling 2003/361/EF, der ikke er en mikrovirksomhed eller en lille virksomhed, og hvor den er givet fremstillingen eller udformningen af et forbundet produkt eller levering af relaterede tjenester i underentreprise. I disse tilfælde er den

virksomhed, der har udliciteret fremstillingen eller udformningen til en mikrovirksomhed eller en lille virksomhed, i stand til at yde en passende godtgørelse til underleverandøren. En mikrovirksomhed eller en lille virksomhed kan dog være omfattet af kravene i denne forordning som dataindehaver, hvis den ikke er producent af det forbundne produkt eller udbyder af relaterede tjenester. Tilsvarende bør en virksomhed, der har været en mellemstor virksomhed i mindre end ét år, og forbundne produkter i ét år efter den dato, hvorpå de blev bragt i omsætning, nyde godt af en overgangsperiode. En sådan étårsperiode gør det muligt for disse mellemstore virksomheder at tilpasse og forberede sig inden de udsættes for konkurrence på tjenestemarkedet for de forbundne produkter, de fremstiller, på grundlag af adgangsrettigheder i henhold til denne forordning. En sådan overgangsperiode finder ikke anvendelse, hvor en sådan mellemstor virksomhed har en partnervirksomhed eller en tilknyttet virksomhed, der ikke er en mikrovirksomhed eller en lille virksomhed, eller hvor en sådan mellemstor virksomhed er givet fremstillingen eller udformningen af det forbundne produkt eller levering af den relaterede tjeneste i underentreprise.

- 42) Under hensyntagen til den række af forskellige omfattede forbundne produkter, som genererer data af forskellig art, mængde og hyppighed, som frembyder forskellige niveauer af datarelaterede risici og cybersikkerhedsrisici, og som giver økonomiske muligheder af forskellig værdi og med henblik på at sikre konsekvens i datadelingspraksis på det indre marked, herunder på tværs af sektorer, og for at tilskynde til og fremme fair datadelingspraksis, selv på områder, hvor der ikke er fastsat en sådan ret til dataadgang, fastsætter denne forordning horisontale regler om de nærmere ordninger for adgang til data, når en dataindehaver i henhold til EU-retten eller national lovgivning, der er vedtaget i overensstemmelse med EU-retten, er forpligtet til at stille data til rådighed for en datamodtager. En sådan adgang bør være baseret på fair, rimelige, ikkeforskelsbehandlende og gennemsigtige vilkår og betingelser. Disse generelle regler om adgang finder ikke anvendelse på forpligtelser til at stille data til rådighed i henhold til forordning (EU) 2016/679. Frivillig datadeling berøres ikke af disse regler. Den ikkebindende model for aftalevilkår for deling af data mellem virksomheder, som Kommissionen skal udvikle og anbefale, kan hjælpe parterne med at indgå aftaler, som omfatter fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser, og som skal gennemføres på en gennemsigtig måde. Indgåelsen af aftaler, som kan indeholde den ikkebindende model for aftalevilkår, bør ikke betyde, at retten til at dele data med tredjeparter på nogen måde er betinget af, at der foreligger en sådan aftale. Hvis parterne ikke er i stand til at indgå en aftale om datadeling, herunder med støtte fra tvistbilæggelsesorganer, kan retten til at dele data med tredjeparter håndhæves ved de nationale domstole eller retter.
- 43) På grundlag af princippet om aftalefrihed bør parterne fortsat frit kunne forhandle de præcise betingelser for at stille data til rådighed i deres aftaler inden for rammerne af de generelle adgangsregler for tilrådighedsstillelse af data. Vilkårene for sådanne aftaler kan omfatte tekniske og organisatoriske foranstaltninger, herunder i forbindelse med datasikkerhed.
- 44) For at sikre at betingelserne for obligatorisk dataadgang er rimelige for begge parter i en aftale, bør der i de generelle regler om dataadgangsrettigheder henvises til reglen om undgåelse af urimelige aftalevilkår.
- 45) Enhver aftale, der indgås i relationer mellem virksomheder om at stille data til rådighed, bør være ikkeforskelsbehandlende mellem sammenlignelige kategorier af datamodtagere, uanset om parterne er store virksomheder eller SMV'er. For at opveje den manglende viden om betingelserne i forskellige aftaler, hvilket gør det vanskeligt for datamodtageren at vurdere, om betingelserne for at stille dataene til rådighed er ikkeforskelsbehandlende, bør det påhvile dataindehavere at påvise, at et aftalevilkår ikke er forskelsbehandlende. Der er ikke tale om ulovlig forskelsbehandling, når en

dataindehaver anvender forskellige aftalevilkår for at stille data til rådighed, hvis disse forskelle er begrundet i objektive forhold. Disse forpligtelser berører ikke forordning (EU) 2016/679.

- 46) For at fremme fortsat investering i generering og tilrådighedsstillelse af værdifulde data, herunder investeringer i relevante tekniske værktøjer, og samtidig undgå uforholdsmæssigt store byrder for adgangen til og anvendelsen af data, hvilket betyder, at datadelingen ikke længere er kommercielt rentabel, indeholder denne forordning princippet om, at dataindehavere i relationer mellem virksomheder kan anmode om rimelig godtgørelse, når de i henhold til EU-retten eller national lovgivning, der er vedtaget i overensstemmelse med EU-retten, er retligt forpligtede til at stille data til rådighed for en datamodtager. En sådan godtgørelse bør ikke forstås som betaling for selve dataene. Kommissionen bør vedtage retningslinjer for beregningen af en rimelig godtgørelse i dataøkonomien.
- 47) For det første kan en rimelig godtgørelse for opfyldelse af forpligtelsen i henhold til EU-retten eller national lovgivning, der er vedtaget i overensstemmelse med EU-retten, til at imødekomme en anmodning om at stille data til rådighed omfatte godtgørelse for de omkostninger, der er forbundet med at stille dataene til rådighed. Disse omkostninger kan være tekniske omkostninger såsom de omkostninger, der er nødvendige for reproduktion, elektronisk formidling og lagring af dataene, men ikke for indsamlingen eller genereringen af dataene. Sådanne tekniske omkostninger kan også omfatte de omkostninger til behandling, der er nødvendige for at stille dataene til rådighed, herunder de omkostninger, der er forbundet med formatering af dataene. Omkostningerne ved at stille dataene til rådighed kan også omfatte omkostningerne ved at fremme konkrete anmodninger om datadeling. De kan også variere afhængigt af datamængden og de ordninger, der indføres for at stille dataene til rådighed. Langsigtede ordninger mellem dataindehavere og datamodtagere, f.eks. via en abonnementsmodel eller brug af intelligente kontrakter, kan reducere omkostningerne ved regelmæssige eller gentagne transaktioner i en forretningsforbindelse. Omkostninger ved at stille data til rådighed er enten specifikke for en bestemt anmodning eller deles med andre anmodninger. I sidstnævnte tilfælde bør en enkelt datamodtager ikke betale de fulde omkostninger ved at stille dataene til rådighed. For det andet kan rimelig godtgørelse også omfatte en margen, undtagen for så vidt angår SMV'er og nonprofitforskningsinstitutioner. En margen kan variere afhængigt af faktorer, der vedrører selve dataene, såsom dataenes mængde, format eller art. Den kan tage hensyn til omkostningerne ved indsamling af dataene. En margen kan derfor falde, hvis dataindehaveren har indsamlet dataene for sin egen virksomhed uden væsentlige investeringer, eller den kan stige, hvis investeringerne i dataindsamlingen med henblik på dataindehaverens virksomhed er store. Den kan begrænses eller endog udelukkes i situationer, hvor datamodtagerens anvendelse af dataene ikke påvirker dataindehaverens egne aktiviteter. Det forhold, at dataene er samgenererede af et forbundet produkt, der er ejet, lejet eller leaset af brugeren, kan også nedsætte godtgørelsesbeløbet i forhold til andre situationer, hvor dataene genereres af dataindehaveren, f.eks. under leveringen af en relateret tjeneste.
- 48) Det er ikke nødvendigt at gribe ind i tilfælde af datadeling mellem store virksomheder, eller hvor dataindehaveren er en lille virksomhed eller en mellemstor virksomhed, og datamodtageren er en stor virksomhed. I sådanne tilfælde anses virksomhederne for at være i stand til at forhandle om godtgørelsen inden for grænserne af, hvad der er rimeligt og ikkeforskelsbehandlende.
- 49) For at beskytte SMV'er mod uforholdsmæssigt store økonomiske byrder, som ville gøre det for vanskeligt for dem kommercielt at udvikle og drive innovative forretningsmodeller, bør den rimelige godtgørelse for at stille data til rådighed, som de skal betale, ikke overstige de omkostninger, der er direkte forbundet med at stille dataene til rådighed. Direkte forbundne omkostninger er de omkostninger, der kan henføres til individuelle anmodninger, idet der tages hensyn til, at datainde-

haveren permanent skal indføre de nødvendige tekniske grænseflader eller relateret software og konnektivitet. Samme ordning bør gælde for nonprofitforskningsinstitutioner.

- 50) I behørigt begrundede tilfælde, herunder hvis der er behov for at sikre forbrugernes deltagelse og konkurrencen eller for at fremme innovation på bestemte markeder, kan der i EU-retten eller national lovgivning, der er vedtaget i overensstemmelse med EU-retten, fastlægges bestemmelser om reguleret godtgørelse for tilrådighedsstillelse af specifikke typer data.
- 51) Gennemsigtighed er et vigtigt princip for at sikre, at den godtgørelse, som en dataindehaver anmoder om, er rimelig, eller, hvis datamodtageren er en SMV eller en nonprofitforskningsinstitution, at godtgørelsen ikke overstiger de omkostninger, der er direkte forbundet med at stille dataene til rådighed for datamodtageren, og at den kan henføres til den pågældende individuelle anmodning. For at datamodtagere kan vurdere og kontrollere, om godtgørelsen opfylder kravene i denne forordning, bør dataindehaveren give datamodtageren tilstrækkeligt detaljerede oplysninger til at kunne beregne godtgørelsen.
- 52) En sikring af adgangen til alternative metoder til bilæggelse af nationale og grænseoverskridende tvister, der opstår i forbindelse med tilrådighedsstillelse af data, bør være til gavn for dataindehavere og datamodtagere og dermed styrke tilliden til datadeling. Hvis parterne ikke kan nå til enighed om fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser for at stille data til rådighed, bør tvistbilæggelsesorganer tilbyde parterne en enkel, hurtig og billig løsning. Selv om denne forordning kun fastsætter de betingelser, som tvistbilæggelsesorganer skal opfylde for at blive certificeret, står det medlemsstaterne frit for at vedtage eventuelle særlige regler for certificeringsproceduren, herunder certificeringens udløb eller tilbagekaldelse. Bestemmelserne i denne forordning om tvistbilæggelse bør ikke forpligte medlemsstaterne til at oprette tvistbilæggelsesorganer.
- 53) Tvistbilæggelsesproceduren i henhold til denne forordning er en frivillig procedure, der gør det muligt for brugere, dataindehavere og datamodtagere at aftale at indbringe deres tvister for tvistbilæggelsesorganer. Parterne bør derfor frit kunne henvende sig til et tvistbilæggelsesorgan efter eget valg, hvad enten det er i eller uden for de medlemsstater, hvor de pågældende parter er etableret.
- 54) For at undgå tilfælde, hvor to eller flere tvistbilæggelsesorganer inddrages i samme tvist, navnlig i en grænseoverskridende situation, bør et tvistbilæggelsesorgan kunne afvise at behandle en anmodning om bilæggelse af en tvist, der allerede er indbragt for et andet tvistbilæggelsesorgan eller for en medlemsstats domstol eller ret.
- 55) For at sikre en ensartet anvendelse af denne forordning bør tvistbilæggelsesorganerne tage hensyn til den ikkebindende model for aftalevilkår, som Kommissionen skal udvikle og anbefale, samt EU-ret eller national ret, som specificerer forpligtelser, eller retningslinjer vedrørende datadeling, som udstedes af sektormyndigheder med henblik på anvendelsen af sådan ret.
- 56) Parterne i tvistbilæggelsesprocedurer bør ikke forhindres i at udøve deres grundlæggende ret til adgang til effektive retsmidler og en retfærdig rettergang. Beslutningen om at indbringe en tvist for et tvistbilæggelsesorgan bør derfor ikke fratage parterne deres ret til prøvelse ved en medlemsstats domstol eller ret. Tvistbilæggelsesorganer bør offentliggøre årlige aktivitetsrapporter.
- 57) Dataindehavere kan anvende passende tekniske beskyttelsesforanstaltninger for at forhindre ulovlig videregivelse af eller adgang til data. Disse foranstaltninger bør dog hverken forskelsbehandle datamodtagere eller hindre brugeres eller datamodtageres adgang til eller anvendelse af data. I tilfælde af misbrug fra en datamodtagers side såsom vildledning af dataindehaveren ved at give urigtige oplysninger med den hensigt at anvende dataene til ulovlige formål, herunder udvikling af

et konkurrerende forbundet produkt på grundlag af dataene, kan dataindehaveren og, i givet fald og hvor de ikke er den samme person, forretningshemmelighedshaveren eller brugeren anmode tredje-part eller datamodtageren om at gennemføre korrigerende eller afhjælpende foranstaltninger uden unødigt ophold. Alle sådanne anmodninger og navnlig anmodninger om at ophøre med produktion, udbud til salg eller bringen i omsætning af varer, afledte data eller tjenester samt anmodninger om at ophøre med import, eksport eller oplagring af krænkende varer eller tilintetgørelse heraf bør vurderes i lyset af, om de står i et rimeligt forhold til dataindehaverens, forretningshemmelighedshaverens eller brugerens interesser.

- 58) Hvis den ene part befinder sig i en stærkere forhandlingsposition, er der risiko for, at denne part kan udnytte en sådan position til skade for den anden kontraherende part i forhandlinger om adgang til data med det resultat, at adgangen til data er kommercielt mindre rentabel eller endda økonomisk uoverkommelig. Sådanne aftalemæssige skævheder skader alle virksomheder, der ikke har en reel evne til at forhandle betingelserne for adgang til data, og som måske ikke har andet valg end at acceptere »take it or leave it«-aftalevilkår. Urimelige aftalevilkår, der regulerer adgang til og anvendelse af data eller ansvar og retsmidler i forbindelse med tilsidesættelse eller ophør af datarelaterede forpligtelser, bør derfor ikke være bindende for virksomheder, når de pågældende vilkår er blevet pålagt disse virksomheder ensidigt.
- 59) I regler om aftalevilkår bør der tages hensyn til princippet om aftalefrihed som et væsentligt begreb i relationer mellem virksomheder. Derfor bør ikke alle aftalevilkår underkastes en urimelighedsprøve, men kun de vilkår, der ensidigt er pålagt. Det omfatter take it or leave it-situationer, hvor den ene part fremsætter et bestemt aftalevilkår, og den anden virksomhed ikke kan påvirke indholdet af dette vilkår på trods af forsøg på forhandling. Et aftalevilkår, der blot fremsættes af en part og accepteres af den anden virksomhed, eller et vilkår, der forhandles og efterfølgende aftales med ændringer mellem kontraherende parter, bør ikke betragtes som ensidigt pålagt.
- 60) Endvidere bør reglerne om urimelige aftalevilkår kun finde anvendelse på de dele af en aftale, der vedrører tilrådighedsstillelse af data, dvs. aftalevilkår vedrørende adgang til og anvendelse af dataene samt ansvar og retsmidler i forbindelse med tilsidesættelse og ophør af datarelaterede forpligtelser. Andre dele af samme aftale, som ikke vedrører tilrådighedsstillelse af data, bør ikke være underlagt en urimelighedsprøve som fastsat i denne forordning.
- 61) Kriterierne for påvisning af urimelige aftalevilkår bør kun anvendes på vidtgående aftalevilkår, hvor en stærkere forhandlingsposition er blevet misbrugt. Langt de fleste aftalevilkår, der er kommercielt gunstigere for den ene part end for den anden, herunder vilkår, der er sædvanlige i aftaler mellem virksomheder, er et normalt udtryk for princippet om aftalefrihed og finder fortsat anvendelse. I denne forordning vil klar afvigelse fra god handelspraksis bl.a. omfatte objektiv forringelse af muligheden for, at den part, som vilkåret ensidigt er blevet pålagt, kan beskytte sin legitime kommercielle interesse i de pågældende data.
- 62) For at sikre retssikkerheden fastlægges der ved denne forordning en liste med bestemmelser, der altid betragtes som urimelige, og en liste med bestemmelser, som formodes at være urimelige. I sidstnævnte tilfælde bør den virksomhed, der pålægger aftalevilkåret, kunne afkræfte formodningen om, at det er urimeligt, ved at påvise, at det i denne forordning anførte aftalevilkår ikke er urimeligt i det konkrete tilfælde. Hvis et aftalevilkår ikke er medtaget på listen over vilkår, der altid betragtes som urimelige, eller som formodes at være urimelige, finder den generelle bestemmelse om urimelige aftalevilkår anvendelse. I denne forbindelse bør de vilkår, der er opregnet som urimelige aftalevilkår i denne forordning, tjene som målestok for fortolkningen af den generelle bestemmelse om urimelige aftalevilkår. Endelig kan den ikkebindende model for aftalevilkår for aftaler om

datadeling mellem virksomheder, der skal udvikles og anbefales af Kommissionen, også være nyttig for kommercielle parter, når der forhandles aftaler. Hvis et aftalevilkår erklæres urimeligt, bør den pågældende aftale fortsat finde anvendelse uden dette vilkår, medmindre det urimelige aftalevilkår ikke kan udskilles fra aftalens øvrige vilkår.

- 63) I tilfælde, hvor der er et ekstraordinært behov, kan det være nødvendigt for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer under udførelsen af deres lovbestemte opgaver i offentlighedens interesse at anvende eksisterende data, herunder, hvis det er relevant, ledsagende metadata, til at reagere på offentlige nødsituationer eller i andre ekstraordinære tilfælde. Ekstraordinære behov er omstændigheder, der er uforudseelige og tidsbegrænsede, i modsætning til andre omstændigheder, der kan være planlagte, fastlagte, periodiske eller hyppige. Selv om begrebet »dataindehaver« generelt ikke omfatter offentlige myndigheder, kan det omfatte offentlige virksomheder. Forskningsinstitutioner og forskningsfinansierende organisationer kan også organiseres som offentlige myndigheder eller offentligretlige organer. For at begrænse byrden for virksomheder bør mikrovirksomheder og små virksomheder kun være forpligtet til at levere data til offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer i tilfælde af ekstraordinært behov, hvor sådanne data er nødvendige for at reagere på en offentlig nødsituation, og den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet er ikke i stand til rettidigt og effektivt at opnå de pågældende data ved hjælp af alternative midler på tilsvarende betingelser.
- 64) I offentlige nødsituationer såsom folkesundhedsmæssige krisesituationer, nødsituationer som følge af naturkatastrofer, herunder katastrofer, der forværres af klimaændringer og miljøforringelse, samt større menneskeskabte katastrofer såsom større cybersikkerhedsrelaterede hændelser vil offentlighedens interesse i anvendelsen af dataene veje tungere end dataindehavernes interesse i frit at kunne disponere over de data, de er i besiddelse af. I disse tilfælde bør dataindehaverne pålægges en forpligtelse til at stille dataene til rådighed for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer på disses anmodning. Eksistensen af en offentlig nødsituation bør bestemmes eller erklæres i overensstemmelse med EU-retten og national ret og på grundlag af de relevante procedurer, herunder relevante internationale organisationers relevante procedurer. I sådanne tilfælde bør den offentlige myndighed påvise, at de data, der er omfattet af anmodningen, ellers ikke kunne opnås rettidigt og effektivt og på tilsvarende betingelser, f.eks. gennem en anden virksomheds frivillige levering af data eller søgning i en offentlig database.
- 65) Et ekstraordinært behov kan også skyldes situationer, der ikke er nødsituationer. I sådanne tilfælde bør en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ kun kunne anmode om andre data end personoplysninger. Den offentlige myndighed bør påvise, at dataene er nødvendige for udførelsen af en specifik opgave i offentlighedens interesse, som udtrykkeligt er fastsat ved lov, såsom udarbejdelse af officielle statistikker eller afbødning eller genopretning efter en offentlig nødsituation. Desuden kan en sådan anmodning kun fremsættes, når den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ har identificeret specifikke data, der ellers ikke kunne opnås rettidigt og effektivt og på tilsvarende betingelser, og kun hvis den eller det har udtømt alle andre til rådighed stående muligheder for at opnå de pågældende data såsom opnåelse af dataene gennem frivillige aftaler, herunder køb af andre data end personoplysninger på markedet ved at tilbyde markedspriser eller ved at gøre brug af eksisterende forpligtelser til at stille data til rådighed, eller vedtagelse af nye lovgivningsmæssige foranstaltninger, der kan garantere rettidig tilgængelighed af dataene. De betingelser og principper, som regulerer anmodninger, såsom vedrørende formålsbegrænsning, proportionalitet, gennemsigtighed og tidsbegrænsning, bør også finde anvendelse. I tilfælde af anmodninger om data, der er

nødvendige for udarbejdelse af officielle statistikker, bør den anmodende offentlige myndighed også påvise, hvorvidt den nationale ret giver den mulighed for at købe andre data end personoplysninger på markedet.

- 66) Denne forordning bør ikke finde anvendelse på eller foregribe frivillige ordninger for udveksling af data mellem private og offentlige enheder, herunder SMV'ers levering af data, og berører ikke EU-retsakter, der indeholder bestemmelser om offentlige enheders obligatoriske anmodninger om oplysninger fra private enheder. Denne forordning bør ikke berøre dataindehaveres forpligtelser til at levere data, der er begrundede i behov af ikkeekstraordinær karakter, navnlig hvis dataomfanget og dataindehaverne er kendte, eller hvis dataanvendelsen kan finde sted regelmæssigt, som det er tilfældet med indberetningsforpligtelser og forpligtelser vedrørende det indre marked. Denne forordning bør heller ikke berøre krav om dataadgang for at kontrollere overholdelsen af gældende regler, herunder hvor offentlige myndigheder overdrager opgaven med kontrol af overholdelsen til andre enheder end offentlige myndigheder.
- 67) Denne forordning supplerer, og berører ikke, EU-retten og national ret om adgang til og anvendelse af data til statistiske formål, navnlig Europa-Parlamentets og Rådets forordning (EF) nr. 223/2009 ⁽²⁷⁾ samt nationale retsakter vedrørende officielle statistikker.
- 68) Offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer bør med henblik på udførelsen af deres opgaver inden for forebyggelse, efterforskning, afsløring eller retsforfølgning af strafferetlige og administrative overtrædelser, fuldbyrdelse af strafferetlige og administrative sanktioner samt indsamling af data til skatte- eller toldformål gøre brug af deres beføjelser i henhold til EU-retten eller national ret. Denne forordning berører derfor ikke lovgivningsmæssige retsakter vedrørende deling af, adgang til og anvendelse af data på disse områder.
- 69) I overensstemmelse med artikel 6, stk. 1 og 3, i forordning (EU) 2016/679 er en forholdsmæssig, begrænset og forudsigelig ramme på EU-plan nødvendig ved fastsættelsen af retsgrundlaget for, at dataindehavere i tilfælde, hvor der er et ekstraordinært behov, kan stille data til rådighed for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer, både for at sikre retssikkerhed og for at minimere de administrative byrder, der pålægges virksomhederne. Med henblik herpå bør dataanmodninger fra offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer til dataindehavere være specifikke, gennemsigtige og forholdsmæssige i omfang og detaljeringsgrad. Formålet med anmodningen og den påtænkte anvendelse af de data, der anmodes om, bør være konkret og tydeligt forklaret, samtidig med at den anmodende enhed gives tilstrækkelig fleksibilitet til at udføre sine specifikke opgaver i offentlighedens interesse. Anmodningen bør også respektere de legitime interesser hos den dataindehaver, som anmodningen rettes til. Byrden for dataindehaverne bør minimeres ved at forpligte de anmodende enheder til at overholde engangsprincippet, hvilket forhindrer, at de samme data rekvireres flere gange af flere offentlige myndigheder eller Kommissionen, Den Europæiske Centralbank eller EU-organer. For at sikre gennemsigtighed bør dataanmodninger fremsat af Kommissionen, Den Europæiske Centralbank eller EU-organer offentliggøres uden unødigt ophold af den enhed, der anmoder om dataene. Den Europæiske Centralbank og EU-organer bør oplyse Kommissionen om deres anmodninger. Hvis dataanmodningen fremsættes af en offentlig myndighed, bør denne myndighed også underrette datakoordinatoren i den medlemsstat, hvor den offentlige myndighed er etableret. Der bør sikres offentlig onlineadgang til alle anmodninger. Efter modtagelsen af en underretning om en dataanmodning kan den kompetente myndighed beslutte at vurdere anmodningens lovlighed og udøve sine funktioner i forbindelse med håndhævelsen og anvendelsen af denne forordning. Datakoordinatoren bør sikre, at alle anmodninger fremsat af offentlige myndigheder er offentligt tilgængelige online.

- 70) Formålet med forpligtelsen til at levere data er at sikre, at offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer har den nødvendige viden til at reagere på, forebygge eller komme på fode igen efter offentlige nødsituationer eller til at opretholde evnen til at udføre specifikke opgaver, der udtrykkeligt er fastsat ved lov. Sådanne data kan være kommercielt følsomme. Hverken forordning (EU) 2022/868 eller Europa-Parlamentets og Rådets direktiv (EU) 2019/1024 ⁽²⁸⁾ bør derfor finde anvendelse på data, der stilles til rådighed i henhold til nærværende forordning, og som derfor ikke bør betragtes som åbne data, der er til rådighed for tredjeparter med henblik på videreanvendelse. Dette bør dog ikke berøre anvendelsen af direktiv (EU) 2019/1024 på videreanvendelse af officielle statistikker, til hvis udarbejdelse data opnået i henhold til denne forordning er blevet anvendt, forudsat at videreanvendelsen ikke omfatter de underliggende data. Forudsat at betingelserne i nærværende forordning er opfyldt, bør muligheden for datadeling med henblik på forskning eller udvikling, udarbejdelse og formidling af officielle statistikker ikke berøres. Offentlige myndigheder bør også have mulighed for at udveksle data, der er opnået i henhold til nærværende forordning, med andre offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer for at imødekomme de ekstraordinære behov, som afstedkom anmodningen om data.
- 71) Dataindehavere bør have mulighed for enten at afslå en anmodning fremsat af en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ eller at anmode om en ændring heraf uden unødigt ophold og i alle tilfælde inden for en periode på fem eller 30 arbejdsdage afhængigt af arten af det ekstraordinære behov, der gøres gældende i anmodningen. Hvor det er relevant, bør dataindehaveren have denne mulighed, hvis vedkommende ikke har kontrol over de data, der anmodes om, dvs. hvis vedkommende ikke har øjeblikkelig adgang til dataene og ikke kan afgøre, om de er til rådighed. Der bør anses for at være en gyldig grund til ikke at stille dataene til rådighed, hvis det kan påvises, at anmodningen svarer til en tidligere indgivet anmodning til samme formål fra en anden offentlig myndighed eller Kommissionen, Den Europæiske Centralbank eller et EU-organ, og dataindehaveren ikke er blevet underrettet om sletningen af dataene i henhold til denne forordning. En dataindehaver, der afviser anmodningen eller anmoder om ændring heraf, bør meddele begrundelsen herfor til den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ, der anmoder om dataene. Hvis *sui generis*-retten i henhold til Europa-Parlamentets og Rådets direktiv 96/9/EF ⁽²⁹⁾ finder anvendelse i forbindelse med de datasæt, der anmodes om, bør dataindehaverne udøve deres rettigheder på en måde, der ikke forhindrer den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet i at opnå dataene eller dele dem i overensstemmelse med denne forordning.
- 72) I tilfælde af et ekstraordinært behov i forbindelse med en reaktion på en offentlig nødsituation bør de offentlige myndigheder så vidt muligt anvende andre data end personoplysninger. I tilfælde af anmodninger baseret på et ekstraordinært behov, der ikke vedrører en offentlig nødsituation, kan der ikke anmodes om personoplysninger. Når anmodningen omfatter personoplysninger, bør dataindehaveren anonymisere dataene. Hvis det er strengt nødvendigt at medtage personoplysninger i de data, der skal stilles til rådighed for en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ, eller hvis anonymisering viser sig umulig, bør den enhed, der anmoder om dataene, påvise den strenge nødvendighed og de specifikke og begrænsede formål med behandlingen. De gældende regler om beskyttelse af personoplysninger bør overholdes. Tilrådighedsstillelsen og den efterfølgende anvendelse af dataene bør ledsages af garantier for beskyttelse af de berørte fysiske personers rettigheder og interesser.
- 73) Data, der stilles til rådighed for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer på grundlag af et ekstraordinært behov, bør kun anvendes til de formål,

hvortil der blev anmodet om dem, medmindre den dataindehaver, der har stillet dataene til rådighed, udtrykkeligt har indvilliget i, at dataene anvendes til andre formål. Medmindre andet er aftalt, bør dataene slettes, når de ikke længere er nødvendige til de i anmodningen anførte formål, og dataindehaveren bør underrettes herom. Denne forordning er baseret på de eksisterende aktindsigtsordninger i Unionen og medlemsstaterne og ændrer ikke national ret om aktindsigt i forbindelse med gennemsigthedsforpligtelser. Data bør slettes, når de ikke længere er nødvendige for at opfylde sådanne gennemsigthedsforpligtelser.

- 74) Ved videreanvendelse af data, som en dataindehaver leveret, bør offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer overholde både eksisterende gældende EU-ret eller national ret og kontraktlige forpligtelser, som dataindehaveren er underlagt. De bør afholde sig fra at udvikle eller forbedre et forbundet produkt eller en relateret tjeneste, der konkurrerer med dataindehaverens produkt eller tjeneste, og fra at dele dataene med en tredjepart til disse formål. De bør ligeledes give dataindehaverne offentlig anerkendelse efter anmodning og være ansvarlige for at opretholde sikkerheden i forbindelse med de modtagne data. Hvis videregivelse af dataindehaverens forretningshemmeligheder til offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer er strengt nødvendig for at opfylde det formål, hvortil der blev anmodet om data, bør der garanteres fortrolighed forud for videregivelsen af dataene.
- 75) Når det drejer sig om beskyttelse af et vigtigt offentligt gode, f.eks. reaktion på offentlige nødsituationer, bør det ikke forventes, at den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller det pågældende EU-organ godtgør virksomhederne for de opnåede data. Offentlige nødsituationer er sjældne begivenheder, og ikke alle sådanne nødsituationer vil kræve anvendelse af virksomheders data. Samtidig kunne forpligtelsen til at levere data udgøre en betydelig byrde for mikrovirksomheder og små virksomheder. De bør derfor have mulighed for at kræve godtgørelse, selv i forbindelse med en reaktion på en offentlig nødsituation. Dataindehavernes forretningsaktiviteter vil derfor sandsynligvis ikke blive påvirket negativt som følge af, at de offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer anvender denne forordning. Et ekstraordinært behov, som ikke er en reaktion på offentlige nødsituationer, kan forekomme hyppigere, og dataindehavere bør i sådanne tilfælde have ret til en rimelig godtgørelse, som ikke bør overstige de tekniske og organisatoriske omkostninger i forbindelse med at efterkomme anmodningen, og den rimelige margen, der er nødvendig for at stille dataene til rådighed for den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet. Godtgørelsen bør ikke forstås som betaling for selve dataene eller som obligatorisk. Dataindehavere bør ikke kunne kræve godtgørelse, hvis national ret forhindrer nationale statistiske kontorer eller andre nationale myndigheder med ansvar for udarbejdelse af statistikker i at yde godtgørelse til dataindehavere for at stille data til rådighed. Den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller det pågældende EU-organ bør kunne anfægte niveauet for den godtgørelse, som dataindehaveren anmoder om, ved at indbringe sagen for den kompetente myndighed i den medlemsstat, hvor dataindehaveren er etableret.
- 76) Den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ bør være berettiget til at dele de efter anmodning opnåede data med andre enheder eller personer, når dette er nødvendigt for at udføre videnskabelige forsknings- eller analyseaktiviteter, som den eller det ikke selv kan udføre, forudsat at disse aktiviteter er forenelige med det formål, hvortil der er anmodet om data. Den eller det bør rettidigt underrette dataindehaveren om en sådan deling. Sådanne data kan under de samme omstændigheder også deles med de nationale statistiske kontorer og Eurostat med henblik på udvikling, udarbejdelse og formidling af officielle statistikker. Sådanne forskningsaktiviteter bør dog være forenelige med det formål, hvortil der blev anmodet om data, og dataindehaveren

bør underrettes om den videre deling af de data, vedkommende har leveret. Personer, der udfører forskning, eller forskningsinstitutioner, som disse data deles med, bør handle enten uden fortjeneste for øje eller med henblik på at opfylde en almennyttig opgave, der anerkendes af staten. Institutioner bør ikke betragtes som forskningsinstitutioner inden for rammerne af denne forordning, når kommercielle foretagender på grund af strukturelle forhold har en væsentlig indflydelse på dem, der gør det muligt for sådanne foretagender at udøve kontrol, idet dette kan medføre privilegeret adgang til forskningsresultater.

- 77) For at håndtere en grænseoverskridende offentlig nødsituation eller et andet ekstraordinært behov kan dataanmodninger rettes til dataindehavere i andre medlemsstater end den anmodende offentlige myndigheds medlemsstat. I så fald bør den anmodende offentlige myndighed underrette den kompetente myndighed i den medlemsstat, hvor dataindehaveren er baseret, således at den kan behandle anmodningen på grundlag af de kriterier, der er fastsat i denne forordning. Det samme bør gælde anmodninger fra Kommissionen, Den Europæiske Centralbank eller et EU-organ. Hvis der anmodes om personoplysninger, bør den offentlige myndighed underrette det tilsynsorgan, der er ansvarlig for at føre tilsyn med anvendelsen af forordning (EU) 2016/679 i den medlemsstat, hvor den offentlige myndighed er etableret. Den berørte kompetente myndighed bør have ret til at råde den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet til at samarbejde med den offentlige myndighed i den medlemsstat, hvor dataindehaveren er etableret, om behovet for at sikre en minimeret administrativ byrde for dataindehaveren. Når den kompetente myndighed har begrundede indsigelser, hvad angår anmodningens efterlevelse af nærværende forordning, bør den afvise anmodningen fra den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet, som bør tage disse indsigelser i betragtning, inden yderligere tiltag træffes, herunder genindsendelse af anmodningen.
- 78) At kunder til databehandlingstjenester, herunder cloud- og edgetjenester, har mulighed for at skifte fra én databehandlingstjeneste til en anden og samtidig er sikret et minimum af tjenestefunktionalitet uden tjenestenedetid eller for at gøre brug af flere udbyderes tjenester samtidig uden at blive pålagt unødige hindringer og omkostninger til dataoverførsel, er en afgørende forudsætning for et mere konkurrencepræget marked med lavere adgangsbarrierer for nye udbydere af databehandlingstjenester og for at sikre yderligere modstandsdygtighed for brugerne af disse tjenester. Kunder, der nyder fordel af tilbud om gratis niveau, bør også nyde fordel af de bestemmelser om skift, der er fastsat i denne forordning, således at disse tilbud ikke fører til en fastlåst situation for kunderne.
- 79) Europa-Parlamentets og Rådets forordning (EU) 2018/1807 ⁽³⁰⁾ tilskynder udbydere af databehandlingstjenester til at udvikle og effektivt gennemføre selvregulerende adfærdskodekser, der omfatter bedste praksis for bl.a. at lette skift af udbydere af databehandlingstjenester og dataportering. I betragtning af den begrænsede udbredelse af de selvregulerende rammer, der er udviklet som reaktion herpå, og den generelle mangel på åbne standarder og grænseflader er det nødvendigt at vedtage et sæt reguleringsmæssige minimumsforpligtelser for udbydere af databehandlingstjenester for at fjerne prækommercielle, kommercielle, tekniske, kontraktmæssige og organisatoriske hindringer, som ikke er begrænset til nedsat hastighed for dataoverførsel ved kundens exit, hvilket hindrer effektivt skift mellem databehandlingstjenester.
- 80) Databehandlingstjenester bør omfatte tjenester, der giver mulighed for alment tilgængelig on demand- netværksadgang til en konfigurerbar, skalerbar og elastisk fælles pulje af distribuerede databehandlingsressourcer. Disse databehandlingsressourcer omfatter ressourcer såsom netværk, servere eller anden virtuel eller fysisk infrastruktur, software, herunder softwareudviklingsværktøjer, lagring, applikationer og tjenester. Den mulighed, som kunden af databehandlingstjenesten har for ensidigt selvforsynende databehandlingskapacitet, f.eks. servertid eller netlagring, uden nogen menneskelig

interaktion fra udbyderen af databehandlingstjenestens side, kan beskrives som noget, der kræver minimal administration og indebærer minimal interaktion mellem udbyder og kunde. Udtrykket »alment tilgængelig« anvendes til at beskrive den databehandlingskapacitet, der leveres over nettet og tilgås gennem mekanismer, der fremmer brugen af heterogene tynde eller tykke klientplatforme (herunder webbrowsere, mobilenheder og arbejdsstationer). Udtrykket »skalerbar« henviser til databehandlingsressourcer, der fordeles fleksibelt af udbyderen af databehandlingstjenester, uanset ressourcernes geografiske placering, med henblik på at håndtere udsving i efterspørgslen. Udtrykket »elastisk« bruges til at beskrive de databehandlingsressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbelastningen. Udtrykket »fælles pulje« bruges til at beskrive de databehandlingsressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr. Udtrykket »distribueret« anvendes til at beskrive de databehandlingsressourcer, der befinder sig på forskellige netforbundne computere eller enheder, og som kommunikerer og koordinerer indbyrdes ved at sende meddelelser. Udtrykket »stærkt distribueret« anvendes til at beskrive databehandlingstjenester, der indebærer databehandling tættere på det sted, hvor data genereres eller indsamles, f.eks. i en tilsluttet databehandlingsenhed. Edgecomputing, som er en form for stærkt distribueret databehandling, forventes at skabe nye forretningsmodeller og modeller for levering af cloudtjenester, som bør være åbne og interoperable fra starten.

- 81) Det generiske begreb »databehandlingstjenester« dækker et betydeligt antal tjenester med en meget bred vifte af forskellige formål, funktionaliteter og tekniske strukturer. Som det almindeligvis forstås af udbydere og brugere og i overensstemmelse med bredt anvendte standarder falder databehandlingstjenester ind under en eller flere af følgende tre modeller for levering af databehandlingstjenester, nemlig Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) og Software-as-a-Service (SaaS). Disse modeller for levering af tjenester udgør en specifik færdigpakket kombination af IKT-ressourcer, der tilbydes af en udbyder af databehandlingstjenester. Disse tre grundlæggende modeller for levering af databehandlingstjenester suppleres yderligere med nye variationer, der hver især består af en særskilt kombination af IKT-ressourcer såsom Storage-as-a-Service og Database-as-a-Service. Databehandlingstjenester kan kategoriseres mere detaljeret og opdeles i en ikkeudtømmende liste af sæt af databehandlingstjenester, der har det samme primære mål og de samme hovedfunktionaliteter samt den samme type databehandlingsmodeller, som ikke har at gøre med tjenestens operationelle karakteristika (samme tjenestetype). Tjenester, der falder ind under den samme tjenestetype, kan have den samme model for levering af databehandlingstjenester, men to databaser kan synes at have det samme primære formål, men efter betragtning af deres databehandlingsmodel, distributionsmodel og de brugstilfælde, de er rettet mod, kan sådanne databaser falde ind under en mere detaljeret underkategori af lignende tjenester. Tjenester af samme tjenestetype kan have forskellige og konkurrerende karakteristika såsom ydeevne, sikkerhed, modstandsdygtighed og tjenestekvalitet.
- 82) Underminering af udtrækningen af de eksporterbare data, som tilhører kunden, fra kildeudbyderen af databehandlingstjenester kan hindre genoprettelsen af tjenestefunktionaliteterne i infrastruktur hos destinationsudbyderen af databehandlingstjenester. For at lette kundens exitstrategi, undgå unødvendige og byrdefulde opgaver og sikre, at kunden ikke mister nogen af sine data som følge af skifteprocessen, bør kildeudbyderen af databehandlingstjenester på forhånd informere kunden om omfanget af de data, der kan eksporteres, når den pågældende kunde beslutter at skifte til en anden tjeneste, der leveres af en anden udbyder af databehandlingstjenester, eller at flytte til en lokal IKT-infrastruktur. Omfanget af eksporterbare data bør som minimum omfatte de input- og outputdata, herunder metadata, der direkte eller indirekte genereres eller samgenereres ved kundens

anvendelse af databehandlingstjenesten, med undtagelse af alle aktiver eller data tilhørende udbyderen af databehandlingstjenester eller en tredjepart. De eksporterbare data bør udelukke aktiver eller data fra udbydere af databehandlingstjenester eller fra tredjeparten, der er beskyttet af intellektuelle ejendomsrettigheder eller udgør forretningshemmeligheder for den pågældende udbyder eller for den pågældende tredjepart, eller data vedrørende tjenestens integritet og sikkerhed, hvis eksporten vil udsætte udbyderne af databehandlingstjenester for cybersikkerhedssårbarheder. Disse undtagelser bør ikke hindre eller forsinke skifteprocessen.

- 83) Digitale aktiver henviser til elementer i digitalt format, som kunden har brugsret til, herunder applikationer og metadata vedrørende konfigurationen af indstillinger, sikkerhed og forvaltning af adgangs- og kontrolrettigheder, og andre elementer såsom udtryk for virtualiseringsteknologier, herunder virtuelle maskiner og beholdere. Digitale aktiver kan overføres, hvis kunden har brugsret, uafhængigt af kontraktforholdet med den databehandlingstjeneste, som vedkommende ønsker at skifte fra. Disse andre elementer er afgørende for en effektiv anvendelse af kundens data og applikationer i miljøet hos destinationsudbyderen af databehandlingstjenester.
- 84) Denne forordning har til formål at gøre det lettere at skifte mellem databehandlingstjenester, hvilket omfatter de betingelser og handlinger, der er nødvendige for, at en kunde kan opsiges en aftale om en databehandlingstjeneste, indgå en eller flere nye aftaler med forskellige udbydere af databehandlingstjenester og portere sine eksporterbare data og digitale aktiver og i givet fald drage fordel af funktionel ækvivalens.
- 85) Skift er en kundedrevet operation, der består af flere trin, herunder dataudtrækning, hvilket henviser til download af data fra økosystemet hos en kildeudbyder af databehandlingstjenester; transformation, hvis dataene er struktureret på en måde, som ikke matcher bestemmelseslokationens skema; og upload af dataene på en ny destinationslokation. I en specifik situation, der er beskrevet i denne forordning, bør adskillelse af en bestemt tjeneste fra aftalen og flytning af den til en anden udbyder også betragtes som skift. Skifteprocessen forvaltes undertiden af en tredjepartsenhed på kundens vegne. I overensstemmelse hermed bør alle de rettigheder og forpligtelser, som kunden har i henhold til denne forordning, herunder forpligtelsen til at samarbejde i god tro, forstås således, at de finder anvendelse på en sådan tredjepartsenhed under de pågældende omstændigheder. Udbydere af databehandlingstjenester og kunder har forskellige ansvarsområder, alt efter trinnene i den omhandlede proces. Kildeudbyderen af databehandlingstjenester er eksempelvis ansvarlig for at udtrække dataene til et maskinlæsbart format, men det er kunden og destinationsudbyderen af databehandlingstjenester, der skal uploade dataene til det nye miljø, medmindre der er indgået en specifik professionel overgangstjeneste. En kunde, der har til hensigt at udøve de rettigheder i forbindelse med skift, der er fastsat i denne forordning, bør informere kildeudbyderen af databehandlingstjenester om beslutningen om enten at skifte til en anden udbyder af databehandlingstjenester, skifte til en lokal IKT-infrastruktur eller slette den pågældende kundes aktiver og eksporterbare data.
- 86) Ved funktionel ækvivalens forstås, at der på grundlag af kundens eksporterbare data og digitale aktiver genetableres et minimumsniveau af funktionalitet i miljøet hos en ny databehandlingstjeneste af samme tjenestetype efter et skift, hvor destinationsdatabehandlingstjenesten leverer et materielt sammenligneligt resultat som svar på det samme input for delte elementer, der leveres til kunden i henhold til aftalen. Udbydere af databehandlingstjenester kan kun forventes at lette den funktionelle ækvivalens for så vidt angår de elementer, som både kilde- og destinationsdatabehandlingstjenesterne tilbyder uafhængigt. Denne forordning udgør ikke en forpligtelse til at lette den funktionelle ækvivalens for andre udbydere af databehandlingstjenester end dem, der tilbyder tjenester ud fra modellen for levering af IaaS.

- 87) Databehandlingstjenester anvendes på tværs af sektorer og varierer i kompleksitet og tjenestetype. Dette er vigtigt at tage i betragtning med hensyn til porteringsprocessen og tidsrammerne. Ikke desto mindre bør en forlængelse af overgangsperioden på grund af teknisk uigennemfærlighed for at gøre det muligt at gennemføre skifteprocessen inden for den givne tidsramme kun påberåbes i behørigt begrundede tilfælde. Bevisbyrden i denne henseende bør fuldt ud påhvile udbyderen af den pågældende databehandlingstjeneste. Dette berører ikke kundens eneret til at forlænge overgangsperioden en enkelt gang med en periode, som kunden finder mere hensigtsmæssig med henblik på sine egne behov. Kunden kan påberåbe sig denne ret til en forlængelse forud for eller under overgangsperioden under hensyntagen til, at aftalen fortsat finder anvendelse i overgangsperioden.
- 88) Skiftegebyrer er gebyrer, som udbydere af databehandlingstjenester pålægger deres kunder for skifteprocessen. Formålet med disse gebyrer er typisk at lægge omkostninger, som kildeudbyderen af databehandlingstjenester kan påføres som følge af skifteprocessen, over på den kunde, der ønsker at skifte. Almindelige eksempler på skiftegebyrer er omkostninger til overførsel af data fra én udbyder af databehandlingstjenester til en anden eller til en lokal IKT-infrastruktur (gebyrer for udgående dataoverførsel) eller de omkostninger, der påløber for specifikke støttehandlinger under skifteprocessen. Unødvendigt høje gebyrer for udgående dataoverførsel og andre uberettigede gebyrer, som ikke vedrører de faktiske omkostninger ved at skifte, forhindrer kunderne i at skifte, begrænser den frie datastrøm, kan potentielt begrænse konkurrencen og forårsage fastlåsningsvirkninger for kunderne, idet incitamenterne til at vælge en anden eller endnu en udbyder mindskes. Skiftegebyrer bør derfor afskaffes efter tre år fra datoen for denne forordnings ikrafttræden. Udbydere af databehandlingstjenester bør kunne pålægge reducerede skiftegebyrer indtil denne dato.
- 89) En kildeudbyder af databehandlingstjenester bør kunne outsource visse opgaver og godtgøre tredjepartsenheder for at opfylde forpligtelserne i denne forordning. En kunde bør ikke bære omkostningerne ved outsourcing af tjenester, der er indgået af kildeudbyderen af databehandlingstjenester under skifteprocessen, og sådanne omkostninger bør betragtes som uberettigede, medmindre de dækker arbejde, der udføres af udbyderen af databehandlingstjenester på kundens anmodning om yderligere støtte i forbindelse med skifteprocessen, og som ligger ud over udbyderens forpligtelser i forbindelse med et skift som udtrykkeligt fastsat i denne forordning. Intet i denne forordning forhindrer en kunde i at godtgøre tredjepartsenheder for støtte i migrationsprocessen eller parterne i at indgå aftaler om databehandlingstjenester af en bestemt varighed, herunder forholdsmæssige sanktioner for førtidig opsigelse til dækning af sådanne aftalers førtidige opsigelse, i overensstemmelse med EU-retten eller national ret. For at fremme konkurrencen bør den gradvise udfasning af de gebyrer, der er forbundet med at skifte mellem databehandlingstjenester, specifikt omfatte gebyrer for udgående dataoverførsel, som en udbyder af databehandlingstjenester pålægger en kunde. Standardtjenestegebyrer for levering af selve databehandlingstjenesterne er ikke skiftegebyrer. Disse standardtjenestegebyrer er ikke underlagt udfasning og forbliver gældende, indtil aftalen om levering af de relevante tjenester ikke længere finder anvendelse. Denne forordning giver kunden mulighed for at anmode om levering af supplerende tjenester, der er mere vidtgående end udbyderens forpligtelser i forbindelse med et skift i henhold til denne forordning. Disse supplerende tjenester kan udføres og pålægges gebyrer af udbyderen, når de udføres på kundens anmodning, og kunden på forhånd accepterer prisen for de pågældende tjenester.
- 90) Der er behov for en ambitiøs og innovationsfremmende reguleringstilgang til interoperabilitet for at overvinde fastlåsningsproblemer til leverandør, som underminerer konkurrencen og udviklingen af nye tjenester. Interoperabilitet mellem databehandlingstjenester involverer flere brugergrænseflader og infrastruktur- og softwarelag og er sjældent begrænset til en binær test af, om det kan lade sig gøre eller ej. Opbygningen af en sådan interoperabilitet er i stedet underlagt en cost-benefit-analyse,

som er nødvendig for at kunne fastslå, om det kan betale sig at forfølge rimeligt forudsigelige resultater. ISO/IEC 19941:2017 er en vigtig international standard, der udgør en reference for opfyldelsen af målene i denne forordning, da den indeholder tekniske overvejelser, der præciserer kompleksiteten af en sådan proces.

- 91) Hvis udbydere af databehandlingstjenester selv er kunder for så vidt angår databehandlingstjenester hos en tredjepartsudbyder, vil de selv drage fordel af et mere effektivt skift, samtidig med at de forbliver bundet af denne forordnings forpligtelser vedrørende deres egne tjenesteudbud.
- 92) Udbydere af databehandlingstjenester bør forpligtes til at tilbyde al den bistand og støtte inden for rammerne af deres kapacitet og forholdsmæssigt til deres respektive forpligtelser, der er nødvendig for at gøre skiftet til en tjeneste hos en anden udbyder af databehandlingstjenester vellykket, effektivt og sikkert. Denne forordning kræver ikke, at udbydere af databehandlingstjenester udvikler nye kategorier af databehandlingstjenester, herunder inden for eller på grundlag af IKT-infrastrukturen hos andre udbydere af databehandlingstjenester for at sikre funktionel ækvivalens i et andet miljø end deres egne systemer. En kildeudbyder af databehandlingstjenester har ikke adgang til eller indsigt i miljøet hos destinationsudbyderen af databehandlingstjenester. Funktionel ækvivalens bør ikke forstås således, at kildeudbyderen af databehandlingstjenester er forpligtet til at genopbygge den pågældende tjeneste inden for infrastrukturen hos destinationsudbyderen af databehandlingstjenester. I stedet bør kildeudbyderen af databehandlingstjenester træffe alle rimelige foranstaltninger inden for rammerne af sine beføjelser til at lette processen med at opnå funktionel ækvivalens ved at stille kapacitet, fyldestgørende information, dokumentation, teknisk støtte og, hvor det er relevant, de nødvendige værktøjer til rådighed.
- 93) Udbydere af databehandlingstjenester bør også pålægges at fjerne eksisterende hindringer og ikke at pålægge nye hindringer, herunder for kunder, der ønsker at skifte til en lokal IKT-infrastruktur. Hindringer kan bl.a. være af prækommerciel, kommerciel, teknisk, kontraktmæssig eller organisatorisk art. Udbydere af databehandlingstjenester bør også være forpligtet til at fjerne hindringer for adskillelse af en specifik individuel tjeneste fra andre databehandlingstjenester, der leveres i henhold til en aftale, og stille den relevante tjeneste til rådighed med henblik på skift, hvis der ikke foreligger væsentlige og påviste tekniske hindringer, der forhindrer en sådan adskillelse.
- 94) Under hele skifteprocessen bør der opretholdes et højt sikkerhedsniveau. Det betyder, at kildeudbyderen af databehandlingstjenester bør udvide det sikkerhedsniveau, som denne har forpligtet sig til for tjenesten, til at omfatte alle tekniske ordninger, som udbyderen er ansvarlig for under skifteprocessen, såsom netværksforbindelser eller fysiske enheder. Eksisterende rettigheder vedrørende opsigelse af aftaler, herunder dem, der blev indført ved forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv (EU) 2019/770 ⁽³¹⁾, bør ikke berøres. Nærværende forordning bør ikke forstås således, at den forhindrer en udbyder af databehandlingstjenester i at levere nye og forbedrede tjenester, elementer og funktionaliteter til sine kunder eller i at konkurrere med andre udbydere af databehandlingstjenester på det grundlag.
- 95) De oplysninger, som udbydere af databehandlingstjenester skal give kunden, vil kunne understøtte kundens exitstrategi. Disse oplysninger bør omfatte procedurer for iværksættelse af skiftet fra databehandlingstjenesten; de maskinlæsbare dataformater, som brugerens data kan eksporteres til; værktøjerne, der er beregnet til at eksportere data, herunder åbne grænseflader og oplysninger om kompatibilitet med harmoniserede standarder eller fælles specifikationer på grundlag af åbne interoperabilitetsspecifikationer; oplysninger om kendte tekniske restriktioner og begrænsninger, der kunne påvirke skifteprocessen; og den anslåede tid, der er nødvendig for at fuldføre skifteprocessen.

- 96) For at lette interoperabiliteten og et skift mellem databehandlingstjenester bør brugere og udbydere af databehandlingstjenester overveje at anvende gennemførelses- og overholdelsesværktøjer, navnlig dem, der offentliggøres af Kommissionen i form af et EU-regelsæt for skyen og en vejledning om offentlige indkøb af databehandlingstjenester. Navnlig er standardkontraktbestemmelser gavnlige, fordi de øger tilliden til databehandlingstjenester, skaber et mere afbalanceret forhold mellem brugere og udbydere af databehandlingstjenester og forbedrer retssikkerheden med hensyn til de betingelser, der gælder for skift til andre databehandlingstjenester. I denne forbindelse bør brugere og udbydere af databehandlingstjenester overveje at anvende standardkontraktbestemmelser eller andre selvregulerende overholdelsesværktøjer, der er udarbejdet af relevante organer eller ekspertgrupper, der er nedsat i henhold til EU-retten, forudsat at de fuldt ud overholder kravene i denne forordning.
- 97) For at gøre det lettere at skifte mellem databehandlingstjenester bør alle involverede parter, herunder både kilde- og destinationsudbydere af databehandlingstjenester, samarbejde i god tro for at gøre skifteprocessen effektiv og muliggøre en sikker og rettidig overførsel af de nødvendige data i et almindeligt anvendt, maskinlæsbart format og ved hjælp af åbne grænseflader, idet driftsafbrydelser undgås og kontinuitet i tjenesten opretholdes.
- 98) Databehandlingstjenester, der vedrører tjenester, hvis vigtigste elementer for størstedelens vedkommende er skræddersyet til at imødekomme en individuel kundes specifikke behov, eller hvor alle komponenter er udviklet med henblik på en individuel kunde, bør undtages fra nogle af de forpligtelser, der gælder for skift af databehandlingstjeneste. Dette bør ikke omfatte tjenester, som udbyderen af databehandlingstjenester tilbyder i stor kommerciel målestok via sit tjenestekatalog. Det er en af forpligtelserne for udbyderen af databehandlingstjenester forud for indgåelsen af en aftale behørigt at informere potentielle kunder til sådanne tjenester om de forpligtelser i denne forordning, der ikke finder anvendelse på de relevante tjenester. Der er intet til hinder for, at udbyderen af databehandlingstjenester i sidste ende indfører sådanne tjenester i stor målestok, i hvilket tilfælde udbyderen vil skulle opfylde alle forpligtelser i forbindelse med skift i denne forordning.
- 99) I overensstemmelse med minimumskravet om at tillade skift mellem udbydere af databehandlingstjenester har denne forordning også til formål at forbedre interoperabiliteten for parallel anvendelse af flere databehandlingstjenester med komplementære funktionaliteter. Dette vedrører situationer, hvor kunderne ikke opsiger en aftale for at skifte til en anden udbyder af databehandlingstjenester, men hvor flere tjenester fra forskellige udbydere anvendes parallelt og på en interoperabel måde for at drage fordel af de forskellige tjenesters komplementære funktionaliteter i opsætningen af kundens system. Det anerkendes dog, at udgående overførsel af data fra én udbyder af databehandlingstjenester til en anden for at lette den parallelle anvendelse af tjenester kan være en løbende aktivitet i modsætning til den engangsoverførsel af udgående data, der kræves som led i skifteprocessen. Udbydere af databehandlingstjenester bør derfor fortsat kunne pålægge gebyrer for udgående dataoverførsel, der ikke overstiger de afholdte omkostninger, med henblik på parallel anvendelse efter tre år fra datoen for denne forordnings ikrafttræden. Dette er bl.a. vigtigt for en vellykket indførelse af multicloudstrategier, der giver kunderne mulighed for at gennemføre fremtidssikrede IKT-strategier, og som mindsker afhængigheden af individuelle udbydere af databehandlingstjenester. Fremme af en multicloudtilgang for kunder til databehandlingstjenester kan også bidrage til at øge deres digitale operationelle modstandsdygtighed, således som det anerkendes for så vidt angår institutioner, der tilbyder finansielle tjenesteydelser, i Europa-Parlamentets og Rådets forordning (EU) 2022/2554⁽³²⁾.

- 100) Åbne interoperabilitetsspecifikationer og -standards, der er udviklet i overensstemmelse med bilag II til Europa- Parlamentets og Rådets forordning (EU) nr. 1025/2012 ⁽³³⁾ inden for interoperabilitet og portabilitet, forventes at muliggøre et cloudmiljø med flere leverandører, hvilket er et centralt krav til åben innovation i den europæiske dataøkonomi. Da markedsudbredelsen af identificerede standarder under initiativet vedrørende koordinering af cloudstandardisering (CSC), der blev afsluttet i 2016, har været begrænset, er det også nødvendigt, at Kommissionen forlader sig på parterne på markedet med hensyn til at udvikle relevante åbne interoperabilitetsspecifikationer for at holde trit med den hurtige teknologiske udvikling i denne industri. Sådanne åbne interoperabilitets specifikationer kan derefter vedtages af Kommissionen i form af fælles specifikationer. Hvis markedsdrevne processer ikke har været tilstrækkelige til at muliggøre fastsættelsen af fælles specifikationer eller standarder, der fremmer effektiv cloudinteroperabilitet på PaaS- og SaaS-niveau, bør Kommissionen på grundlag af denne forordning og i overensstemmelse med forordning (EU) nr. 1025/2012 endvidere kunne anmode europæiske standardiseringsorganer om at udvikle sådanne standarder for specifikke tjenestetyper, hvor sådanne standarder endnu ikke findes. Derudover vil Kommissionen tilskynde markedsaktørerne til at udvikle relevante åbne interoperabilitetsspecifikationer. Efter høring af de interesserede parter bør Kommissionen ved hjælp af gennemførelsesretsakter kunne fastsætte brugen af harmoniserede standarder for interoperabilitet eller fælles specifikationer for specifikke tjenestetyper gennem en reference i et centralt EU-standardiseringsregister for databehandlingstjenesters interoperabilitet. Udbydere af databehandlingstjenester bør sikre kompatibilitet med disse harmoniserede standarder og fælles specifikationer på grundlag af åbne interoperabilitetsspecifikationer, hvilket ikke bør påvirke datasikkerheden eller -integriteten negativt. Der vil kun blive refereret til harmoniserede standarder for interoperabiliteten af databehandlingstjenester og fælles specifikationer på grundlag af åbne interoperabilitetsspecifikationer, hvis de er i overensstemmelse med kriterierne i denne forordning, som har samme betydning som kravene i bilag II til forordning (EU) nr. 1025/2012 og de interoperabilitetsfacetter, der er defineret i den internationale standard ISO/IEC 19941:2017. Desuden bør standardiseringen tage hensyn til SMV'ers behov.
- 101) Tredjelande kan vedtage love, forskrifter og andre retsakter, der har til formål direkte at overføre eller give statslig adgang til andre data end personoplysninger, der befinder sig uden for deres grænser, herunder i Unionen. En dom afsagt af en domstol eller ret eller en afgørelse truffet af andre judicielle eller administrative myndigheder, herunder retshåndhævende myndigheder, i et tredjeland, ifølge hvilken der pålægges krav om overførsel af eller adgang til andre data end personoplysninger, bør kunne håndhæves, hvis den er baseret på en international aftale såsom en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller en medlemsstat. I andre tilfælde kan der opstå situationer, hvor en anmodning om overførsel af eller adgang til andre data end personoplysninger, der følger af et tredjelandets ret, er i strid med en forpligtelse til at beskytte sådanne data i henhold til EU-retten eller i henhold til den relevante medlemsstats nationale ret, navnlig med hensyn til beskyttelsen af den enkeltes grundlæggende rettigheder såsom retten til sikkerhed og adgang til effektive retsmidler, eller en medlemsstats grundlæggende interesser i forbindelse med national sikkerhed eller forsvar, samt beskyttelse af kommercielt følsomme data, herunder beskyttelse af forretningshemmeligheder, og beskyttelse af intellektuelle ejendomsrettigheder, herunder kontraktlige forpligtelser vedrørende fortrolighed i overensstemmelse med sådan ret. I mangel af internationale aftaler om sådanne spørgsmål bør overførsel eller adgang til andre data end personoplysninger kun tillades, hvis det er blevet verificeret, at tredjelandets retssystem kræver, at begrundelsen for og proportionaliteten af afgørelsen angives, at dommen eller afgørelsen er af specifik karakter, og at en begrundet indsigelse fra adressaten kan prøves ved en kompetent tredjelandsdømstol eller -ret, som har beføjelse til at tage behørigt hensyn til de relevante retlige

interesser hos den, der stiller de pågældende data til rådighed. Når det er muligt i henhold til betingelserne i anmodningen om dataadgang fra tredjelandets myndighed, bør udbyderen af databehandlingstjenester, inden der gives adgang til de pågældende data, kunne informere den kunde, hvis data der anmodes om, med henblik på at kontrollere, om der er en potentiel konflikt mellem en sådan adgang og EU-retten eller national ret, f.eks. retten om beskyttelse af kommercielt følsomme data, herunder beskyttelse af forretningshemmeligheder og intellektuelle ejendomsrettigheder, og de kontraktlige forpligtelser vedrørende fortrolighed.

- 102) For at øge datatilliden er det vigtigt, at der så vidt muligt gennemføres sikkerhedsforanstaltninger, således at unionsborgere, offentlige myndigheder og virksomhederne har kontrol over deres data. Desuden bør EU-retten og Unionens værdier og standarder med hensyn til bl.a. sikkerhed, databeskyttelse og privatlivets fred, og forbrugerbeskyttelse opretholdes. For at forhindre ulovlig statslig adgang til andre data end personoplysninger fra tredjelandsmyndigheders side bør udbydere af databehandlingstjenester, der er omfattet af denne forordning, såsom cloud- og edgetjenester, træffe alle rimelige foranstaltninger for at forhindre adgang til de systemer, hvorpå andre data end personoplysninger er lagret, herunder, hvor det er relevant, gennem kryptering af data, hyppig indgivelse af revisioner, verificeret overholdelse af relevante certificeringsordninger for sikkerhedsgarantier og ændring af virksomhedspolitikker.
- 103) Standardisering og semantisk interoperabilitet bør være i centrum, når der skal tilvejebringes tekniske løsninger til sikring af interoperabilitet inden for og mellem fælles europæiske dataområder, som er formåls- eller sektorspecifikke eller tværsektorielle interoperable rammer for fælles standarder og praksis med hensyn til deling eller fælles behandling af data, bl.a. udvikling af nye produkter og tjenester, videnskabelig forskning eller civilsamfundsinitiativer. Denne forordning fastsætter visse væsentlige krav til interoperabilitet. Deltagere i dataområder, der tilbyder data eller datatjenester til andre deltagere, som er enheder, der letter eller deltager i datadeling inden for fælles europæiske dataområder, herunder dataindehavere, bør opfylde disse krav for så vidt angår elementer, der er under deres kontrol. Overholdelse af disse regler kan sikres ved at opfylde de væsentlige krav, der er fastsat i denne forordning, eller formodes ved at overholde harmoniserede standarder eller fælles specifikationer gennem en formodning om overensstemmelse. For at lette overensstemmelsen med interoperabilitetskravene er det nødvendigt at fastsætte bestemmelser om en formodning om overensstemmelse for interoperabilitetsløsninger, der lever op til harmoniserede standarder eller dele deraf i overensstemmelse med forordning (EU) nr. 1025/2012, som udgør standardrammen for udarbejdelse af standarder, der indeholder bestemmelser om sådanne formodninger. Kommissionen bør vurdere hindringer for interoperabilitet og prioritere standardiseringsbehov, på grundlag af hvilke den kan anmode en eller flere europæiske standardiseringsorganisationer om i henhold til forordning (EU) nr. 1025/2012 at udarbejde harmoniserede standarder, der opfylder de væsentlige krav i nærværende forordning. Hvis sådanne anmodninger ikke fører til harmoniserede standarder, eller de pågældende harmoniserede standarder ikke er tilstrækkelige til at sikre overensstemmelse med de væsentlige krav i nærværende forordning, bør Kommissionen kunne vedtage fælles specifikationer på disse områder, forudsat at den i denne forbindelse behørigt respekterer standardiseringsorganisationernes rolle og funktioner. Fælles specifikationer bør kun vedtages som en ekstraordinær nødløsning for at lette opfyldelsen af de væsentlige krav, der er fastsat i nærværende forordning, eller når standardiseringsprocessen er blokeret, eller når der er forsinkelser i fastlæggelsen af passende harmoniserede standarder. Hvis en sådan forsinkelse skyldes den pågældende standards tekniske kompleksitet, bør Kommissionen tage dette i betragtning, inden det overvejes at udarbejde fælles specifikationer. Fælles specifikationer bør udvikles på en åben og inklusiv måde og, hvor det er relevant, tage hensyn til rådgivningen fra Det Europæiske Datainnovationsråd (EDIB), der er oprettet ved forordning (EU) 2022/868. Desuden kan der vedtages fælles specifikationer

i forskellige sektorer i overensstemmelse med EU-retten eller national ret på grundlag af disse sektors specifikke behov. Endvidere bør Kommissionen have mulighed for at give mandat til udvikling af harmoniserede standarder for databehandlingstjenesters interoperabilitet.

- 104) For at fremme interoperabiliteten mellem værktøjer til automatisk gennemførelse af datadelingsaftaler er det nødvendigt at fastsætte væsentlige krav til intelligente kontrakter, som fagpersoner opretter for andre eller integrerer i applikationer, der understøtter gennemførelsen af aftaler om datadeling. For at lette sådanne intelligente kontraktors overensstemmelse med de væsentlige krav er det nødvendigt at fastsætte bestemmelser om en formodning om overensstemmelse for intelligente kontrakter, der lever op til harmoniserede standarder eller dele deraf i overensstemmelse med forordning (EU) nr. 1025/2012. Begrebet »intelligent kontrakt« i nærværende forordning er teknologineutralt. Intelligente kontrakter kan f.eks. være forbundet med en elektronisk hovedbog. De væsentlige krav bør kun gælde for leverandører af intelligente kontrakter, dog ikke når de udvikler intelligente kontrakter internt udelukkende til intern brug. Det væsentlige krav, der skal sikre, at intelligente kontrakter kan afsluttes og opsiges, indebærer gensidigt samtykke fra parterne i aftalen om datadeling. Anvendelsen af de relevante civil-, aftale- og forbrugerbeskyttelsesretlige regler på datadelingsaftaler berøres ikke eller bør ikke berøres af anvendelsen af intelligente kontrakter med henblik på automatisk gennemførelse af sådanne aftaler.
- 105) For at påvise, at de væsentlige krav i denne forordning er opfyldt, bør leverandøren af en intelligent kontrakt eller, hvis en sådan ikke findes, den person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med gennemførelsen af en aftale eller en del heraf om at stille data til rådighed i forbindelse med denne forordning, foretage en overensstemmelsesvurdering og udstede en EU-overensstemmelseserklæring. En sådan overensstemmelsesvurdering bør være underlagt de generelle principper i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 ⁽³⁴⁾ og Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF ⁽³⁵⁾.
- 106) Ud over forpligtelsen for professionelle udviklere af intelligente kontrakter til at opfylde væsentlige krav er det også vigtigt at tilskynde de deltagere i dataområder, der tilbyder data eller databaserede tjenester til andre deltagere i og på tværs af fælles europæiske dataområder, til at understøtte interoperabiliteten mellem værktøjer til datadeling, herunder intelligente kontrakter.
- 107) For at sikre anvendelse og håndhævelse af denne forordning bør medlemsstaterne udpege en eller flere kompetente myndigheder. Hvis en medlemsstat udpeger mere end én kompetent myndighed, bør den også udpege en datakoordinator iblandt dem. De kompetente myndigheder bør samarbejde med hinanden. De kompetente myndigheder bør gennem udøvelsen af deres undersøgelsesbeføjelser i overensstemmelse med gældende nationale procedurer kunne søge efter og opnå oplysninger, navnlig vedrørende enheders aktiviteter inden for deres kompetence og, herunder i forbindelse med fælles undersøgelser, under behørig hensyntagen til, at tilsyns- og håndhævelsesforanstaltninger vedrørende en enhed, der er underlagt en anden medlemsstats kompetence, bør vedtages af den kompetente myndighed i denne anden medlemsstat, hvor det er relevant i overensstemmelse med procedurerne for grænseoverskridende samarbejde. Kompetente myndigheder bør bistå hinanden rettidigt, navnlig når en kompetent myndighed i en medlemsstat ligger inde med relevante oplysninger med henblik på en undersøgelse foretaget af de kompetente myndigheder i andre medlemsstater eller er i stand til at indsamle sådanne oplysninger, som de kompetente myndigheder i den medlemsstat, hvor enheden er etableret, ikke har adgang til. Kompetente myndigheder og datakoordinatorer bør identificeres i et offentligt register, som Kommissionen fører. Datakoordinatoren vil kunne være et yderligere middel til at lette samarbejdet i grænseoverskridende situationer, såsom når en kompetent myndighed fra en given medlemsstat ikke ved, hvilken myndighed den bør henvende sig til i datakoordinatorens medlemsstat, f.eks. hvis sagen vedrører mere end én

kompetent myndighed eller sektor. Datakoordinatoren bør bl.a. fungere som et enkelt kontaktpunkt for alle spørgsmål vedrørende denne forordnings anvendelse. Hvis der ikke er udpeget nogen datakoordinator, bør den kompetente myndighed påtage sig de opgaver, som datakoordinatoren pålægges i henhold til denne forordning. De myndigheder, der er ansvarlige for at føre tilsyn med overholdelsen af databeskyttelsesretten, og de kompetente myndigheder, der er udpeget i henhold til EU-retten eller national ret, bør være ansvarlige for anvendelsen af denne forordning inden for deres respektive kompetenceområder. For at undgå interessekonflikter bør de kompetente myndigheder, der er ansvarlige for denne forordnings anvendelse og håndhævelse med hensyn til at stille data til rådighed efter en anmodning på grundlag af et ekstraordinært behov, ikke have ret til at indsende en sådan anmodning.

- 108) For at håndhæve deres rettigheder i henhold til denne forordning bør fysiske og juridiske personer have ret til at søge erstatning for krænkelse af deres rettigheder i henhold til denne forordning ved at indgive klager. Datakoordinatoren bør efter anmodning give alle nødvendige oplysninger til fysiske og juridiske personer med henblik på indgivelsen af deres klager til den relevante kompetente myndighed. Disse myndigheder bør have pligt til at samarbejde for at sikre, at en klage effektivt og rettidigt behandles og løses på passende vis. For at gøre brug af forbrugerbeskyttelsesnetværket og muliggøre gruppesøgsmål ændre denne forordning bilagene til Europa-Parlamentets og Rådets forordning (EU) 2017/2394 ⁽³⁶⁾ og Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 ⁽³⁷⁾.
- 109) Kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i denne forordning, er underlagt sanktioner. Sådanne sanktioner kan omfatte økonomiske sanktioner, advarsler, irettesættelser eller påbud om at bringe forretningspraksis i overensstemmelse med forpligtelserne pålagt ved denne forordning. Sanktioner, der fastsættes af medlemsstaterne, bør være effektive, stå i et rimeligt forhold til overtrædelserne og have en afskrækkende virkning og bør tage hensyn til anbefalingerne fra EDIB og dermed bidrage til at opnå den størst mulige grad af konsekvens i fastsættelsen og anvendelsen af sanktioner. De kompetente myndigheder bør, hvor det er relevant, gøre brug af foreløbige forholdsregler for at begrænse virkningerne af en påstået overtrædelse, mens undersøgelsen af den pågældende overtrædelse pågår. I forbindelse hermed bør de bl.a. tage hensyn til overtrædelsens art, grovhed, omfang og varighed set i lyset af de samfundsmæssige hensyn, der varetages, omfanget og arten af de aktiviteter, der udføres, og den krænkende parts økonomiske formåen. De bør også tage hensyn til, om den krænkende part systematisk eller gentagne gange har undladt at opfylde sine forpligtelser i henhold til denne forordning. For at sikre overholdelse af *ne bis in idem*-princippet og navnlig for at undgå, at samme overtrædelse af en forpligtelse fastsat i denne forordning sanktioneres mere end én gang, bør en medlemsstat, der agter at udøve sin kompetence vedrørende en overtrædende part, der ikke er etableret og ikke har udpeget en retlig repræsentant i Unionen, uden unødigt ophold informere alle datakoordinatorer samt Kommissionen.
- 110) EDIB bør rådgive og bistå Kommissionen med at koordinere nationale praksisser og politikker vedrørende de emner, der er omfattet af denne forordning, samt med at opfylde dennes mål i forbindelse med teknisk standardisering for at øge interoperabiliteten. EDIB bør også spille en central rolle med hensyn til at lette omfattende drøftelser mellem de kompetente myndigheder om denne forordnings anvendelse og håndhævelse. Denne udveksling af oplysninger har til formål at øge den effektive adgang til domstolsprøvelse samt håndhævelsen og det retlige samarbejde i hele Unionen. De kompetente myndigheder bør bl.a. gøre brug af EDIB som en platform til at evaluere, koordinere og vedtage anbefalinger om fastsættelsen af sanktioner for overtrædelser af denne forordning. Det bør give de kompetente myndigheder mulighed for med bistand fra Kommissionen at koordinere den optimale tilgang til fastlæggelse og pålæggelse af sådanne sanktioner. Denne

tilgang forhindrer fragmentering, samtidig med at den giver medlemsstaterne fleksibilitet, og bør føre til effektive anbefalinger, der støtter en konsekvent anvendelse af denne forordning. EDIB bør også have en rådgivende rolle i forbindelse med standardiseringsprocesserne og vedtagelsen af fælles specifikationer ved hjælp af gennemførelsesretsakter, i forbindelse med vedtagelsen af delegerede retsakter med henblik på at oprette en overvågningsmekanisme for skiftegebyrer, som udbydere af databehandlingstjenester pålægger, og for yderligere at præcisere de væsentlige krav til interoperabilitet mellem data, mellem datadelingsmekanismer og -tjenester og mellem de fælles europæiske dataområder. Det bør også rådgive og bistå Kommissionen i forbindelse med vedtagelsen af de retningslinjer, der fastsætter interoperabilitetsspecifikationer for driften af de fælles europæiske dataområder.

- 111) For at hjælpe virksomhederne med at udarbejde og forhandle aftaler bør Kommissionen udvikle og anbefale en ikkebindende model for aftalevilkår for aftaler om datadeling mellem virksomheder, om nødvendigt under hensyntagen til betingelserne i specifikke sektorer og den eksisterende praksis med frivillige datadelingsmekanismer. Denne model for aftalevilkår bør først og fremmest være et praktisk redskab, der kan hjælpe især SMV'er med at indgå aftaler. Når denne model for aftalevilkår anvendes bredt og integreret, må den også forventes at have en gavnlig virkning på udformningen af aftaler vedrørende adgang til og anvendelse af data og derfor i bredere forstand føre til mere retfærdige aftaleforhold i forbindelse med adgang til og deling af data.
- 112) For at fjerne risikoen for, at indehavere af data i databaser, der er opnået eller genereret ved hjælp af fysiske komponenter, f.eks. sensorer, af et forbundet produkt og en relateret tjeneste eller andre maskingenererede data, påberåber sig sui generis-retten i henhold til artikel 7 i direktiv 96/9/EF og derved navnlig hindrer brugernes effektive udøvelse af deres ret til at tilgå og anvende data og deres ret til at dele data med tredjeparter i henhold til denne forordning, bør det præciseres, at sui generis-retten ikke finder anvendelse på sådanne databaser. Dette berører ikke den mulige anvendelse af den i artikel 7 i direktiv 96/9/EF fastsatte sui generis-ret på databaser, som indeholder data, der ikke er omfattet af denne forordnings anvendelsesområde, såfremt kravene til beskyttelse i henhold til nævnte artikels stk. 1 er opfyldt.
- 113) For at tage hensyn til de tekniske aspekter af databehandlingstjenester bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for så vidt angår supplerende af denne forordning for at oprette en overvågningsmekanisme for de skiftegebyrer, som udbydere af databehandlingstjenester pålægger på markedet, og for at præcisere de væsentlige interoperabilitetskrav til deltagere i dataområder, der tilbyder data eller datatjenester til andre deltagere. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning⁽³⁸⁾. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.
- 114) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser med hensyn til vedtagelsen af fælles specifikationer for at sikre interoperabilitet mellem data, mellem datadelingsmekanismer og -tjenester og mellem fælles europæiske dataområder, fælles specifikationer for databehandlingstjenesters interoperabilitet, og fælles specifikationer for interoperabilitet mellem intelligente kontrakter. Kommissionen bør også tillægges gennemførelsesbeføjelser med henblik på at offentliggøre gennemførelsesretsakter referencerne for harmoniserede standarder og fælles specifikationer for databehandlingstjenesters interoperabilitet

i et centralt EU-standardiseringsregister for databehandlingstjenesters interoperabilitet. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ⁽³⁹⁾.

- 115) Denne forordning bør ikke berøre regler, der vedrører behov, der er specifikke for individuelle sektorer eller områder af offentlig interesse. Sådanne regler kan omfatte yderligere krav til tekniske aspekter af dataadgangen såsom grænsefladerne for dataadgang, eller hvordan dataadgang kan gives, f.eks. direkte fra produktet eller via dataformidlingstjenester. Sådanne regler kan også omfatte begrænsninger af dataindehavernes ret til adgang til eller anvendelse af brugerdata eller kan omfatte andre aspekter ud over dataadgang og -anvendelse såsom forvaltningsaspekter eller sikkerhedskrav, herunder cybersikkerhedskrav. Denne forordning bør heller ikke berøre mere specifikke regler i forbindelse med udviklingen af fælles europæiske dataområder eller, med de undtagelser, der er fastsat i denne forordning, EU-ret og national ret, der indeholder bestemmelser om adgang til og tilladelse til anvendelse af data til videnskabelige forskningsformål.
- 116) Denne forordning bør ikke berøre anvendelsen af konkurrencereglerne, særlig artikel 101 og 102 i TEUF. Foranstaltningerne i denne forordning bør ikke anvendes til at begrænse konkurrencen på en måde, der er i strid med TEUF.
- 117) For at give aktører inden for denne forordnings anvendelsesområde mulighed for at tilpasse sig de nye regler i denne forordning og træffe de nødvendige tekniske ordninger bør disse regler finde anvendelse fra den 12. september 2025.
- 118) Den Europæiske Tilsynsførende for Databeskyttelse og Det Europæiske Databeskyttelsesråd er blevet hørt i overensstemmelse med artikel 42, stk. 1 og 2, i forordning (EU) 2018/1725 og afgav deres udtalelse den 4. maj 2022.
- 119) Målene for denne forordning, nemlig sikring af fairness i fordelingen af værdi fra data mellem aktører i dataøkonomien og fremme af fair adgang til og anvendelse af data med henblik på at bidrage til at etablere et ægte indre marked for data, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang eller virkninger og grænseoverskridende anvendelse af data bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål —

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Ved denne forordning fastsættes der harmoniserede regler for bl.a.:

- a) tilrådighedsstillelse af produktdata og relaterede tjenstedata for brugeren af det forbundne produkt eller den relaterede tjeneste
- b) dataindehaveres tilrådighedsstillelse af data for datamodtagere
- c) dataindehaveres tilrådighedsstillelse af data for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer, hvis der er et ekstraordinært behov for de pågældende data med henblik på udførelse af en specifik opgave i offentlighedens interesse
- d) lettelse af skift mellem databehandlingstjenester
- e) indførelse af sikkerhedsforanstaltninger mod tredjeparts ulovlige adgang til andre data end personoplysninger, og
- f) sikring af udvikling af interoperabilitetsstandarder for data, der skal tilgås, overføres og anvendes.

2. Denne forordning omfatter personoplysninger og andre data end personoplysninger, herunder følgende datatyper, i følgende sammenhænge:

- a) Kapitel II finder anvendelse på data, bortset fra indhold, vedrørende produkters og relaterede tjenesters ydeevne, anvendelse og omgivelser.
- b) Kapitel III finder anvendelse på data fra den private sektor, der er underlagt lovbestemte forpligtelser vedrørende datadeling.
- c) Kapitel IV finder anvendelse på data fra den private sektor, der tilgås og anvendes på grundlag af aftaler mellem virksomheder.
- d) Kapitel V finder anvendelse på data fra den private sektor med fokus på andre data end personoplysninger.
- e) Kapitel VI finder anvendelse på data og tjenester, der behandles af udbydere af databehandlingstjenester.
- f) Kapitel VII finder anvendelse på andre data end personoplysninger, som udbydere af databehandlingstjenester er i besiddelse af i Unionen.

3. Denne forordning finder anvendelse på:

- a) producenter af forbundne produkter, som bringes i omsætning i Unionen, og udbydere af relaterede tjenester, uanset disse producenters og udbyderes etableringssted

- b) brugere i Unionen af forbundne produkter eller relaterede tjenester, jf. litra a)
- c) dataindehavere, uanset deres etableringssted, der stiller data til rådighed for datamodtagere i Unionen
- d) datamodtagere i Unionen, som dataene stilles til rådighed for
- e) offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer, der anmoder dataindehavere om at stille data til rådighed, hvis der er et ekstraordinært behov for de pågældende data med henblik på udførelse af en specifik opgave i offentlighedens interesse, og de dataindehavere, der leverer disse data som følge af en sådan anmodning
- f) udbydere af databehandlingstjenester, uanset deres etableringssted, der udbyder sådanne tjenester til kunder i Unionen
- g) deltagere i dataområder og leverandører af applikationer, der anvender intelligente kontrakter, og personer, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med gennemførelsen af en aftale.

4. Når der i denne forordning henvises til forbundne produkter eller relaterede tjenester, skal sådanne henvisninger forstås som omfattende også virtuelle assistenter, for så vidt som de interagerer med et forbundet produkt eller en relateret tjeneste.

5. Denne forordning berører ikke EU-retten og national ret om beskyttelse af personoplysninger, privatlivets fred og kommunikationshemmeligheden samt integriteten af terminaludstyr, som finder anvendelse på personoplysninger, der behandles i forbindelse med de rettigheder og forpligtelser, der er fastsat i denne forordning, navnlig forordning (EU) 2016/679 og (EU) 2018/1725 og direktiv 2002/58/EF, herunder tilsynsmyndighedernes beføjelser og kompetencer og de registreredes rettigheder. For så vidt som brugere er registrerede, supplerer de rettigheder, der er fastsat i nærværende forordnings kapitel II, registreredes indsigtret og retten til dataportabilitet i henhold til artikel 15 og 20 i forordning (EU) 2016/679. I tilfælde af uoverensstemmelse mellem nærværende forordning og EU-retten om beskyttelse af personoplysninger eller privatlivets fred eller national ret vedtaget i overensstemmelse med EU-retten har den relevante EU-ret eller nationale ret om beskyttelse af personoplysninger eller privatlivets fred forrang.

6. Denne forordning finder ikke anvendelse på og foregriber heller ikke frivillige ordninger for udveksling af data mellem private og offentlige enheder, navnlig frivillige ordninger for deling af data.

Denne forordning berører ikke EU-retsakter eller nationale retsakter om deling af, adgang til og anvendelse af data med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, eller til told- og skatteformål, navnlig forordning (EU) 2021/784, (EU) 2022/2065 og (EU) 2023/1543 og direktiv (EU) 2023/1544, eller internationalt samarbejde på dette område. Nærværende forordning finder ikke anvendelse på indsamling eller deling af, adgang til eller anvendelse af data i henhold til forordning (EU) 2015/847 og direktiv (EU) 2015/849. Nærværende forordning finder ikke anvendelse på områder, der falder uden for EU-rettens anvendelsesområde, og berører under ingen omstændigheder medlemsstaternes kompetencer vedrørende offentlig sikkerhed, forsvar eller national sikkerhed, uanset hvilken type enhed medlemsstaterne har bemyndiget til at udføre opgaver i forbindelse med disse kompetencer, eller deres beføjelse til at beskytte andre væsentlige statslige

funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden. Nærværende forordning berører ikke medlemsstaternes kompetencer vedrørende told- og skatteforvaltning eller borgernes sundhed og sikkerhed.

7. Denne forordning supplerer selvreguleringstilgangen i forordning (EU) 2018/1807 ved at tilføje alment gældende forpligtelser vedrørende cloudskift.

8. Denne forordning berører ikke EU-retsakter og nationale retsakter om beskyttelse af intellektuelle ejendomsrettigheder, navnlig direktiv 2001/29/EF, 2004/48/EF og (EU) 2019/790.

9. Denne forordning supplerer og berører ikke EU-ret, der har til formål at fremme forbrugernes interesser og sikre et højt forbrugerbeskyttelsesniveau og at beskytte deres sundhed, sikkerhed og økonomiske interesser, navnlig direktiv 93/13/EØF, 2005/29/EF og 2011/83/EU.

10. Denne forordning er ikke til hinder for, at der kan indgås frivillige lovlige datadelingsaftaler, herunder aftaler, der er indgået på et gensidigt grundlag, og som opfylder kravene i denne forordning.

Artikel 2

Definitioner

I denne forordning forstås ved:

- 1) »data«: enhver digital repræsentation af handlinger, kendsgerninger eller oplysninger og enhver samling af sådanne handlinger, kendsgerninger eller oplysninger, herunder i form af lyd- eller videooptagelser eller audiovisuelle optagelser
- 2) »metadata«: en struktureret beskrivelse af indholdet eller anvendelsen af de data, hvormed søgningen i eller anvendelsen af disse data lettes
- 3) »personoplysninger«: personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679
- 4) »andre data end personoplysninger«: data, der ikke er personoplysninger
- 5) »forbundet produkt«: en genstand, som opnår, genererer eller indsamler data vedrørende sin anvendelse eller sine omgivelser, og som er i stand til at kommunikere produktdata via en elektronisk kommunikationstjeneste, en fysisk forbindelse eller adgang på en enhed, og hvis primære funktion ikke er lagring, behandling eller overførsel af data på vegne af andre parter end brugeren
- 6) »relateret tjeneste«: en digital tjeneste, bortset fra en elektronisk kommunikationstjeneste, herunder software, som på købs-, leje- eller leasingtidspunktet er forbundet med produktet på en sådan måde, at fraværet heraf ville forhindre det forbundne produkt i at udføre en eller flere af sine funktioner, eller som

producenten eller en tredjepart efterfølgende har forbundet med produktet for at supplere, ajourføre eller tilpasse det forbundne produkts funktioner

7) »behandling«: enhver aktivitet eller række af aktiviteter, med eller uden brug af automatisk behandling, som data eller datasæt gøres til genstand for, såsom indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, hentning, søgning, brug, videregivelse ved overførsel, formidling eller enhver anden form for tilrådighedsstillelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

8) »databehandlingstjeneste«: en digital tjeneste, der leveres til en kunde, og som muliggør alment tilgængelig og on demand-netværksadgang til en fælles pulje af konfigurerbare, skalerbare og elastiske databehandlingsressourcer af central, distribueret eller stærkt distribueret karakter, og som kan tilvejebringes hurtigt og stilles til rådighed med minimal administrativ indsats eller tjenesteudbyderinteraktion

9) »samme tjenestetype«: en gruppe af databehandlingstjenester, der har samme primære formål, model for levering af databehandlingstjenester og hovedfunktionaliteter

10) »dataformidlingstjeneste«: dataformidlingstjeneste som defineret i artikel 2, nr. 11), i forordning (EU) 2022/868

11) »den registrerede«: den registrerede som omhandlet i artikel 4, nr. 1), i forordning (EU) 2016/679

12) »bruger«: en fysisk eller juridisk person, der ejer et forbundet produkt, eller til hvem midlertidige brugsrettigheder til det forbundne produkt kontraktligt er blevet overdraget, eller som modtager relaterede tjenester

13) »dataindehaver«: en fysisk eller juridisk person, der i overensstemmelse med denne forordning, gældende EU-ret eller national lovgivning, der er vedtaget i overensstemmelse med EU-retten, har ret eller pligt til at anvende data og stille data til rådighed, herunder, hvis det er aftalt, produktdata eller relaterede tjenstedata, som vedkommende har hentet eller genereret under leveringen af en relateret tjeneste

14) »datamodtager«: en fysisk eller juridisk person, der uden at være brugeren af et forbundet produkt eller en relateret tjeneste som led i udøvelsen af sit erhverv, sin forretning, sit håndværk eller sin profession får stillet data til rådighed af dataindehaveren, herunder en tredjepart efter anmodning fra brugeren til dataindehaveren eller i overensstemmelse med en retlig forpligtelse i henhold til EU-retten eller national lovgivning vedtaget i overensstemmelse med EU-retten

15) »produktdata«: data, der er genereret ved brug af et forbundet produkt, som producenten har udformet til via en elektronisk kommunikationstjeneste, en fysisk forbindelse eller adgang på en enhed at kunne hentes af en bruger, dataindehaver eller en tredjepart, herunder, hvis det er relevant, producenten

16) »relaterede tjenstedata«: data, der repræsenterer en digitalisering af brugerhandlinger eller -begivenheder i forbindelse med det forbundne produkt, som registreres bevidst af brugeren eller genereres som et biprodukt af brugerens handling under udbyderens levering af en relateret tjeneste

-
- 17) »let tilgængelige data«: produktdata og relaterede tjenstedata, som en dataindehaver lovligt opnår eller lovligt kan opnå fra det forbundne produkt eller den relaterede tjeneste uden et uforholdsmæssigt stort arbejde, der ikke kan klares som en simpel ekspeditionssag
- 18) »forretningshemmelighed«: en forretningshemmelighed som defineret i artikel 2, nr. 1), i direktiv (EU) 2016/943
- 19) »forretningshemmelighedshaver«: en forretningshemmelighedshaver som defineret i artikel 2, nr. 2), i direktiv (EU) 2016/943
- 20) »profilering«: profilering som defineret i artikel 4, nr. 4), i forordning (EU) 2016/679
- 21) »gøre tilgængelig på markedet«: enhver levering af et forbundet produkt med henblik på distribution, forbrug eller anvendelse på EU-markedet som led i erhvervsvirksomhed, hvad enten det er mod vederlag eller gratis
- 22) »bringe i omsætning«: første tilgængeliggørelse af et forbundet produkt på EU-markedet
- 23) »forbruger«: enhver fysisk person, der ikke handler som led i den pågældende persons erhverv, forretning, håndværk eller profession
- 24) »virksomhed«: en fysisk eller juridisk person, der i forbindelse med aftaler og praksisser, der er omfattet af denne forordning, handler som led i udøvelsen af sit erhverv, sin forretning, sit håndværk eller sin profession
- 25) »lille virksomhed«: en lille virksomhed som defineret i artikel 2, stk. 2, i bilaget til henstilling 2003/361/EF
- 26) »mikrovirksomhed«: en mikrovirksomhed som defineret i artikel 2, stk. 3, i bilaget til henstilling 2003/361/EF
- 27) »EU-organer«: de EU-organer, -kontorer og -agenturer, der er oprettet ved eller i henhold til retsakter vedtaget på grundlag af traktaten om Den Europæiske Union, TEUF eller traktaten om oprettelse af Det Europæiske Atomenergifællesskab
- 28) »offentlig myndighed«: nationale, regionale eller lokale myndigheder i medlemsstaterne, offentligretlige organer i medlemsstaterne, sammenslutninger af en eller flere af disse myndigheder eller et eller flere af disse organer
- 29) »offentlig nødsituation«: en tidsbegrænset ekstraordinær situation såsom en folkesundhedsmæssig krisesituation, en nødsituation som følge af naturkatastrofer eller en større menneskeskabt katastrofe, herunder en større cybersikkerhedsrelateret hændelse, der har negative virkninger for befolkningen i Unionen eller hele eller en del af en medlemsstat, med risiko for alvorlige og varige følgevirkninger for levevilkårene, for den økonomiske stabilitet eller den finansielle stabilitet eller med risiko for en væsentlig og omgående forringelse af Unionens eller den relevante medlemsstats økonomiske aktiver, og

som er konstateret eller officielt erklæret efter de relevante procedurer i overensstemmelse med EU-retten eller national ret

30) »kunde«: en fysisk eller juridisk person, der har indgået et kontraktforhold med en udbyder af databehandlingstjenester med det formål at anvende en eller flere databehandlingstjenester

31) »virtuelle assistenter«: software, der kan behandle instrukser, opgaver eller spørgsmål, herunder sådanne, der er afgivet ved hjælp af lyd, skriftligt input, gestik eller bevægelser, og som baseret på disse instrukser, opgaver eller spørgsmål giver adgang til andre tjenester eller kontrollerer forbundne produkters funktioner

32) »digitale aktiver«: elementer i digitalt format, herunder applikationer, som kunden har brugsret over, uafhængigt af kontraktforholdet med den databehandlingstjeneste, som vedkommende ønsker at skifte fra

33) »lokal IKT-infrastruktur«: IKT-infrastruktur og databehandlingsressourcer, der ejes, lejes eller leases af kunden, og som befinder sig i kundens eget datacenter og drives af kunden eller en tredjepart

34) »skift«: en proces, der involverer en kildeudbyder af databehandlingstjenester, en kunde af en databehandlingstjeneste og, hvor det er relevant, en destinationsudbyder af databehandlingstjenester, hvorved kunden af en databehandlingstjeneste skifter fra at anvende én databehandlingstjeneste til at anvende en anden databehandlingstjeneste af samme tjenestetype eller en anden tjeneste, der tilbydes af en anden udbyder af databehandlingstjenester, eller til en lokal IKT-infrastruktur, herunder ved at udtrække, transformere og uploade dataene

35) »gebyrer for udgående dataoverførsel«: gebyrer for dataoverførsel, der pålægges kunder for at udtrække deres data gennem nettet fra IKT-infrastrukturen hos en udbyder af databehandlingstjenester til systemet hos en anden udbyder eller til lokal IKT-infrastruktur

36) »skiftegebyrer«: gebyrer, bortset fra standardtjenestegebyrer eller sanktioner ved førtidig opsigelse, som en udbyder af databehandlingstjenester pålægger en kunde for de handlinger, der i henhold til denne forordning kræves for at skifte til en anden udbyders system eller til lokal IKT-infrastruktur, herunder gebyrer for udgående dataoverførsel

37) »funktionel ækvivalens«: genetablering på grundlag af kundens eksporterbare data og digitale aktiver af et minimumsniveau af funktionalitet i en ny databehandlingstjenestes miljø af den samme tjenestetype efter skifteprocessen, hvor destinationsdatabehandlingstjenesten leverer et materielt sammenligneligt resultat som svar på det samme input for delte elementer, der leveres til kunden i henhold til aftalen

38) »eksporterbare data« med henblik på artikel 23-31 og 35: de input- og outputdata, herunder metadata, der direkte eller indirekte genereres eller samgenereres ved kundens anvendelse af databehandlingstjenesten, med undtagelse af aktiver eller data, der er beskyttet af intellektuelle ejendomsrettigheder eller udgør en forretningshemmelighed, og som tilhører udbydere af databehandlingstjenester eller tredjeparter

39) »intelligent kontrakt«: et computerprogram, der anvendes til automatisk gennemførelse af en aftale eller en del heraf ved hjælp af en sekvens af elektroniske dataposter, som sikrer deres integritet og nøjagtigheden af deres kronologiske rækkefølge

40) »interoperabilitet«: evnen hos to eller flere dataområder eller kommunikationsnet, systemer, forbundne produkter, applikationer, databehandlingstjenester eller komponenter til at udveksle og anvende data for at kunne udføre deres funktioner

41) »åbne interoperabilitetsspecifikationer«: en teknisk specifikation på området informations- og kommunikationsteknologi, som er resultatorienteret med henblik på at opnå interoperabilitet mellem databehandlingstjenester

42) »fælles specifikationer«: et dokument, der ikke er en standard, og som indeholder tekniske løsninger, der giver mulighed for at opfylde visse krav og forpligtelser fastsat i denne forordning

43) »harmoniseret standard«: en harmoniseret standard som defineret i artikel 2, nr. 1), litra c), i forordning (EU) nr. 1025/2012.

KAPITEL II

DATADELING MELLEM VIRKSOMHEDER OG FORBRUGERE OG MELLEM VIRKSOMHEDER

Artikel 3

Forpligtelse til at gøre produktdata og relaterede tjenstedata tilgængelige for brugeren

1. Forbundne produkter udformes og fremstilles, og relaterede tjenester udformes og leveres, på en sådan måde, at produktdataene og de relaterede tjenstedata, herunder de relevante metadata, der er nødvendige for at fortolke og anvende dataene, som standard på en let og sikker måde gratis og i et fyldestgørende, struktureret, almindeligt anvendt og maskinlæsbart format og, hvis det er relevant og teknisk muligt, er direkte tilgængelige for brugeren.

2. Inden der indgås en aftale om køb, leje eller leasing af et forbundet produkt, skal sælgeren, udlejerens eller leasinggiveren, som kan være producenten, som minimum give brugeren følgende oplysninger på en klar og forståelig måde:

a) typen, formatet og den anslåede mængde af produktdata, som det forbundne produkt er i stand til at generere

b) hvorvidt det forbundne produkt er i stand til at generere data kontinuerligt og i realtid

c) hvorvidt det forbundne produkt er i stand til at lagre data på enheden eller på en fjernserver, herunder i givet fald den planlagte varighed af opbevaringen

d) hvordan brugeren kan tilgå, hente eller, hvor det er relevant, slette dataene, herunder de tekniske midler til at gøre dette, samt betingelserne for deres anvendelse og tjenestekvalitet.

3. Inden der indgås en aftale om levering af en relateret tjeneste, skal udbyderen af en sådan relateret tjeneste som minimum give brugeren følgende oplysninger på en klar og forståelig måde:

a) arten og den anslåede mængde af og indsamlingshyppigheden for de produktdata, som den potentielle dataindehaver forventes at opnå, og, hvor det er relevant, ordningerne for brugerens adgang til eller hentning af de pågældende data, herunder den potentielle dataindehavers lagringsordninger og varigheden af opbevaring

b) arten og den anslåede mængde af relaterede tjenstedata, der skal genereres, samt ordningerne for brugerens adgang til eller hentning af de pågældende data, herunder den potentielle dataindehavers lagringsordninger og varigheden af opbevaring

c) hvorvidt den potentielle dataindehaver forventer at anvende let tilgængelige data selv og de formål, hvortil disse data skal anvendes, og hvorvidt vedkommende har til hensigt at tillade en eller flere tredjeparter at anvende dataene til formål, der er aftalt med brugeren

d) den potentielle dataindehavers identitet såsom firmanavn og firmaets fysiske adresse og i givet fald tilsvarende for andre databehandlingsparter

e) hvilke kommunikationsmidler der gør det muligt hurtigt at kontakte den potentielle dataindehaver og kommunikere effektivt med denne

f) hvordan brugeren kan anmode om, at dataene deles med en tredjepart, og i givet fald bringe datadelingen til ophør

g) brugerens ret til at indgive en klage over en overtrædelse af en af dette kapitels bestemmelser til den kompetente myndighed, der er udpeget i henhold til artikel 37

h) hvorvidt en potentiel dataindehaver er indehaver af forretningshemmeligheder, som er indeholdt i de data, der er tilgængelige fra det forbundne produkt eller genereret under leveringen af en relateret tjeneste, og, hvis den potentielle dataindehaver ikke er forretningshemmelighedsindehaveren, forretningshemmelighedshaverens identitet

i) varigheden af aftalen mellem brugeren og den potentielle dataindehaver samt ordningerne for opsigelse af en sådan aftale.

Artikel 4

Brugeres og dataindehaveres rettigheder og forpligtelser for så vidt angår at tilgå og anvende produktdata og relaterede tjenstedata og stille dem til rådighed

1. Hvis brugeren ikke direkte kan tilgå data fra det forbundne produkt eller den relaterede tjeneste, gør dataindehaverne let tilgængelige data og de relevante metadata, der er nødvendige for at fortolke og anvende disse data, tilgængelige for brugeren uden unødigt ophold, i samme kvalitet som dataindehaveren har til rådighed, på en let og sikker måde, gratis og i et fyldestgørende, struktureret, almindeligt anvendt og maskinlæsbart format og, hvis det er relevant og teknisk muligt, kontinuerligt og i realtid. Dette skal ske på grundlag af en simpel anmodning ad elektronisk vej, hvor det er teknisk muligt.

2. Brugere og dataindehavere kan indgå aftale om at begrænse eller forbyde adgang til eller anvendelse eller yderligere deling af data, hvis en sådan behandling kan underminere det forbundne produkts sikkerhedskrav, der er fastsat i EU-retten eller national ret, med en alvorlig negativ virkning for fysiske personers sundhed og sikkerhed. Sektormyndigheder kan yde brugere og dataindehavere teknisk ekspertise i denne forbindelse. Hvis dataindehaveren afslår at dele data i henhold til denne artikel, underretter vedkommende den kompetente myndighed, der er udpeget i henhold til artikel 37.

3. Uden at det berører brugerens ret til prøvelse ved en medlemsstats domstol eller ret på et hvilket som helst tidspunkt, kan brugeren i forbindelse med enhver tvist med dataindehaveren vedrørende de kontraktlige begrænsninger eller forbud, der er omhandlet i stk. 2:

a) indgive klage til den kompetente myndighed i overensstemmelse med artikel 37, stk. 5, litra b), eller

b) aftale med dataindehaveren, at sagen indbringes for et tvistbilæggelsesorgan i overensstemmelse med artikel 10, stk. 1.

4. Dataindehavere må ikke gøre brugerens udøvelse af valgmuligheder eller rettigheder i henhold til denne artikel unødigt vanskelig, herunder ved at tilbyde brugerne valgmuligheder på en ikkeneutral måde eller ved at undergrave eller begrænse brugerens autonomi, beslutningstagning eller valgmuligheder via den måde, som en digital brugergrænseflade eller en del heraf er struktureret, udformet, fungerer eller betjenes på.

5. For at fastslå om en fysisk eller juridisk person er en bruger med henblik på stk. 1 må en dataindehaver ikke kræve, at denne person skal fremlægge oplysninger ud over, hvad der er nødvendigt. Dataindehavere må ikke opbevare oplysninger, navnlig logdata, om brugerens adgang til de ønskede data ud over, hvad der er nødvendigt for en forsvarlig udførelse af brugerens anmodning om adgang og af hensyn til sikkerheden og vedligeholdelsen af datainfrastrukturen.

6. Forretningshemmeligheder skal beskyttes og må kun videregives, hvis dataindehaveren og brugeren forud for videregivelsen træffer alle nødvendige foranstaltninger for at beskytte deres fortrolighed, navnlig over for tredjeparter. Dataindehaveren eller, når det ikke er den samme person, forretningshemmelighedshaveren identificerer de data, der er beskyttet som forretningshemmeligheder, herunder i de relevante metadata, og aftaler med brugeren forholdsmæssige tekniske og organisatoriske foranstaltninger, der er nødvendige for at beskytte fortroligheden af de delte data, navnlig over for tredjeparter, såsom en model for aftalevilkår, fortrolighedsaftaler, strenge adgangsprotokoller, tekniske standarder og anvendelse af adfærdskodekser.

7. Hvis der ikke foreligger nogen aftale om de nødvendige foranstaltninger omhandlet i stk. 6, eller hvis brugeren undlader at gennemføre de foranstaltninger, der er aftalt i henhold til stk. 6, eller undergraver

fortroligheden af forretningshemmeligheder, kan dataindehaveren tilbageholde eller i givet fald suspendere delingen af data, der er identificeret som forretningshemmeligheder. Dataindehaverens beslutning skal være behørigt begrundet og meddeles brugeren skriftligt uden unødigt ophold. I sådanne tilfælde underretter dataindehaveren den kompetente myndighed, der er udpeget i henhold til artikel 37, om, at den har tilbageholdt eller suspenderet datadeling, og udpeger de foranstaltninger, der ikke er aftalt eller gennemført, og, hvis det er relevant, de forretningshemmeligheder, hvis fortrolighed er undergravet.

8. Under ekstraordinære omstændigheder, hvor dataindehaveren, der er forretningshemmelighedshaver, kan påvise, at vedkommende højst sandsynligt vil lide alvorlig økonomisk skade som følge af videregivelsen af forretningshemmeligheder på trods af de tekniske og organisatoriske foranstaltninger, som brugeren har truffet i henhold til denne artikels stk. 6, kan den pågældende dataindehaver fra sag til sag afslå en anmodning om adgang til de pågældende specifikke data. Denne påvisning skal være behørigt begrundet i objektive forhold, navnlig muligheden for at håndhæve beskyttelsen af forretningshemmeligheder i tredjelande, arten og graden af fortrolighed for de ønskede data og det forbundne produkts unikke og nyskabende karakter, og skal gives brugeren skriftligt uden unødigt ophold. Hvor dataindehaveren afslår at dele data i henhold til nærværende stykke, underretter vedkommende den kompetente myndighed, der er udpeget i henhold til artikel 37.

9. Uden at dette berører en brugers ret til prøvelse ved en medlemsstats domstol eller ret på et hvilket som helst tidspunkt, kan en bruger, der ønsker at anfægte en dataindehavers beslutning om at afslå eller om at tilbageholde eller suspendere datadelingen i henhold til stk. 7 og 8:

a) i overensstemmelse med artikel 37, stk. 5, litra b), indgive klage til den kompetente myndighed, som uden unødigt ophold skal beslutte, om og på hvilke betingelser datadelingen skal påbegyndes eller genoptages, eller

b) aftale med dataindehaveren, at sagen indbringes for et tvistbilæggelsesorgan i overensstemmelse med artikel 10, stk. 1.

10. Brugeren må ikke anvende de data, der er opnået på grundlag af en anmodning omhandlet i stk. 1, til at udvikle et forbundet produkt, der konkurrerer med det forbundne produkt, som dataene stammer fra, og heller ikke dele dataene med en tredjepart med henblik herpå og må ikke anvende de pågældende data til at opnå indsigt i producentens eller i givet fald dataindehaverens økonomiske situation, aktiver og produktionsmetoder.

11. Brugeren må ikke anvende tvangsmidler eller misbruge mangler i en dataindehavers tekniske databeskyttelsesinfrastruktur for at få adgang til data.

12. Hvis brugeren ikke er den registrerede, hvis personoplysninger der anmodes om, må alle personoplysninger, der er genereret ved brug af et forbundet produkt eller en relateret tjeneste, kun stilles til rådighed af dataindehaveren for brugeren, hvis der er et gyldigt retsgrundlag for behandling i henhold til artikel 6 i forordning (EU) 2016/679, og, hvor det er relevant, betingelserne i artikel 9 i nævnte forordning og i artikel 5, stk. 3, i direktiv 2002/58/EF er opfyldt.

13. En dataindehaver må kun anvende let tilgængelige andre data end personoplysninger, på grundlag af en aftale med brugeren. En dataindehaver må ikke anvende sådanne data til at opnå indsigt i brugerens

økonomiske situation, aktiver og produktionsmetoder eller anvendelse af disse på en anden måde, som kunne underminere denne brugers forretningsmæssige stilling på de markeder, hvor brugeren er aktiv.

14. Dataindehavere må ikke stille andre produktdata end personoplysninger til rådighed for tredjeparter til andre kommercielle eller ikkekommercielle formål end opfyldelsen af deres aftale med brugeren. Hvor det er relevant, forpligter dataindehavere kontraktligt tredjeparter til ikke at dele data, som de har modtaget fra dem, med andre.

Artikel 5

Brugerens ret til at dele data med tredjeparter

1. Efter anmodning fra en bruger eller en part, der handler på dennes vegne, stiller dataindehaveren let tilgængelige data og de relevante metadata, der er nødvendige for at fortolke og anvende disse data, til rådighed for en tredjepart uden unødigt ophold, i samme kvalitet som dataindehaveren har til rådighed, på en let og sikker måde, gratis for brugeren, i et fyldestgørende, struktureret, almindeligt anvendt og maskinlæsbart format og, hvis det er relevant og teknisk muligt, kontinuerligt og i realtid. Dataene stilles til rådighed af dataindehaveren for tredjeparten i overensstemmelse med artikel 8 og 9.

2. Stk. 1 finder ikke anvendelse på let tilgængelige data i forbindelse med afprøvning af nye forbundne produkter, stoffer eller processer, der endnu ikke er blevet bragt i omsætning, medmindre en tredjeparts anvendelse heraf er kontraktligt tilladt.

3. Enhver virksomhed, der er udpeget som gatekeeper i henhold til artikel 3 i forordning (EU) 2022/1925, må ikke være en berettiget tredjepart i henhold til nærværende artikel og må derfor ikke:

a) på nogen måde anmode en bruger om eller kommercielt tilskynde en bruger til, herunder ved at yde økonomisk eller anden godtgørelse, at stille data, som brugeren har opnået på grundlag af en anmodning i henhold til artikel 4, stk. 1, til rådighed for en af virksomhedens tjenester

b) anmode eller kommercielt tilskynde en bruger til at anmode dataindehaveren om at stille data til rådighed for en af virksomhedens tjenester i henhold til denne artikels stk. 1

c) modtage data fra en bruger, som brugeren har opnået på grundlag af en anmodning i henhold til artikel 4, stk. 1.

4. For at fastslå om en fysisk eller juridisk person er en bruger eller en tredjepart med henblik på stk. 1 er brugeren eller tredjeparten ikke forpligtet til at fremlægge oplysninger ud over, hvad der er nødvendigt. Dataindehavere må ikke opbevare oplysninger om tredjepartens adgang til de ønskede data ud over, hvad der er nødvendigt for en forsvarlig udførelse af tredjepartens anmodning om adgang og af hensyn til sikkerheden og vedligeholdelsen af datainfrastrukturen.

5. Tredjeparten må ikke anvende tvangsmidler eller misbruge mangler i en dataindehavers tekniske databeskyttelsesinfrastruktur for at få adgang til data.

6. En dataindehaver må ikke anvende let tilgængelige data til at opnå indsigt i tredjepartens økonomiske situation, aktiver og produktionsmetoder eller anvendelse af disse på en anden måde, som kan underminere tredjepartens forretningsmæssige stilling på de markeder, hvor tredjeparten er aktiv, medmindre tredjeparten har givet tilladelse til en sådan anvendelse og har teknisk mulighed for let at trække tilladelsen tilbage på et hvilket som helst tidspunkt.

7. Hvis brugeren ikke er den registrerede, hvis personoplysninger der anmodes om, må enhver personoplysning, der er genereret ved anvendelse af et forbundet produkt eller en relateret tjeneste, kun stilles til rådighed af dataindehaveren til tredjeparten, hvis der er et gyldigt retsgrundlag for behandling i henhold til artikel 6 i forordning (EU) 2016/679, og, hvor det er relevant, betingelserne i artikel 9 i nævnte forordning og artikel 5, stk. 3, i direktiv 2002/58/EF er opfyldt.

8. Enhver uenighed mellem dataindehaver og tredjepart om ordninger for overførsel af data må ikke berøre, hindre eller gribe ind i den registreredes udøvelse af rettigheder i henhold til forordning (EU) 2016/679, navnlig med hensyn til retten til dataportabilitet i henhold til nævnte forordnings artikel 20.

9. Forretningshemmeligheder skal bevares og må kun videregives til tredjeparter, i det omfang sådan videregivelse er strengt nødvendig for at opfylde det formål, der er aftalt mellem brugeren og tredjeparten. Dataindehaveren eller, når det ikke er den samme person, forretningshemmelighedshaveren identificerer de data, der er beskyttet som forretningshemmeligheder, herunder i de relevante metadata, og aftaler med tredjeparten alle forholdsmæssige tekniske og organisatoriske foranstaltninger, der er nødvendige for at beskytte fortroligheden af de delte data, såsom en model for aftalevilkår, fortrolighedsaftaler, strenge adgangsprotokoller, tekniske standarder og anvendelse af adfærdskodekser.

10. Hvis der ikke foreligger nogen aftale om de i denne artikels stk. 9 omhandlede nødvendige foranstaltninger, eller hvis tredjeparten undlader at gennemføre de foranstaltninger, der er aftalt i henhold til denne artikels stk. 9, eller undergraver fortroligheden af forretningshemmeligheder, kan dataindehaveren tilbageholde eller i givet fald suspendere delingen af data, der er identificeret som forretningshemmeligheder. Dataindehaverens beslutning skal være behørigt begrundet og meddeles tredjeparten skriftligt uden unødigt ophold. I sådanne tilfælde underretter dataindehaveren den kompetente myndighed, der er udpeget i henhold til artikel 37, om, at den har tilbageholdt eller suspenderet datadelingen, og udpeger de foranstaltninger, der ikke er aftalt eller gennemført, og, hvis det er relevant, de forretningshemmeligheder, hvis fortrolighed er undergravet.

11. Når dataindehaveren, der er en forretningshemmelighedshaver, under ekstraordinære omstændigheder kan påvise, at vedkommende højst sandsynligt vil lide alvorlig økonomisk skade som følge af videregivelsen af forretningshemmeligheder på trods af de tekniske og organisatoriske foranstaltninger, som tredjeparten har truffet i henhold til denne artikels stk. 9, kan den pågældende dataindehaver fra sag til sag afslå en anmodning om adgang til de pågældende specifikke data. Denne påvisning skal være behørigt begrundet i objektive forhold, navnlig muligheden for at håndhæve beskyttelsen af forretningshemmeligheder i tredjelande, arten og graden af fortrolighed for de ønskede data og det forbundne produkts unikke og nyskabende karakter, og skal meddeles tredjeparten skriftligt uden unødigt ophold. Hvor dataindehaveren afslår at dele data i henhold til nærværende stykke, underretter vedkommende den kompetente myndighed, der er udpeget i henhold til artikel 37.

12. Uden at det berører en tredjeparts ret til prøvelse ved en medlemsstats domstol eller ret på et hvilket som helst tidspunkt, kan en tredjepart, der ønsker at anfægte en dataindehavers beslutning om at afslå eller om at tilbageholde eller suspendere datadeling i henhold til stk. 10 og 11:

a) i overensstemmelse med artikel 37, stk. 5, litra b), indgive klage til den kompetente myndighed, som uden unødigt ophold skal beslutte, om og på hvilke betingelser datadelingen skal påbegyndes eller genoptages, eller

b) aftale med dataindehaveren, at sagen indbringes for et tvistbilæggelsesorgan i overensstemmelse med artikel 10, stk. 1.

13. Den rettighed, der er omhandlet i stk. 1, må ikke krænke registreredes rettigheder i henhold til gældende EU-ret og national ret om beskyttelse af personoplysninger.

Artikel 6

Forpligtelser for tredjeparter, der modtager data efter anmodning fra brugeren

1. En tredjepart behandler kun de data, som den har fået stillet til rådighed i henhold til artikel 5, til de formål og på de betingelser, der er aftalt med brugeren, og under anvendelse af EU-retten og national ret om beskyttelse af personoplysninger, herunder den registreredes rettigheder for så vidt angår personoplysninger. Tredjeparten sletter dataene, når de ikke længere er nødvendige til det aftalte formål, medmindre andet er aftalt med brugeren i forbindelse med andre data end personoplysninger.

2. Tredjeparten må ikke:

a) gøre brugerens udøvelse af valgmuligheder eller rettigheder efter artikel 5 og nærværende artikel unødigt vanskelig, herunder ved at tilbyde brugerne valgmuligheder på en ikkeneutral måde, eller ved at tvinge, vildlede eller manipulere brugeren eller ved at undergrave eller begrænse brugernes autonomi, beslutningstagning eller valgmuligheder, herunder ved hjælp af en digital brugergrænseflade eller en del deraf

b) uanset artikel 22, stk. 2, litra a) og c) i forordning (EU) 2016/679, anvende de modtagne data til profilering, medmindre det er nødvendigt for at levere den tjeneste, som brugeren har anmodet om

c) stille de modtagne data til rådighed for en anden tredjepart, medmindre dataene stilles til rådighed på grundlag af en aftale med brugeren, og forudsat at den anden tredjepart træffer alle nødvendige foranstaltninger, der er aftalt mellem dataindehaveren og tredjeparten, for at beskytte fortroligheden af forretningshemmeligheder

d) stille de modtagne data til rådighed for en virksomhed, der er udpeget som gatekeeper i henhold til artikel 3 i forordning (EU) 2022/1925

e) anvende de modtagne data til at udvikle et produkt, der konkurrerer med det produkt, som de modtagne data stammer fra, eller dele dataene med en anden tredjepart til dette formål; tredjeparter må heller ikke anvende andre produktdata eller relaterede tjenstedata end personoplysninger, der stilles til rådighed for dem, til at opnå indsigt i dataindehaverens økonomiske situation, aktiver og produktionsmetoder eller anvendelse af disse

f) anvende de modtagne data på en måde, der påvirker det forbundne produkts eller de relaterede tjenesters sikkerhed negativt

g) tilsidesætte de specifikke foranstaltninger, der er aftalt med dataindehaveren eller forretningshemmelighedshaveren i henhold til artikel 5, stk. 9, og undergraver fortroligheden af forretningshemmeligheder

h) forhindre brugeren, der er en forbruger, herunder på grundlag af en aftale, i at stille de data, som vedkommende modtager, til rådighed for andre parter.

Artikel 7

Omfanget af forpligtelser vedrørende datadeling mellem virksomheder og forbrugere og mellem virksomheder

1. Forpligtelserne i dette kapitel finder ikke anvendelse på data genereret ved anvendelse af forbundne produkter, der fremstilles eller udformes, eller relaterede tjenester, der leveres, af en mikrovirksomhed eller en lille virksomhed, forudsat at denne virksomhed ikke har en partnervirksomhed eller en tilknyttet virksomhed som omhandlet i artikel 3 i bilaget til henstilling 2003/361/EF, der ikke er en mikrovirksomhed eller en lille virksomhed, og hvor mikrovirksomheden og den lille virksomhed ikke har fået fremstilling eller udformning af et forbundet produkt eller levering af en relateret tjeneste i underentreprise.

Det samme gælder for data genereret ved anvendelse af forbundne produkter, som fremstilles af, eller forbundne produkter, som leveres af, en mellemstor virksomhed, der har været en mellemstor virksomhed i henhold til artikel 2 i bilaget til henstilling 2003/361/EF i mindre end ét år, og for forbundne produkter i ét år efter den dato, hvorpå de blev bragt i omsætning af en mellemstor virksomhed.

2. Aftalevilkår, der til skade for brugeren udelukker anvendelsen af, fraviger eller ændrer virkningen af brugerens rettigheder i henhold til dette kapitel, er ikke bindende for brugeren.

KAPITEL III

FORPLIGTELSE FOR DATAINDEHAVERE, DER ER FORPLIGTEDE TIL AT STILLE DATA TIL RÅDIGHED I HENHOLD TIL EU-RETEN

Artikel 8

Betingelser, hvorunder dataindehavere stiller data til rådighed for datamodtagere

1. Hvis en dataindehaver i relationer mellem virksomheder er forpligtet til at stille data til rådighed for en datamodtager i medfør af artikel 5 eller i medfør af anden gældende EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten, skal denne med en datamodtager aftale ordningerne for tilrådighedsstillelsen af dataene, og det skal ske på fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser og på en gennemsigtig måde i overensstemmelse med dette kapitel og kapitel IV.
2. Et aftalevilkår om adgang til og anvendelse af data eller om ansvar og retsmidler i forbindelse med tilsidesættelse eller ophør af datarelaterede forpligtelser er ikke bindende, hvis det udgør et urimeligt aftalevilkår i den i artikel 13 anvendte betydning, eller hvis det til skade for brugeren udelukker anvendelsen af, fraviger eller ændrer virkningen af brugerens rettigheder i henhold til kapitel II.
3. Når en dataindehaver stiller data til rådighed, må denne ikke med hensyn til ordningerne for tilrådighedsstillelse af data forskelsbehandle sammenlignelige kategorier af datamodtagere, herunder dataindehaverens partnervirksomheder eller tilknyttede virksomheder. Hvis en datamodtager mener, at de betingelser, hvorunder den pågældende har fået dataene stillet til rådighed, er forskelsbehandlende, skal dataindehaveren uden unødigt ophold og på datamodtagerens begrundede anmodning give denne oplysninger, der viser, at tilrådighedsstillelsen ikke er forskelsbehandlende.
4. En dataindehaver må ikke stille data til rådighed for en datamodtager, herunder med eneret, medmindre brugeren anmoder herom i henhold til kapitel II.
5. Dataindehavere og datamodtagere er ikke forpligtede til at give oplysninger ud over, hvad der er nødvendigt for at kontrollere overholdelsen af de aftalte vilkår for dataenes tilrådighedsstillelse eller af deres forpligtelser i medfør af denne forordning eller anden gældende EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten.
6. Medmindre andet er fastsat i EU-retten, herunder denne forordnings artikel 4, stk. 6, og artikel 5, stk. 9, eller i national lovgivning vedtaget i overensstemmelse med EU-retten, indebærer en forpligtelse til at stille data til rådighed for en datamodtager ikke, at forretningshemmeligheder skal videregives.

Artikel 9

Godtgørelse for at stille data til rådighed

1. Enhver godtgørelse, der aftales mellem en dataindehaver og en datamodtager for at stille data til rådighed i relationer mellem virksomheder, skal være ikkeforskelsbehandlende og rimelig og kan omfatte en margin.
2. Når de indgår aftale om godtgørelse, skal dataindehaveren og datamodtageren navnlig tage hensyn til:

a) omkostninger ved at stille dataene til rådighed, herunder navnlig de omkostninger, der er nødvendige for formatering af dataene, elektronisk formidling og lagring

b) investeringer i indsamling og produktion af data, i givet fald under hensyntagen til, om andre parter har bidraget til at opnå, generere eller indsamle de pågældende data.

3. Den i stk. 1 omhandlede godtgørelse kan også afhænge af dataenes mængde, format og art.

4. Hvis datamodtageren er en SMV eller en nonprofitforskningsinstitution, og hvis en sådan datamodtager ikke har partnervirksomheder eller tilknyttede virksomheder, der ikke betegnes som SMV'er, må den aftalte godtgørelse ikke overstige de omkostninger, der er omhandlede i stk. 2, litra a).

5. Kommissionen vedtager retningslinjer for beregningen af rimelig godtgørelse under hensyntagen til rådgivningen fra Det Europæiske Datainnovationsråd (EDIB), der er omhandlet i artikel 42.

6. Denne artikel er ikke til hinder for, at anden EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten, udelukker godtgørelse for at stille data til rådighed eller fastsætter en lavere godtgørelse.

7. Dataindehaveren skal oplyse datamodtageren om grundlaget for beregningen af godtgørelsen i tilstrækkelig detaljeret grad til, at datamodtageren kan vurdere, om kravene i stk. 1-4 er opfyldt.

Artikel 10

Tvistbilæggelse

1. Brugere, dataindehavere og datamodtagere skal have adgang til et tvistbilæggelsesorgan, der er certificeret i overensstemmelse med denne artikels stk. 5, til at bilægge tvister i henhold til artikel 4, stk. 3 og 9, og artikel 5, stk. 12, samt tvister vedrørende de fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser for og en gennemsigtig måde at stille data til rådighed på i overensstemmelse med dette kapitel og kapitel IV.

2. Et tvistbilæggelsesorgan skal gøre de berørte parter bekendt med dets gebyrer eller med de mekanismer, der anvendes til at fastsætte gebyrerne, inden disse parter anmoder om en afgørelse.

3. For tvister som forelægges et tvistbilæggelsesorgan i henhold til artikel 4, stk. 3 og 9, og artikel 5, stk. 12, afholder dataindehaveren, hvis tvistbilæggelsesorganet træffer afgørelse om en tvist til fordel for brugeren eller for datamodtageren, alle de gebyrer, som tvistbilæggelsesorganet opkræver, og godtgør den pågældende bruger eller datamodtager alle andre rimelige udgifter, som denne har måttet afholde i forbindelse med tvistbilæggelsen. Hvis tvistbilæggelsesorganet afgør en tvist til fordel for dataindehaveren, skal brugeren eller datamodtageren ikke være forpligtet til at godtgøre gebyrer eller andre udgifter, som dataindehaveren har betalt eller skal betale i forbindelse med tvistbilæggelsen, medmindre tvistbilæggelsesorganet finder, at brugeren eller datamodtageren åbenlyst har handlet i ond tro.

4. Kunder og udbydere af databehandlingstjenester skal have adgang til et tvistbilægelsesorgan, der er certificeret i overensstemmelse med denne artikels stk. 5, til at bilægge tvister i forbindelse med overtrædelse af kundernes rettigheder og de forpligtelser, der påhviler udbydere af databehandlingstjenester, i overensstemmelse med artikel 23-31.

5. Den medlemsstat, hvori tvistbilægelsesorganet er etableret, certificerer det pågældende organ efter dets anmodning, hvis det har godtgjort, at det opfylder alle følgende betingelser:

a) det er upartisk og uafhængigt, og det skal træffe sine afgørelser i overensstemmelse med klare, ikkeforskelsbehandlende og fair procedureregler

b) det har den nødvendige ekspertise, navnlig med hensyn til fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser, herunder godtgørelse, og om at stille data til rådighed på en gennemsigtig måde, således at organet effektivt kan fastsætte disse vilkår og betingelser

c) det er let at kontakte ved hjælp af elektronisk kommunikation

d) det er i stand til at vedtage sine afgørelser på en hurtig og omkostningseffektiv måde på mindst ét af Unionens officielle sprog.

6. Medlemsstaterne underretter Kommissionen om de tvistbilægelsesorganer, der er certificeret i overensstemmelse med stk. 5. Kommissionen offentliggør en liste over disse organer på et særligt websted og holder den ajour.

7. Et tvistbilægelsesorgan afviser at behandle en anmodning om bilægelse af en tvist, der allerede er indbragt for et andet tvistbilægelsesorgan eller for en medlemsstats domstol eller ret.

8. Et tvistbilægelsesorgan giver parterne mulighed for inden for en rimelig frist at fremsætte deres synspunkter vedrørende de sager, som parterne har indbragt for dette organ. I denne forbindelse gives hver part i en tvist gives adgang til indlæg fra den anden part i deres tvist og til eventuelle ekspertudtalelser. Parterne skal gives mulighed for at fremsætte bemærkninger til disse indlæg og udtalelser.

9. Et tvistbilægelsesorgan skal vedtage sin afgørelse i den sag, der indbringes for det, senest 90 dage efter modtagelsen af en anmodning i henhold til stk. 1 og 4. Denne afgørelse skal være skriftlig eller på et varigt medium og skal understøttes af en begrundelse.

10. Tvistbilægelsesorganer udfærdiger og offentliggør årlige aktivitetsrapporter. Sådanne årlige rapporter skal navnlig indeholde følgende generelle oplysninger:

a) en samlet oversigt over udfaldet af tvister

b) den gennemsnitlige tid, det har taget at bilægge tvister

c) de mest almindelige årsager til tvister.

11. Et offentligt tvistbilæggelsesorgan kan med henblik på at fremme udvekslingen af oplysninger og bedste praksis beslutte i den stk. 10 omhandlede rapport at medtage anbefalinger til, hvordan problemer kan undgås eller løses.

12. Et tvistbilæggelsesorgans afgørelse er kun bindende for parterne, hvis parterne udtrykkeligt har givet deres samtykke til dens bindende karakter, inden tvistbilæggelsesproceduren indledes.

13. Denne artikel berører ikke parterets ret til adgang til effektive retsmidler ved en medlemsstats domstol eller ret.

Artikel 11

Tekniske beskyttelsesforanstaltninger om uautoriseret anvendelse eller videregivelse af data

1. En dataindehaver kan anvende passende tekniske beskyttelsesforanstaltninger, herunder intelligente kontrakter og kryptering, for at forhindre uautoriseret adgang til data, herunder metadata, og sikre overholdelse af artikel 4, 5, 6, 8 og 9 samt af de aftalte kontraktvilkår for at stille data til rådighed. Sådanne tekniske beskyttelsesforanstaltninger må hverken forskelsbehandle datamodtagere eller hindre en brugers ret til at få en kopi af, hente, anvende eller tilgå data eller levere data til tredjeparter i henhold til artikel 5 eller en tredjeparts rettigheder i henhold til EU-retten eller national lovgivning vedtaget i overensstemmelse med EU-retten. Brugere, tredjeparter og datamodtagere må ikke ændre eller fjerne sådanne tekniske beskyttelsesforanstaltninger, medmindre det er aftalt med dataindehaveren.

2. I de tilfælde, der er omhandlet i stk. 3, skal tredjeparten eller datamodtageren uden unødigt ophold imødekomme anmodningerne fra dataindehaveren og i givet fald og hvor de ikke er den samme person, forretningshemmelighedshaveren eller fra brugeren om at:

a) slette de data, som dataindehaveren har stillet til rådighed, samt alle kopier heraf

b) ophøre med produktion, udbud til salg, bringen i omsætning eller anvendelse af varer, afledte data eller tjenester, der er fremstillet på grundlag af viden, der er opnået ved hjælp af sådanne data, samt ophøre med import, eksport eller oplagring af sådanne krænkende varer og tilintetgøre alle krænkende varer, hvis der er alvorlig risiko for, at ulovlig anvendelse af disse data vil forvolde dataindehaveren, forretningshemmelighedshaveren eller brugeren væsentlig skade, eller hvis en sådan foranstaltning ikke vil være uforholdsmæssig i forhold til dataindehaverens, forretningshemmelighedshaverens eller brugerens interesser

c) informere brugeren om den uautoriserede anvendelse eller videregivelse af data samt om de foranstaltninger, der er truffet for at bringe den uautoriserede anvendelse eller videregivelse af dataene til ophør

d) yde godtgørelse til den part, der lider skade på grund af misbrug eller videregivelse af sådanne data, som er tilgået eller anvendt ulovligt.

3. Stk. 2 finder anvendelse, hvis en tredjepart eller en datamodtager:

a) med henblik på opnåelse af data har givet urigtige oplysninger til en dataindehaver, har anvendt vildledende midler eller tvangsmidler, eller har misbrugt mangler i dataindehaverens tekniske databeskyttelsesinfrastruktur

b) har anvendt de data, der er stillet til rådighed, til uautoriserede formål, herunder udvikling af et konkurrerende forbundet produkt som omhandlet i artikel 6, stk. 2, litra e)

c) ulovligt har videregivet data til en anden part

d) ikke har opretholdt de tekniske og organisatoriske foranstaltninger, der er aftalt i henhold til artikel 5, stk. 9, eller

e) har ændret eller fjernet tekniske beskyttelsesforanstaltninger, som dataindehaveren anvender i henhold til nærværende artikels stk. 1, uden dataindehaverens samtykke.

4. Stk. 2 finder også anvendelse, hvis en bruger ændrer eller fjerner tekniske beskyttelsesforanstaltninger, som dataindehaveren anvender, eller ikke opretholder de tekniske og organisatoriske foranstaltninger, som brugeren har truffet efter aftale med dataindehaveren eller, når det ikke er den samme person, forretningshemmelighedshaveren, for at beskytte forretningshemmeligheder, samt hvad angår enhver anden part, der modtager dataene fra brugeren ved hjælp af en overtrædelse af denne forordning.

5. Hvis datamodtageren overtræder artikel 6, stk. 2, litra a) eller b), har brugere de samme rettigheder som dataindehavere i henhold til nærværende artikels stk. 2.

Artikel 12

Omfanget af forpligtelser for dataindehavere, der er forpligtede i henhold til EU-retten til at stille data til rådighed

1. Dette kapitel finder anvendelse, når en dataindehaver i relationer mellem virksomheder er forpligtet til at stille data til rådighed for en datamodtager i medfør af artikel 5 eller i medfør af gældende EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten.

2. Et aftalevilkår i en aftale om datadeling, som til skade for en part eller i givet fald til skade for brugeren udelukker anvendelsen af dette kapitel, fraviger det eller ændrer dets virkning, er ikke bindende for den pågældende part.

KAPITEL IV

URIMELIGE AFTALEVILKÅR VEDRØRENDE DATAADGANG OG -ANVENDELSE MEL- LEM VIRKSOMHEDER

Artikel 13

Urimelige aftalevilkår, der ensidigt pålægges en anden virksomhed

1. Et aftalevilkår om adgang til og anvendelse af data eller om ansvar og retsmidler ved tilsidesættelse eller ophør af datarelaterede forpligtelser, som en virksomhed ensidigt har pålagt en anden virksomhed, er ikke bindende for sidstnævnte virksomhed, hvis det er urimeligt.
2. Et aftalevilkår, der afspejler ufravigelige bestemmelser i EU-retten eller bestemmelser i EU-retten, som ville finde anvendelse, hvis aftalevilkårene ikke regulerede spørgsmålet, skal ikke anses for at være urimeligt.
3. Et aftalevilkår er urimeligt, hvis det er af en sådan art, at dets anvendelse klart afviger fra god handelspraksis med hensyn til dataadgang og -anvendelse i strid med god tro og redelig handlemåde.
4. Med henblik på stk. 3 anses et aftalevilkår navnlig for at være urimeligt, hvis dets formål eller virkning er:
 - a) at udelukke eller begrænse ansvaret for forsætlige handlinger eller grov uagtsomhed for den part, der ensidigt har pålagt vilkåret
 - b) at udelukke de retsmidler, som den part, der ensidigt er blevet pålagt vilkåret, har til rådighed i tilfælde af manglende opfyldelse af kontraktlige forpligtelser eller det ansvar, der påhviler den part, som ensidigt har pålagt vilkåret, i tilfælde af tilsidesættelse af disse forpligtelser
 - c) at give den part, der ensidigt har pålagt vilkåret, eneret til at afgøre, om de leverede data opfylder aftalevilkårene, eller til at fortolke de enkelte aftalevilkår.
5. Med henblik på stk. 3 formodes et aftalevilkår at være urimeligt, hvis dets formål eller virkning er:
 - a) på upassende vis at begrænse retsmidlerne i tilfælde af manglende opfyldelse af kontraktlige forpligtelser eller på upassende vis at begrænse ansvaret i tilfælde af tilsidesættelse af disse forpligtelser eller udvide det ansvar, der påhviler den virksomhed, som ensidigt er blevet pålagt vilkåret
 - b) at give den part, der ensidigt har pålagt vilkåret, tilladelse til at tilgå og anvende den anden kontraherende parts data på en måde, der er til betydelig skade for den anden kontraherende parts legitime interesser, navnlig når de pågældende data indeholder kommercielt følsomme data eller er beskyttet af forretningshemmeligheder eller af intellektuelle ejendomsrettigheder

c) at forhindre den part, som ensidigt er blevet pålagt vilkåret, i at anvende de data, som denne part har leveret eller genereret i løbet af aftalens gyldighedsperiode, eller at begrænse anvendelsen af sådanne data i et sådant omfang, at denne part ikke har ret til at anvende, indsamle, tilgå eller kontrollere sådanne data eller udnytte værdien af sådanne data på en hensigtsmæssig måde

d) at forhindre den part, som ensidigt er blevet pålagt vilkåret, i at opsige aftalen inden for en rimelig frist

e) at forhindre den part, som er blevet ensidigt pålagt vilkåret, i at få en kopi af de data, som denne part har leveret eller genereret i løbet af aftalens gyldighedsperiode eller inden for en rimelig frist efter dens ophør

f) at give den part, der ensidigt har pålagt vilkåret, mulighed for at opsige aftalen med urimeligt kort varsel, under hensyntagen til den anden kontraherende parts rimelige mulighed for at skifte til en alternativ og sammenlignelig tjeneste og den økonomiske skade, som en sådan opsigelse forvolder, medmindre der er tungtvejende grunde hertil

g) at give den part, der ensidigt har pålagt vilkåret, mulighed for i væsentlig grad at ændre den pris, der er anført i aftalen, eller enhver anden materiel betingelse vedrørende arten, formatet, kvaliteten eller mængden af de data, der skal deles, hvis der i aftalen ikke er anført nogen gyldig grund til og ingen ret for den anden part til at opsige aftalen i tilfælde af en sådan ændring.

Første afsnit, litra g), berører ikke vilkår, hvorved den part, der ensidigt har pålagt vilkåret, forbeholder sig ret til ensidigt at ændre vilkårene i en aftale af ubestemt varighed, forudsat at der i aftalen er anført en gyldig grund for en sådan ensidig ændring, at den part, der ensidigt har pålagt vilkåret, er forpligtet til at give den anden kontraherende part et rimeligt varsel om en sådan påtænkt ændring, og at den anden kontraherende part frit kan opsige aftalen uden omkostninger i tilfælde af en ændring.

6. Et aftalevilkår anses for at være ensidigt pålagt som omhandlet i denne artikel, hvis det er fremsat af en af de kontraherende parter, og den anden kontraherende part ikke har kunnet påvirke dets indhold på trods af et forsøg på at forhandle om vilkåret. Det påhviler den af de kontraherende parter, der har fremsat aftalevilkåret, at bevise, at dette vilkår ikke er ensidigt pålagt. Den kontraherende part, der har fremsat det omtvistede aftalevilkår, kan ikke gøre gældende, at vilkåret er et urimeligt aftalevilkår.

7. Hvis det urimelige aftalevilkår kan adskilles fra de øvrige aftalevilkår, er disse øvrige aftalevilkår bindende.

8. Denne artikel finder ikke anvendelse på aftalevilkår, der definerer aftalens hovedgenstand, eller på overensstemmelsen mellem prisen og de data, der er leveret som modydelse herfor.

9. Parterne i en aftale, der er omfattet af stk. 1, må ikke udelukke anvendelsen af, fravige eller ændre virkningerne af denne artikel.

KAPITEL V

TILRÅDIGHEDSSTILLELSE AF DATA FOR OFFENTLIGE MYNDIGHEDER, KOMMISSIONEN, DEN EUROPÆISKE CENTRALBANK OG EU-ORGANER PÅ GRUNDLAG AF ET EKSTRAORDINÆRT BEHOV

Artikel 14

Forpligtelse til at stille data til rådighed på grundlag af et ekstraordinært behov

Hvis en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ påviser, at der foreligger et ekstraordinært behov, jf. artikel 15, for at anvende visse data, herunder de relevante metadata, der er nødvendige for at fortolke og anvende disse data, for at udføre sine lovbestemte opgaver i offentlighedens interesse, stiller dataindehavere, der er juridiske personer, men ikke offentlige myndigheder, og som er i besiddelse af de pågældende data, dem til rådighed efter en behørigt begrundet anmodning.

Artikel 15

Ekstraordinært behov for at anvende data

1. Et ekstraordinært behov for at anvende visse data som omhandlet i dette kapitel skal være begrænset i tid og omfang og skal kun anses for at foreligge under enhver af følgende omstændigheder:

a) de data, der anmodes om, er nødvendige for at reagere på en offentlig nødsituation, og den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet er ikke i stand til rettidigt og effektivt at opnå de pågældende data ved hjælp af alternative midler på tilsvarende betingelser

b) under omstændigheder, der ikke er omfattet af litra a), og kun for så vidt angår andre data end personoplysninger, hvis:

i) en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ handler på grundlag af EU-retten eller national ret og har identificeret specifikke data, som den eller det mangler for at kunne fuldføre en specifik opgave udført i offentlighedens interesse, som udtrykkeligt er fastsat ved lov, såsom udarbejdelse af officielle statistikker eller afbødning eller genopretning efter en offentlig nødsituation, og

ii) den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet har udtømt alle andre til rådighed stående muligheder for at opnå de pågældende data, herunder køb af andre data end personoplysninger på markedet ved at tilbyde markedspriser eller gøre brug af eksisterende forpligtelser til at stille data til rådighed eller vedtagelse af nye lovgivningsmæssige foranstaltninger, der kunne garantere rettidig tilgængelighed af dataene.

2. Stk. 1, litra b), finder ikke anvendelse på mikrovirksomheder og små virksomheder.

3. Forpligtelsen til at påvise, at den offentlige myndighed ikke var i stand til at opnå andre data end personoplysninger ved at købe dem på markedet, finder ikke anvendelse, hvis den specifikke opgave udført i offentlighedens interesse består i udarbejdelse af officielle statistikker, og hvis købet af sådanne data ikke er tilladt i henhold til national ret.

Artikel 16

Sammenhæng med andre forpligtelser til at stille data til rådighed for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer

1. Dette kapitel berører ikke de forpligtelser, der er fastsat i EU-retten eller national ret med henblik på indberetning, efterkommelse af anmodninger om adgang til oplysninger eller påvisning eller verifikation af overholdelse af retlige forpligtelser.

2. Dette kapitel finder ikke anvendelse på offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer, der udfører aktiviteter med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafferetlige eller administrative overtrædelser eller fuldbyrdelse af strafferetlige sanktioner eller på told- og skatteforvaltning. Dette kapitel berører ikke gældende EU-ret og national ret om forebyggelse, efterforskning, afsløring eller retsforfølgning af strafferetlige eller administrative overtrædelser eller fuldbyrdelse af strafferetlige eller administrative sanktioner eller om told- og skatteforvaltning.

Artikel 17

Anmodninger om at få stillet data til rådighed

1. Når offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller et EU-organ anmoder om data i henhold til artikel 14 skal de:

a) præcisere de nødvendige data, herunder de relevante metadata, der er nødvendige for at fortolke og anvende disse data

b) påvise, at de nødvendige betingelser for, at der foreligger et ekstraordinært behov som omhandlet i artikel 15, hvortil der anmodes om data, er opfyldt

c) forklare formålet med anmodningen, den påtænkte anvendelse af de data, der anmodes om, herunder i givet fald af en tredjepart i overensstemmelse med nærværende artikels stk. 4, varigheden af denne anvendelse, og, hvor det er relevant, hvordan behandlingen af personoplysninger skal imødekomme det ekstraordinære behov

d) om muligt angive, hvornår dataene forventes at blive slettet af alle parter, der har adgang til dem

- e) begrunde valget af dataindehaver, som anmodningen er rettet til
- f) angive andre offentlige myndigheder eller Kommissionen, Den Europæiske Centralbank eller EU-organer og de tredjeparter, som de data, der anmodes om, forventes at blive delt med
- g) hvis der anmodes om personoplysninger, angive eventuelle tekniske og organisatoriske foranstaltninger, der er nødvendige og forholdsmæssige for at implementere databeskyttelsesprincipper, og nødvendige sikkerhedsforanstaltninger såsom pseudonymisering og hvorvidt dataindehaveren kan anvende anonymisering, inden dataene stilles til rådighed
- h) angive den retlige bestemmelse, som tildeler den anmodende offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet den specifikke opgave udført i offentlighedens interesse, der er relevant for anmodningen om data
- i) angive den frist, inden for hvilken dataene skal stilles til rådighed, og den i artikel 18, stk. 2, omhandlede frist, inden for hvilken dataindehaveren kan afslå eller anmode om ændring af anmodningen
- j) gøre deres bedste for at undgå, at en efterkommelse af dataanmodningen fører til, at dataindehaverne er ansvarlige for overtrædelse af EU-retten eller national ret.

2. En anmodning om data i henhold til denne artikels stk. 1 skal:

- a) være formuleret skriftligt og i et klart, koncist og almindeligt sprog, der er forståeligt for dataindehaveren
- b) være specifik med hensyn, hvilken type data der anmodes om, og vedrøre data, som dataindehaveren har kontrol over på tidspunktet for anmodningen
- c) stå i et rimeligt forhold til det ekstraordinære behov og være behørigt begrundet med hensyn til de ønskede datas detaljeringsgrad, mængde og tilgangshyppighed
- d) respektere dataindehaverens legitime mål og indeholde tilsagn om at sikre beskyttelsen af forretningshemmeligheder i overensstemmelse med artikel 19, stk. 3, og de omkostninger og den indsats, der kræves for at stille dataene til rådighed
- e) vedrøre andre data end personoplysninger og, kun hvis det påvises, at dette er utilstrækkeligt til at imødekomme det ekstraordinære behov for at anvende data, jf. artikel 15, stk. 1, litra a), anmode om personoplysninger i pseudonymiseret form og fastsætte de tekniske og organisatoriske foranstaltninger, der skal træffes for at beskytte dataene
- f) informere dataindehaveren om de sanktioner, der i tilfælde af manglende efterkommelse af anmodningen skal pålægges i henhold til artikel 40 af den kompetente myndighed, der er udpeget i henhold til artikel 37

g) hvis anmodningen er foretaget af en offentlig myndighed, overføres til den i artikel 37 omhandlede datakoordinator i den medlemsstat, hvor den anmodende offentlige myndighed er etableret, som uden unødigt ophold skal gøre anmodningen offentligt tilgængelig online, medmindre datakoordinatoren finder, at sådan offentliggørelse vil udgøre en risiko for den offentlige sikkerhed

h) hvis anmodningen er foretaget af Kommissionen, Den Europæiske Centralbank eller et EU-organ, gøres tilgængelig online uden unødigt ophold

i) hvis der anmodes om personoplysninger, uden unødigt ophold meddeles den tilsynsmyndighed, der er ansvarlig for at overvåge anvendelsen af forordning (EU) 2016/679 i den medlemsstat, hvor den offentlige myndighed er etableret.

Den Europæiske Centralbank og EU-organerne underretter Kommissionen om deres anmodninger.

3. En offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ må ikke stille data, der er opnået i henhold til dette kapitel, til rådighed for videreanvendelse som defineret i artikel 2, nr. 2), i forordning (EU) 2022/868 eller i artikel 2, nr. 11), direktiv (EU) 2019/1024. Forordning (EU) 2022/868 og direktiv (EU) 2019/1024 finder ikke anvendelse på data i offentlige myndigheders besiddelse, der er opnået i henhold til dette kapitel.

4. Denne artikels stk. 3 er ikke til hinder for, at en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ udveksler data, der er opnået i henhold til dette kapitel, med en anden offentlig myndighed eller Kommissionen, Den Europæiske Centralbank eller et EU-organ med henblik på at udføre opgaverne omhandlet i artikel 15, som anført i anmodningen i overensstemmelse med nærværende artikels stk. 1, litra f), eller stiller dataene til rådighed for en tredjepart, når tekniske inspektioner eller andre funktioner ved hjælp af en offentlig aftale er outsourcet til denne tredjepart. De forpligtelser, der påhviler offentlige myndigheder i henhold til artikel 19, navnlig sikkerhedsforanstaltninger til at beskytte fortroligheden af forretningshemmeligheder, finder også anvendelse på sådanne tredjeparter. Hvis en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ overfører eller stiller data til rådighed i henhold til nærværende stykke, underrettes den dataindehaver, som dataene er modtaget fra, uden unødigt ophold.

5. Hvis dataindehaveren mener, at dennes rettigheder i henhold til dette kapitel er blevet krænket ved overførsel eller tilrådighedsstillelse af data, kan dataindehaveren indgive en klage til den kompetente myndighed, der er udpeget i henhold til artikel 37, i den medlemsstat, hvor dataindehaveren er etableret.

6. Kommissionen udarbejder en standardmodel for anmodninger i henhold til denne artikel.

Artikel 18

Efterkommelse af anmodninger om data

1. En dataindehaver, der modtager en anmodning om tilrådighedsstillelse af data i henhold til dette kapitel, stiller dataene til rådighed for den anmodende offentlige myndighed, Kommissionen, Den Europæiske

Centralbank eller et EU-organ uden unødigt ophold og under hensyntagen til de nødvendige tekniske, organisatoriske og retlige foranstaltninger.

2. Uden at det berører specifikke behov vedrørende tilgængeligheden af data som defineret i EU-retten eller national ret, kan en dataindehaver afslå eller anmode om ændring af en anmodning om tilrådighedsstillelse af data i medfør af dette kapitel uden unødigt ophold og under alle omstændigheder senest fem arbejdsdage efter modtagelsen af en anmodning om de data, der er nødvendige for at reagere på en offentlig nødsituation, og uden unødigt ophold og under alle omstændigheder senest 30 arbejdsdage efter modtagelsen af en sådan anmodning i andre tilfælde af et ekstraordinært behov af enhver af følgende grunde:

a) dataindehaveren har ikke kontrol over de data, der anmodes om

b) en lignende anmodning til samme formål er tidligere blevet indgivet af en anden offentlig myndighed eller Kommissionen, Den Europæiske Centralbank eller et EU-organ, og dataindehaveren er ikke blevet underrettet om sletningen af dataene i henhold til artikel 19, stk. 1, litra c)

c) anmodningen opfylder ikke betingelserne i artikel 17, stk. 1 og 2.

3. Hvis dataindehaveren beslutter at afslå eller anmode om ændring af anmodningen i overensstemmelse med stk. 2, litra b), angiver dataindehaveren identiteten på den offentlige myndighed eller Kommissionen, Den Europæiske Centralbank eller EU-organet, der tidligere har indgivet en anmodning til samme formål.

4. Hvis de data, der anmodes om, omfatter personoplysninger, anonymiserer dataindehaveren dataene korrekt, medmindre efterkommelsen af anmodningen om at stille data til rådighed for en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ kræver videregivelse af personoplysninger. I så fald pseudonymiserer dataindehaveren dataene.

5. Hvis den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet ønsker at anfægte en dataindehavers afslag på at levere de data, der anmodes om, eller hvis dataindehaveren ønsker at anfægte anmodningen, og sagen ikke kan løses ved en passende ændring af anmodningen, forelægges sagen for den kompetente myndighed, der er udpeget i henhold til artikel 37, i den medlemsstat, hvor dataindehaveren er etableret.

Artikel 19

Offentlige myndigheders, Kommissionens, Den Europæiske Centralbanks og EU-organers forpligtelser

1. Når offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller et EU-organ modtager data på grundlag af en anmodning i henhold til artikel 14:

a) må de ikke anvende dataene på en måde, der er uforenelig med det formål, hvortil der blev anmodet om dem

b) skal de have gennemført tekniske og organisatoriske foranstaltninger, der beskytter fortroligheden og integriteten af de data, der anmodes om, og sikkerheden i forbindelse med overførslerne af data, navnlig personoplysninger, og beskytter de registreredes rettigheder og frihedsrettigheder

c) skal de slette dataene, så snart de ikke længere er nødvendige til det angivne formål, og uden unødigt ophold underrette dataindehaveren og de enkeltpersoner eller organisationer, der modtog dataene i henhold til artikel 21, stk. 1, om, at dataene er blevet slettet, medmindre det er påkrævet at arkivere dataene i henhold til EU-retten eller national ret om aktindsigt i forbindelse med gennemsigtighedsforpligtelser.

2. En offentlig myndighed, Kommissionen, Den Europæiske Centralbank, et EU-organ eller en tredjepart, som modtager data i henhold til dette kapitel, må ikke:

a) anvende dataene eller indsigt i dataindehaverens økonomiske situation, aktiver og produktions- eller driftsmetoder til at udvikle eller forbedre et forbundet produkt eller en relateret tjeneste, der konkurrerer med dataindehaverens forbundne produkt eller relaterede tjeneste

b) dele dataene med en anden tredjepart til et af de i litra a) omhandlede formål.

3. Videregivelse af forretningshemmeligheder til en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ er kun påkrævet i det omfang, det er strengt nødvendigt for at opfylde formålet med en anmodning i henhold til artikel 15. I så fald udpeger dataindehaveren eller, når det ikke er den samme person, forretningshemmelighedshaveren de data, der er beskyttet som forretningshemmeligheder, herunder i de relevante metadata. Den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet træffer forud for videregivelsen af forretningshemmeligheder alle nødvendige og passende tekniske og organisatoriske foranstaltninger for at sikre fortroligheden af forretningshemmelighederne, herunder i relevant omfang en model for aftalevilkår, tekniske standarder og anvendelse af adfærdskodekser.

4. En offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ er ansvarlig for sikkerheden af de data, som den eller det modtager.

Artikel 20

Godtgørelse i tilfælde af et ekstraordinært behov

1. Dataindehavere, som ikke er mikrovirksomheder eller små virksomheder, stiller gratis data til rådighed, der er nødvendige for at reagere på en offentlig nødsituation i henhold til artikel 15, stk. 1, litra a). Den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet, som har modtaget data, giver en dataindehaver offentlig anerkendelse, hvis dataindehaveren anmoder om det.

2. En dataindehaver har ret til en rimelig godtgørelse for at efterkomme en anmodning om at stille data til rådighed i efterkommelse af artikel 15, stk. 1, litra b). En sådan godtgørelse skal dække de tekniske og organisatoriske omkostninger, der afholdes for at efterkomme anmodningen, herunder i givet fald omkostningerne ved anonymisering, pseudonymisering, aggregering og teknisk tilpasning, og en rimelig margin. Efter anmodning fra den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet, fremlægger dataindehaveren oplysninger om beregningen af omkostningerne og den rimelige margin.

3. Stk. 2 finder ligeledes anvendelse, hvis en mikrovirksomhed og lille virksomhed kræver godtgørelse for at stille data til rådighed.

4. Dataindehavere er ikke berettigede til godtgørelse for at efterkomme en anmodning om at stille data til rådighed i henhold til artikel 15, stk. 1, litra b), hvis den specifikke opgave udført i offentlighedens interesse er udarbejdelse af officielle statistikker, og hvis køb af data ikke er tilladt i henhold til national ret. Medlemsstaterne underretter Kommissionen, hvis køb af data til udarbejdelse af officielle statistikker ikke er tilladt i henhold til national ret.

5. Hvis den offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet er uenige om størrelsen af den godtgørelse, som dataindehaveren anmoder om, kan de indgive en klage til den kompetente myndighed, der er udpeget i henhold til artikel 37, i den medlemsstat, hvor dataindehaveren er etableret.

Artikel 21

Deling af data, der er indhentet i forbindelse med et ekstraordinært behov, med forskningsinstitutioner eller statistiske kontorer

1. En offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ har ret til at dele data modtaget i henhold til dette kapitel:

a) med enkeltpersoner eller organisationer med henblik på at udføre videnskabelig forskning eller analyse, der er forenelig med det formål, hvortil der blev anmodet om dataene, eller

b) med nationale statistiske kontorer og Eurostat med henblik på udarbejdelse af officielle statistikker.

2. Enkeltpersoner eller organisationer, der modtager data i henhold til stk. 1, handler uden fortjeneste for øje eller i forbindelse med en almenyttig opgave, der er anerkendt i henhold til EU-retten eller national ret. De omfatter ikke organisationer, som kommercielle virksomheder har væsentlig indflydelse på, og som sandsynligvis vil føre til privilegeret adgang til forskningsresultaterne.

3. Enkeltpersoner eller organisationer, der modtager data i henhold til denne artikels stk. 1, skal opfylde de samme forpligtelser, som er gældende for offentlige myndigheder, Kommissionen, Den Europæiske Centralbank eller EU-organer i henhold til artikel 17, stk. 3, og artikel 19.

4. Uanset artikel 19, stk. 1, litra c), må enkeltpersoner eller organisationer, der modtager data i henhold til nærværende artikels stk. 1, opbevare de modtagne data til det formål, til hvilket der blev anmodet om dataene, i op til seks måneder, efter at de offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer har slettet dem.

5. Hvis en offentlig myndighed, Kommissionen, Den Europæiske Centralbank eller et EU-organ har til hensigt at overføre eller stille data til rådighed i henhold til denne artikels stk. 1, underretter den eller det uden unødigt ophold den dataindehaver, som dataene er modtaget fra, om identiteten på og kontaktoplysningerne for den organisation eller enkeltperson, der modtager dataene, formålet med overførslen eller tilrådighedsstillelsen af dataene, den periode, for hvilken dataene skal anvendes, samt de trufne tekniske beskyttelsesforanstaltninger og organisatoriske foranstaltninger, herunder hvis personoplysninger eller forretningshemmeligheder er involveret. Hvis dataindehaveren er uenig i overførslen eller tilrådighedsstillelsen af data, kan denne indgive en klage til den kompetente myndighed, der er udpeget i henhold til artikel 37, i den medlemsstat, hvor dataindehaveren er etableret.

Artikel 22

Gensidig bistand og grænseoverskridende samarbejde

1. Offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer samarbejder og bistår hinanden med henblik på at gennemføre dette kapitel på en sammenhængende måde.

2. Data, der udveksles i forbindelse med bistand, der anmodes om og ydes i henhold til stk. 1, må ikke anvendes på en måde, der er uforenelig med det formål, hvortil der blev anmodet om dem.

3. Hvis en offentlig myndighed har til hensigt at anmode om data fra en dataindehaver, der er etableret i en anden medlemsstat, underretter den først den kompetente myndighed, der er udpeget i henhold til artikel 37, i nævnte medlemsstat om denne hensigt. Dette krav finder også anvendelse på anmodninger fra Kommissionen, Den Europæiske Centralbank og EU-organer. Anmodningen behandles af den kompetente myndighed i den medlemsstat, hvor dataindehaveren er etableret.

4. Efter at have behandlet en anmodning i lyset af kravene i artikel 17 udfører den relevante kompetente myndighed uden unødigt ophold en af følgende tiltag:

a) fremsender anmodningen til dataindehaveren og i givet fald rådgiver den anmodende offentlige myndighed, Kommissionen, Den Europæiske Centralbank eller EU-organet om et eventuelt behov for at samarbejde med offentlige myndigheder i den medlemsstat, hvor dataindehaveren er etableret, med henblik på at mindske den administrative byrde for dataindehaveren ved efterkommelse af anmodningen

b) afviser anmodningen med behørig begrundelse i overensstemmelse med dette kapitel.

Den anmodende offentlige myndighed, Kommissionen, Den Europæiske Centralbank og EU-organet tager hensyn til rådgivningen og begrundelserne fra den relevante kompetente myndighed i henhold

til første afsnit, inden den træffer yderligere tiltag såsom genindsendelse af anmodningen, hvis det er relevant.

KAPITEL VI

SKIFT MELLEM DATABEHANDLINGSTJENESTER

Artikel 23

Fjernelse af hindringer for effektive skift

Udbydere af databehandlingstjenester træffer de foranstaltninger, der er fastsat i artikel 25, 26, 27, 29 og 30, for at gøre det muligt for kunder at skifte til en databehandlingstjeneste, der dækker samme tjenestetype, og som leveres af en anden udbyder af databehandlingstjenester, eller til lokal IKT-infrastruktur, eller, hvor det er relevant, at anvende flere udbydere af databehandlingstjenester på samme tid. Udbydere af databehandlingstjenester må navnlig ikke pålægge og skal fjerne prækommercielle, kommercielle, tekniske, kontraktmæssige og organisatoriske hindringer, som forhindrer kunder i at:

- a) bringe aftalen om databehandlingstjenesteydelsen til ophør efter den maksimale opsigelsesfrist og efter en vellykket afslutning på skifteprocessen i overensstemmelse med artikel 25
- b) indgå nye aftaler med en anden udbyder af databehandlingstjenester, der dækker samme tjenestetype
- c) portere kunders eksporterbare data og andre digitale aktiver til en anden udbyder af databehandlingstjenester eller til en lokal IKT-infrastruktur, herunder efter at have nydt godt af et tilbud om gratis niveau
- d) opnå funktionel ækvivalens i overensstemmelse med artikel 24 i forbindelse med anvendelse af den nye databehandlingstjeneste i IKT-miljøet hos en anden udbyder af databehandlingstjenester, der dækker samme tjenestetype
- e) hvis det er teknisk muligt, adskille databehandlingstjenester omhandlet i artikel 30, stk. 1, fra andre databehandlingstjenester, der leveres af udbyderen af databehandlingstjenester.

Artikel 24

Omfang af de tekniske forpligtelser

Ansvarsområderne for udbydere af databehandlingstjenester fastlagt i artikel 23, 25, 29, 30 og 34 finder kun anvendelse på tjenesteydelser, aftaler eller handelspraksis udbudt af kildeudbyderen af databehandlingstjenester.

*Artikel 25***Aftalevilkår i forbindelse med skift**

1. Kundens rettigheder og de forpligtelser, der påhviler udbyderen af databehandlingstjenester i forbindelse med skift mellem udbydere af sådanne tjenester eller i givet fald til en lokal IKT-infrastruktur, skal fremgå klart af en skriftlig aftale. Udbyderen af databehandlingstjenester skal gøre denne aftale tilgængelig for kunden, inden aftalen underskrives, på en måde, som giver kunden mulighed for at lagre og gengive aftalen.

2. Uden at det berører direktiv (EU) 2019/770, skal den i denne artikels stk. 1 omhandlede aftale mindst indeholde følgende:

a) bestemmelser, der gør det muligt for kunden efter anmodning at skifte til en databehandlingstjeneste, der tilbydes af en anden udbyder af databehandlingstjenester, eller at portere alle eksporterbare data og digitale aktiver til en lokal IKT- infrastruktur uden unødigt forsinkelse og under alle omstændigheder ikke efter den obligatoriske maksimale overgangsperiode på 30 kalenderdage, som påbegyndes efter den maksimale opsigelsesfrist omhandlet i litra d), i løbet af hvilken tjenesteydelsesaftalen fortsat finder anvendelse, og hvori udbyderen af databehandlingstjenester skal:

i) yde rimelig bistand til kunden og tredjeparter, der er godkendt af kunden, i skifteprocessen

ii) handle med fornøden omhu for at opretholde forretningskontinuitet og fortsætte leveringen af de funktioner eller tjenester, der er omfattet af aftalen

iii) fremlægge klare oplysninger om kendte risici for kontinuitet i leveringen af funktionerne eller tjenesterne på vegne af kildeudbyderen af databehandlingstjenester

iv) sikre, at der opretholdes et højt sikkerhedsniveau i hele skifteprocessen, navnlig datasikkerhed under overførslen og fortsat datasikkerhed i den udtræksperiode, der er fastsat i litra g), i overensstemmelse med gældende EU-ret eller national ret

b) en forpligtelse for udbyderen af databehandlingstjenester til at støtte kundens exitstrategi, der er relevant for de aftalte tjenester, herunder ved at stille alle relevante oplysninger til rådighed

c) en bestemmelse om, at aftalen anses for at være ophørt, og at kunden skal underrettes om ophøret, i et af følgende tilfælde:

i) i givet fald efter vellykket afslutning på skifteprocessen

ii) ved udløbet af den maksimale opsigelsesfrist omhandlet i litra d), hvis kunden ikke ønsker at skifte, men at slette sine eksporterbare data og digitale aktiver ved tjenestens ophør

- d) en maksimal opsigelsesfrist for indledning af skifteprocessen, som ikke må overstige to måneder
- e) en udtømmende specifikation af alle kategorier af data og digitale aktiver, der kan porteres i skifteprocessen, herunder som minimum alle eksporterbare data
- f) en udtømmende specifikation af datakategorier, der er specifikke for udbyderens databehandlingstjenestes interne funktion, og som skal undtages fra de eksporterbare data i henhold til dette stykkes litra e), hvis der er risiko for brud på udbyderens forretningshemmeligheder, forudsat at sådanne undtagelser ikke hindrer eller forsinker skifteprocessen foreskrevet i artikel 23
- g) en minimumsperiode for dataudtræk på mindst 30 kalenderdage begyndende efter udløbet af den overgangsperiode, der er aftalt mellem kunden og udbyderen af databehandlingstjenester i overensstemmelse med dette stykkes litra a) og stk. 4
- h) en bestemmelse, der sikrer fuldstændig sletning af alle eksporterbare data og digitale aktiver, som er genereret direkte af kunden, eller som vedrører kunden direkte, efter udløbet af den i litra g) omhandlede udtræksperiode eller efter udløbet af en alternativ aftalt periode på en senere dato end den udløbsdato for udtræksperioden, der er omhandlet i litra g), forudsat at skifteprocessen er afsluttet på en vellykket måde
- i) skiftegebyrer, der kan pålægges af udbydere af databehandlingstjenester i henhold til artikel 29.

3. Aftalen omhandlet i stk. 1 skal indeholde bestemmelser om, at kunden kan underrette udbyderen af databehandlingstjenester om sin beslutning om at udføre en eller flere af følgende handlinger ved udløbet af den maksimale opsigelsesfrist omhandlet i stk. 2, litra d):

- a) skifte til en anden udbyder af databehandlingstjenester, i hvilket tilfælde kunden skal give de nødvendige oplysninger om den pågældende udbyder
- b) skifte til en lokal IKT- infrastruktur
- c) slette sine eksporterbare data og digitale aktiver.

4. Hvis den obligatoriske maksimale overgangsperiode som fastlagt i stk. 2, litra a), ikke er teknisk gennemførlig, underretter udbyderen af databehandlingstjenester kunden inden for 14 arbejdsdage efter indgivelse af anmodningen om skift og begrundet behørigt den manglende tekniske gennemførlighed og angiver en alternativ overgangsperiode, som ikke må overstige syv måneder. I overensstemmelse med stk. 1 skal der sikres driftskontinuitet i hele den alternative overgangsperiode.

5. Uden at det berører stk. 4, skal aftalen omhandlet i stk. 1 indeholde bestemmelser, der giver kunden ret til at forlænge overgangsperioden én gang med en periode, som kunden anser for at være mere hensigtsmæssig med henblik på dennes egne interesser.

Artikel 26

Oplysningspligt for udbydere af databehandlingstjenester

En udbyder af databehandlingstjenester giver kunder:

- a) oplysninger om tilgængelige procedurer for skift og portering til databehandlingstjenesten, herunder oplysninger om tilgængelige skifte- og porteringsmetoder og -formater samt restriktioner og tekniske begrænsninger, som udbyderen af databehandlingstjenester har kendskab til
- b) en henvisning til et ajourført onlineregister, der hostes af udbydere af databehandlingstjenester, med nærmere oplysninger om alle de datastrukturer og dataformater samt de relevante standarder og åbne interoperabilitetsspecifikationer, hvori de eksporterbare data, jf. artikel 25, stk. 2, litra e), skal være tilgængelige.

Artikel 27

Forpligtelse til god tro

Alle involverede parter, herunder destinationsudbydere af databehandlingstjenester, samarbejder i god tro om at gøre skifteprocessen effektiv, muliggøre rettidig overførsel af data og opretholde kontinuitet af databehandlingstjenesten.

Artikel 28

Kontraktlige gennemsigtighedsforpligtelser vedrørende international adgang og overførsel

1. Udbydere af databehandlingstjenester stiller følgende oplysninger til rådighed på deres websteder og ajourfører disse oplysninger:

- a) den jurisdiktion, som den IKT-infrastruktur, der anvendes til databehandling af deres individuelle tjenester, er underlagt
- b) en overordnet beskrivelse af de tekniske, organisatoriske og kontraktlige foranstaltninger, som udbyderen af databehandlingstjenester har truffet for at forhindre international statslig adgang til, eller overførsel af, andre data end personoplysninger, der er lagret i Unionen, hvis en sådan adgang eller overførsel ville være i strid med EU-retten eller den relevante medlemsstats nationale ret.

2. De websteder, der er omhandlet i stk. 1, skal anføres i aftaler om alle databehandlingstjenester, der tilbydes af udbydere af databehandlingstjenester.

Artikel 29

Gradvis fjernelse af skiftegebyrer

1. Fra den 12. januar 2027 må udbydere af databehandlingstjenester ikke pålægge kunder skiftegebyrer for skifteprocessen.
2. Fra den 11. januar 2024 til den 12. januar 2027 kan udbydere af databehandlingstjenester pålægge kunder nedsatte skiftegebyrer for skifteprocessen.
3. De nedsatte skiftegebyrer, der er omhandlet i stk. 2, må ikke overstige de omkostninger, som udbydere af databehandlingstjenester afholder, og som er direkte forbundet med den pågældende skifteproces.
4. Forud for indgåelse af en aftale med en kunde giver udbydere af databehandlingstjenester den potentielle kunde klare oplysninger om de standardtjenestegebyrer og sanktioner for for tidlig opsigelse, som kan pålægges, samt om de nedsatte skiftegebyrer, som kan pålægges i den i stk. 2 omhandlede tidsramme.
5. Hvor det er relevant, giver udbydere af databehandlingstjenester oplysninger til en kunde om databehandlingstjenester, der indebærer et særligt komplekst eller omkostningsfuldt skift, eller for hvilke det er umuligt at skifte uden betydelig indgriben i arkitekturen for data, digitale aktiver eller tjenester.
6. I givet fald gør udbydere af databehandlingstjenester de i stk. 4 og 5 omhandlede oplysninger offentligt tilgængelige for kunderne via et særligt afsnit på deres websted eller på en anden lettilgængelig måde.
7. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 45 for at supplere denne forordning ved at oprette en overvågningsmekanisme, således at Kommissionen kan overvåge skiftegebyrer, der pålægges af udbydere af databehandlingstjenester på markedet, for at sikre, at fjernelsen og nedsættelsen af skiftegebyrer i henhold til nærværende artikels stk. 1 og 2 gennemføres inden for de frister, der er fastsat i disse stykker.

Artikel 30

Tekniske aspekter af skift

1. Udbydere af databehandlingstjenester, der vedrører skalerbare og elastiske databehandlingsressourcer, som er begrænset til infrastrukturelle elementer såsom servere, netværk og de virtuelle ressourcer, der er nødvendige for at drive infrastruktur, men som ikke giver adgang til driftstjenester, software og applikationer, der lagres eller på anden måde behandles eller anvendes i disse infrastrukturelle elementer, træffer i overensstemmelse med artikel 27 alle rimelige foranstaltninger inden for rammerne af deres beføjelser for at lette, at kunden efter at have skiftet til en tjeneste, der dækker den samme tjenestetype, opnår funktionel ækvivalens ved anvendelse af destinationsdatabehandlingstjenesten. Kildeudbyderen af databehandlingstjenester letter skifteprocessen ved at stille kapacitet, tilstrækkelig oplysning, dokumentation, teknisk støtte og, hvor det er relevant, de nødvendige værktøjer til rådighed.

2. Andre udbydere af databehandlingstjenester end dem, der er omhandlet i stk. 1, stiller gratis åbne grænseflader til rådighed i lige høj grad for alle deres kunder og de berørte destinationsudbydere af databehandlingstjenester for at lette skifteprocessen. Disse grænseflader skal omfatte tilstrækkelige oplysninger om den pågældende tjeneste til at muliggøre udvikling af software, der skal kommunikere med tjenesterne, med henblik på dataportabilitet og interoperabilitet.

3. For andre databehandlingstjenester end dem, der er omhandlet i denne artikels stk. 1, sikrer udbydere af databehandlingstjenester kompatibilitet med fælles specifikationer baseret på åbne interoperabilitetsspecifikationer eller harmoniserede standarder for interoperabilitet senest 12 måneder efter, at henvisninger til fælles specifikationer eller harmoniserede standarder for databehandlingstjenesters interoperabilitet er offentliggjort i det centrale EU-standardiseringsregister for databehandlingstjenesters interoperabilitet efter offentliggørelse af de underliggende gennemførelsesretsakter i *Den Europæiske Unions Tidende* i overensstemmelse med artikel 35, stk. 8.

4. Udbydere af andre databehandlingstjenester end dem, der er omhandlet i denne artikels stk. 1, ajourfører onlineregistret omhandlet i artikel 26, litra b), i overensstemmelse med deres forpligtelser i henhold til nærværende artikels stk. 3.

5. I tilfælde af skift mellem tjenester af samme tjenestetype, for hvilke fælles specifikationer eller harmoniserede standarder for interoperabilitet omhandlet i denne artikels stk. 3 ikke er blevet offentliggjort i det centrale EU-standardiseringsregister for databehandlingstjenesters interoperabilitet i overensstemmelse med artikel 35, stk. 8, eksporterer udbyderen af databehandlingstjenesterne på kundens anmodning alle eksporterbare data i et struktureret, almindeligt anvendt og maskinlæsbart format.

6. Udbydere af databehandlingstjenester er ikke forpligtet til at udvikle nye teknologier eller tjenester eller videregive eller overføre digitale aktiver, som er beskyttede af intellektuelle ejendomsrettigheder eller udgør en forretningshemmelighed, til en kunde eller til en anden udbyder af databehandlingstjenester eller bringe kundens eller udbyderens sikkerhed og tjenesteintegriteten i fare.

Artikel 31

Særlig ordning for visse databehandlingstjenester

1. Forpligtelserne i artikel 23, litra d), artikel 29 og artikel 30, stk. 1 og 3, finder ikke anvendelse på databehandlingstjenester, hvis vigtigste elementer for størstedelens vedkommende er skræddersyet til at imødekomme en individuel kundes specifikke behov, eller hvor alle komponenter er udviklet med henblik på en individuel kunde, og hvor disse databehandlingstjenester ikke tilbydes i stor kommerciel målestok via tjenestekataloget for udbyderen af databehandlingstjenester.

2. De forpligtelser, der er fastsat i dette kapitel, finder ikke anvendelse på databehandlingstjenester, der leveres som en ikkeproduktionsversion med henblik på afprøvning og evaluering i en begrænset periode.

3. Forud for indgåelse af en aftale om levering af de databehandlingstjenester, der er omhandlet i denne artikel, informerer udbyderen af databehandlingstjenester potentielle kunder om de forpligtelser i dette kapitel, der ikke finder anvendelse.

KAPITEL VII

ULOVLIG INTERNATIONAL STATSIG ADGANG OG OVERFØRSEL AF ANDRE DATA END PERSONOPLYSNINGER

Artikel 32

International statslig adgang og overførsel

1. Udbydere af databehandlingstjenester træffer alle passende tekniske, organisatoriske og retlige foranstaltninger, herunder aftaler, for at forhindre international statslig adgang til og overførsel af og tredjelandes statslige adgang til og overførsel af andre data end personoplysninger, der er lagret i Unionen, hvis en sådan overførsel eller adgang ville være i strid med EU-retten eller med den relevante medlemsstats nationale ret, jf. dog stk. 2 eller 3.

2. Enhver afgørelse truffet eller dom afsagt af et tredjelandets domstol eller ret og enhver afgørelse truffet af et tredjelandes administrative myndighed, der kræver, at en udbyder af databehandlingstjenester overfører eller giver adgang til andre data end personoplysninger, der er omfattet af denne forordnings anvendelsesområde, og som er lagret i Unionen, anerkendes eller håndhæves kun på nogen måde, hvis den bygger på en international aftale såsom en traktat om gensidig retshjælp mellem det anmodende tredjeland og Unionen eller enhver sådan aftale mellem det anmodende tredjeland og en medlemsstat.

3. Hvis der ikke foreligger en international aftale som omhandlet i stk. 2, og en udbyder af databehandlingstjenester er adressat for en afgørelse truffet eller dom afsagt af et tredjelandets domstol eller ret eller en afgørelse truffet af et tredjelandes administrative myndighed om at overføre eller give adgang til andre data end personoplysninger, der er omfattet af denne forordnings anvendelsesområde, og som er lagret i Unionen, og hvis overholdelsen af en sådan afgørelse risikerer at medføre, at adressaten handler i strid med EU-retten eller med den relevante medlemsstats nationale ret, må overførslen af sådanne data til den pågældende tredjelandsmyndighed eller dennes adgang til sådanne data kun finde sted, hvis:

a) tredjelandets system kræver, at begrundelsen for og proportionaliteten af en sådan afgørelse eller dom angives, og at en sådan afgørelse eller dom er af specifik karakter, f.eks. ved at fastslå en tilstrækkelig forbindelse til visse mistænkte personer eller overtrædelser

b) en begrundet indsigelse fra adressaten kan prøves ved tredjelandets kompetente domstol eller ret, og

c) tredjelandets kompetente domstol eller ret, der udsteder afgørelsen eller dommen eller prøver en administrativ myndigheds afgørelse, i henhold til det pågældende tredjelandes ret har beføjelse til at tage

behørigt hensyn til de relevante retlige interesser hos den, der stiller de data til rådighed, som er beskyttet af EU-retten eller af den relevante medlemsstats nationale ret.

Adressaten for afgørelsen eller dommen kan anmode om en udtalelse fra det relevante nationale organ eller den relevante nationale myndighed, der er kompetent med hensyn til internationalt retligt samarbejde, med henblik på at fastslå, om betingelserne i første afsnit er opfyldt, navnlig hvis den finder, at afgørelsen kan vedrøre forretningshemmeligheder eller andre forretningsmæssigt følsomme oplysninger samt indhold, der er beskyttet af intellektuelle ejendomsrettigheder, eller at overførslen kan føre til genidentifikation. Det relevante nationale organ eller den relevante nationale myndighed kan høre Kommissionen. Hvis adressaten finder, at afgørelsen eller dommen kan påvirke Unionens eller dens medlemsstats nationale sikkerheds- eller forsvarsinteresser, beder den om en udtalelse fra det relevante nationale organ eller den relevante nationale myndighed for at fastslå, om de ønskede data vedrører Unionens eller dens medlemsstats nationale sikkerheds- eller forsvarsinteresser. Hvis adressaten ikke har modtaget svar inden for én måned, eller hvis det i udtalelsen fra et sådant organ eller en sådan myndighed konkluderes, at betingelserne i første afsnit ikke er opfyldt, kan adressaten give afslag på anmodningen om overførsel af eller adgang til andre data end personoplysninger med denne begrundelse.

EDIB, jf. artikel 42, rådgiver og bistår Kommissionen i forbindelse med udarbejdelse af retningslinjer for vurdering af, om betingelserne i dette stykkes første afsnit er opfyldt.

4. Hvis betingelserne i stk. 2 eller 3 er opfyldt, leverer udbyderen af databehandlingstjenester den mindste mængde data, der er tilladt som svar på en anmodning, på grundlag af en rimelig fortolkning af denne anmodning fra udbyderen eller det relevante kompetente organ eller den relevante kompetente myndighed, der er omhandlet i stk. 3, andet afsnit.

5. Udbyderen af databehandlingstjenester underretter kunden om, at der foreligger en anmodning fra et tredjelandsmyndighed om at få adgang til vedkommendes data, inden den pågældende anmodning imødekommes, undtagen i tilfælde, hvor anmodningen tjener retshåndhævelsesformål, og så længe dette er nødvendigt for at bevare retshåndhævelsesaktivitetens effektivitet.

KAPITEL VIII

INTEROPERABILITET

Artikel 33

Væsentlige krav vedrørende interoperabilitet mellem data, mellem datadelingsmekanismer og -tjenester og mellem fælles europæiske dataområder

1. Deltagere i dataområder, der udbyder data eller datatjenester til andre deltagere, opfylder følgende væsentlige krav for at lette interoperabilitet mellem data, mellem datadelingsmekanismer og -tjenester og mellem fælles europæiske dataområder, som er formåls- eller sektorspecifikke eller tværsektorielle interoperable rammer for fælles standarder og praksis med hensyn til deling eller fælles behandling

af data med henblik på bl.a. udvikling af nye produkter og tjenester, videnskabelig forskning eller civilsamfundsinitiativer:

- a) datasætindhold, anvendelsesbegrænsninger, licenser, dataindsamlingsmetoder, datakvalitet og usikkerhed skal, i givet fald i et maskinlæsbart format, beskrives tilstrækkeligt til, at modtageren kan finde, få adgang til og anvende dataene
- b) datastrukturer, dataformater, ordlister, klassifikationsordninger, taksonomier og kodelister skal, hvis de er tilgængelige, beskrives på en offentligt tilgængelig og sammenhængende måde
- c) de tekniske midler til at få adgang til dataene såsom programmeringsgrænseflader for applikationer og betingelserne for deres anvendelse og tjenestekvalitet skal beskrives tilstrækkeligt til at muliggøre automatisk adgang til og overførsel af data mellem parter, herunder kontinuerligt, som massedownloads eller i realtid i et maskinlæsbart format, hvis det er teknisk muligt og ikke hindrer, at det forbundne produkt fungerer tilfredsstillende
- d) i givet fald midler til at muliggøre interoperabilitet mellem værktøjer til automatisk gennemførelse af datadelingsaftaler såsom intelligente kontrakter skal tilvejebringes.

Kravene kan være generiske eller vedrøre specifikke sektorer, samtidig med at der tages fuldt hensyn til sammenhængen med krav fra anden EU-ret eller national ret.

2. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 45 for at supplere denne forordning ved yderligere at præcisere de væsentlige krav i nærværende artikels stk. 1, vedrørende de pågældende krav, som i medfør af deres karakter ikke kan skabe den tilsigtede virkning, medmindre de præciseres yderligere i bindende EU-retsakter, og med henblik på på behørig vis at afspejle den teknologiske udvikling og markedsudviklingen.

Kommissionen tager ved vedtagelsen af delegerede retsakter hensyn til EDIB's rådgivning i overensstemmelse med artikel 42, litra c), nr. iii).

3. Deltagerne i dataområder, der udbyder data eller datatjenester til andre deltagere i dataområder, som opfylder de harmoniserede standarder eller dele heraf, hvis reference er offentliggjort i Den Europæiske Unions Tidende, formodes at være i overensstemmelse med de væsentlige krav i stk. 1, for så vidt som disse krav er dækket af sådanne harmoniserede standarder eller dele heraf.

4. Kommissionen anmoder i henhold til artikel 10 i forordning (EU) nr. 1025/2012 én eller flere europæiske standardiseringsorganisationer om at udarbejde harmoniserede standarder, der opfylder de væsentlige krav i nærværende artikels stk. 1.

5. Kommissionen kan ved hjælp af gennemførelsesretsakter vedtage fælles specifikationer, der opfylder ethvert eller alle de væsentlige krav i stk. 1, hvis følgende betingelser er opfyldt:

a) Kommissionen har i henhold til artikel 10, stk. 1, i forordning (EU) nr. 1025/2012, anmodet en eller flere europæiske standardiseringsorganisationer om at udarbejde en harmoniseret standard, der opfylder de væsentlige krav i nærværende artikels stk. 1, og:

i) anmodningen er ikke blevet imødekommet

ii) de harmoniserede standarder, der omhandler anmodningen, er ikke leveret inden for den tidsfrist, der er fastsat i overensstemmelse med artikel 10, stk. 1, i forordning (EU) nr. 1025/2012, eller

iii) de harmoniserede standarder efterlever ikke anmodningen, og

b) ingen reference til harmoniserede standarder, der dækker de relevante væsentlige krav i denne artikels stk. 1, er offentliggjort i Den Europæiske Unions Tidende i overensstemmelse med i forordning (EU) nr. 1025/2012, og ingen reference af denne art forventes at blive offentliggjort inden for et rimeligt tidsrum.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 46, stk. 2.

6. Inden Kommissionen udarbejder et udkast til gennemførelsesretsakt omhandlet i denne artikels stk. 5, underretter den det udvalg, der er omhandlet i artikel 22 i forordning (EU) nr. 1025/2012, om, at den anser betingelserne i nærværende artikels stk. 5 for opfyldt.

7. Ved udarbejdelsen af udkastet til gennemførelsesretsakt omhandlet i stk. 5 tager Kommissionen hensyn til EDIB's rådgivning og andre relevante organers eller ekspertgruppers synspunkter og hører på behørig vis alle relevante interessenter.

8. Deltagerne i dataområder, der udbyder data eller datatjenester til andre deltagere i dataområder, som opfylder de fælles specifikationer, der er fastsat ved gennemførelsesretsakter omhandlet i stk. 5 eller dele heraf, formodes at være i overensstemmelse med de væsentlige krav i stk. 1, for så vidt som disse krav er dækket af sådanne fælles specifikationer eller dele heraf.

9. Hvis en harmoniseret standard vedtages af en europæisk standardiseringsorganisation og foreslås Kommissionen med henblik på offentliggørelse af en reference hertil i Den Europæiske Unions Tidende, vurderer Kommissionen den harmoniserede standard i overensstemmelse med forordning (EU) nr. 1025/2012. Hvor referencen for en harmoniseret standard offentliggøres i Den Europæiske Unions Tidende, ophæver Kommissionen den gennemførelsesretsakt, der er omhandlet i denne artikels stk. 5, eller dele heraf, som dækker de samme væsentlige krav som dem, der er dækket af denne harmoniserede standard.

10. Hvis en medlemsstat finder, at en fælles specifikation ikke lever helt op til de væsentlige krav i stk. 1, underretter medlemsstaten Kommissionen herom ved at indgive en udførlig forklaring. Kommissionen vurderer denne udførlige forklaring og kan, hvis det er hensigtsmæssigt, ændre den gennemførelsesretsakt, som fastsætter den pågældende fælles specifikation.

11. Kommissionen kan under hensyntagen til forslaget fra EDIB vedtage retningslinjer i overensstemmelse med artikel 30, litra h), i forordning (EU) 2022/868, der fastsætter interoperable rammer for fælles standarder og praksis med henblik på fælles europæiske dataområders funktion.

Artikel 34

Interoperabilitet med henblik på parallel anvendelse af databehandlingstjenester

1. Kravene i artikel 23 og 24, artikel 25, stk. 2, litra a), nr. ii) og iv), og litra e) og f), og artikel 30, stk. 2-5, finder også tilsvarende anvendelse på udbydere af databehandlingstjenester for at lette interoperabilitet med henblik på parallel anvendelse af databehandlingstjenester.
2. Hvor en databehandlingstjeneste anvendes parallelt med en anden databehandlingstjeneste, kan udbyderen af databehandlingstjenester pålægge gebyrer for udgående dataoverførsel, men kun med henblik på at overvælte påløbne omkostninger ved udgående dataoverførsel og uden at overstige sådanne omkostninger.

Artikel 35

Interoperabilitet mellem databehandlingstjenester

1. Åbne interoperabilitetsspecifikationer og harmoniserede standarder for interoperabilitet mellem databehandlingstjenester
 - a) skal, hvor det er teknisk muligt, opnå interoperabilitet mellem forskellige databehandlingstjenester, der dækker samme tjenestetype
 - b) skal øge portabiliteten af digitale aktiver mellem forskellige databehandlingstjenester, der dækker samme tjenestetype
 - c) skal, hvor det er teknisk muligt, lette funktionel ækvivalens mellem forskellige tjenester, der er omhandlet i artikel 30, stk. 1, og som dækker samme tjenestetype
 - d) må ikke have en negativ indvirkning på databehandlingstjenesters og datas sikkerhed og integritet
 - e) skal udformes på en sådan måde, at tekniske fremskridt og medtagelse af nye funktioner og innovation inden for databehandlingstjenester tillades.
2. Åbne interoperabilitetsspecifikationer og harmoniserede standarder for interoperabilitet mellem databehandlingstjenester skal på passende vis omhandle:
 - a) cloudinteroperabilitetsaspekterne af transportinteroperabilitet, syntaktisk interoperabilitet, semantisk datainteroperabilitet, adfærdsmæssig interoperabilitet og politikinteroperabilitet

b) clouddataportabilitetsaspekterne af datasyntaktisk portabilitet, datasemantisk portabilitet og datapolitikportabilitet

c) cloudapplikationsaspekterne af applikationssyntaktisk portabilitet, applikationsinstruksportabilitet, applikationsmetadataportabilitet, applikationsadfærdsportabilitet og applikationspolitikportabilitet.

3. Åbne interoperabilitetsspecifikationer skal efterleve bilag II til forordning (EU) nr. 1025/2012.

4. Under hensyntagen til relevante internationale og europæiske standarder og selvreguleringsinitiativer kan Kommissionen i overensstemmelse med artikel 10, stk. 1, i forordning (EU) nr. 1025/2012 anmode en eller flere europæiske standardiseringsorganisationer om at udarbejde harmoniserede standarder, der opfylder de væsentlige krav i nærværende artikels stk. 1 og 2.

5. Kommissionen kan ved hjælp af gennemførelsesretsakter vedtage fælles specifikationer på grundlag af åbne interoperabilitetsspecifikationer, der dækker alle de væsentlige krav i stk. 1 og 2.

6. Ved udarbejdelsen af udkastet til gennemførelsesretsakt omhandlet i denne artikels stk. 5 tager Kommissionen hensyn til synspunkterne fra de relevante kompetente myndigheder omhandlet i artikel 37, stk. 5, litra h), og fra andre relevante organer eller ekspertgrupper og hører på behørig vis alle relevante interessenter.

7. Hvis en medlemsstat finder, at en fælles specifikation ikke lever helt op til de væsentlige krav i stk. 1 og 2, underretter medlemsstaten Kommissionen herom ved at indgive en udførlig forklaring. Kommissionen vurderer denne udførlige forklaring og kan, hvis det er hensigtsmæssigt, ændre den gennemførelsesretsakt, der fastsætter den pågældende fælles specifikation.

8. Med henblik på artikel 30, stk. 3, offentliggør Kommissionen ved hjælp af gennemførelsesretsakter referencerne for harmoniserede standarder og fælles specifikationer for databehandlingstjenesters interoperabilitet i et centralt EU-standardiseringsregister for databehandlingstjenesters interoperabilitet.

9. De gennemførelsesretsakter, der er omhandlet i denne artikel, vedtages efter undersøgelsesproceduren, jf. artikel 46, stk. 2.

Artikel 36

Væsentlige krav vedrørende intelligente kontrakter med henblik på gennemførelse af aftaler om datadeling

1. Leverandøren af en applikation, der anvender intelligente kontrakter, eller i mangel heraf en person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med gennemførelse af en aftale eller en del heraf om at stille data til rådighed, sikrer, at disse intelligente kontrakter opfylder følgende væsentlige krav om:

a) robusthed og adgangskontrol for at sikre, at den intelligente kontrakt indeholder mekanismer til adgangskontrol og en meget høj grad af robusthed for at undgå funktionsfejl og modstå tredjeparters manipulation

b) sikker afslutning og afbrydelse for at sikre, at der findes en mekanisme til at bringe fortsat udførelse af transaktioner til ophør, og at den intelligente kontrakt omfatter interne funktioner, som kan nulstille aftalen eller instruere den om at afslutte eller afbryde sin funktion, navnlig for at undgå fremtidige utilsigtede udførelser

c) dataarkivering og datakontinuitet for under omstændigheder, hvor en intelligent kontrakt skal afsluttes eller deaktiveres, at sikre, at der er en mulighed for at arkivere transaktionsdataene og den intelligente kontrakts logik og kode for at bevare registreringen af operationer, der tidligere er udført med dataene (mulighed for revision)

d) adgangskontrol for at sikre, at en intelligent kontrakt er beskyttet med strenge mekanismer til adgangskontrol både på styrings- og kontraktniveau, og

e) overensstemmelse for at sikre overensstemmelse med betingelserne i den datadelingsaftale, som den intelligente kontrakt gennemfører.

2. Leverandøren af en intelligent kontrakt eller i mangel heraf en person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med udførelse af en aftale eller en del heraf om at stille data til rådighed, skal foretage en overensstemmelsesvurdering med henblik på at opfylde de væsentlige krav i stk. 1 og, når disse krav er opfyldt, udstede en EU-overensstemmelseserklæring.

3. Ved at udarbejde en EU-overensstemmelseserklæring er leverandøren af en applikation, der anvender intelligente kontrakter, eller i mangel heraf en person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med udførelse af en aftale eller en del heraf om at stille data til rådighed, ansvarlig for at opfylde de væsentlige krav i stk. 1.

4. En intelligent kontrakt, der er i overensstemmelse med de harmoniserede standarder eller de relevante dele heraf, og hvis referencer er offentliggjort i Den Europæiske Unions Tidende, formodes at være i overensstemmelse med de væsentlige krav i stk. 1, for så vidt som disse krav er dækket af sådanne harmoniserede standarder eller dele heraf.

5. Kommissionen anmoder i henhold til artikel 10 i forordning (EU) nr. 1025/2012 én eller flere europæiske standardiseringsorganisationer om at udarbejde harmoniserede standarder, der opfylder de væsentlige krav i nærværende artikels stk. 1.

6. Kommissionen kan ved hjælp af gennemførelsesretsakter vedtage fælles specifikationer, der dækker ethvert eller alle de væsentlige krav i stk. 1, hvis følgende betingelser er opfyldt:

a) Kommissionen har i henhold til artikel 10, stk. 1, i forordning (EU) nr. 1025/2012 anmodet en eller flere europæiske standardiseringsorganisationer om at udarbejde en harmoniseret standard, der opfylder de væsentlige krav i nærværende artikels stk. 1, og:

i) anmodningen er ikke blevet imødekommet

ii) de harmoniserede standarder, der omhandler anmodningen, er ikke leveret inden for den tidsfrist, som er fastsat i overensstemmelse med artikel 10, stk. 1, i forordning (EU) nr. 1025/2012, eller

iii) de harmoniserede standarder efterlever ikke anmodningen, og

b) ingen reference til harmoniserede standarder, der dækker de relevante væsentlige krav i denne artikels stk. 1, er offentliggjort i Den Europæiske Unions Tidende i overensstemmelse med forordning (EU) nr. 1025/2012, og ingen reference af denne art forventes at blive offentliggjort inden for et rimeligt tidsrum.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 46, stk. 2.

7. Inden Kommissionen udarbejder et udkast til gennemførelsesretsakt omhandlet i denne artikels stk. 6, underretter den det udvalg, der er omhandlet i artikel 22 i forordning (EU) nr. 1025/2012, om, at den anser betingelserne i nærværende artikels stk. 6 for opfyldt.

8. Ved udarbejdelsen af udkastet til gennemførelsesretsakt som omhandlet i stk. 6 tager Kommissionen hensyn til EDIB's rådgivning og andre relevante organers eller ekspertgruppers synspunkter og hører på behørig vis alle relevante interessenter.

9. Leverandøren af en intelligent kontrakt eller i mangel heraf en person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med udførelse af en aftale eller en del heraf om at stille data til rådighed, der opfylder de fælles specifikationer, som er fastsat ved gennemførelsesretsakter som omhandlet i stk. 6 eller dele heraf, formodes at være i overensstemmelse med de væsentlige krav i stk. 1, for så vidt som disse krav er dækket af sådanne fælles specifikationer eller dele deraf.

10. Hvis en harmoniseret standard vedtages af en europæisk standardiseringsorganisation og foreslås af Kommissionen med henblik på offentliggørelse af en reference hertil i *Den Europæiske Unions Tidende*, vurderer Kommissionen den harmoniserede standard i overensstemmelse med forordning (EU) nr. 1025/2012. Hvor referencen for en harmoniseret standard offentliggøres i *Den Europæiske Unions Tidende*, ophæver Kommissionen de gennemførelsesretsakter, der er omhandlet i denne artikels stk. 6, eller dele deraf, som omfatter de samme væsentlige krav som dem, der er dækket af denne harmoniserede standard.

11. Hvis en medlemsstat finder, at en fælles specifikation ikke lever helt op til de væsentlige krav i stk. 1, underretter medlemsstaten Kommissionen herom ved at indgive en udførlig forklaring. Kommissionen vurderer denne udførlige forklaring og kan, hvis det er hensigtsmæssigt, ændre den gennemførelsesretsakt, som fastsætter den pågældende fælles specifikation.

KAPITEL IX

GENNEMFØRELSE OG HÅNDHÆVELSE

Artikel 37

Kompetente myndigheder og datakoordinatorer

1. Hver medlemsstat udpeger én eller flere kompetente myndigheder til at have ansvaret for anvendelsen og håndhævelsen af denne forordning (kompetente myndigheder). Medlemsstaterne kan oprette en eller flere nye myndigheder eller forlade sig på eksisterende myndigheder.

2. Hvis en medlemsstat udpeger mere end én kompetent myndighed, udpeger den en datakoordinator blandt dem for at lette samarbejdet mellem de kompetente myndigheder og for at bistå enheder inden for denne forordnings anvendelsesområde i forbindelse med alle spørgsmål vedrørende dens anvendelse og håndhævelse. Kompetente myndigheder samarbejder med hinanden ved udøvelsen af de opgaver og beføjelser, som de er tillagt i henhold til stk. 5.

3. De tilsynsmyndigheder, der er ansvarlige for at overvåge anvendelsen af forordning (EU) 2016/679, er ansvarlige for at overvåge anvendelsen af nærværende forordning for så vidt angår beskyttelse af personoplysninger. Kapitel VI og VII i forordning (EU) 2016/679 finder tilsvarende anvendelse.

Den Europæiske Tilsynsførende for Databeskyttelse er ansvarlig for overvågning af nærværende forordnings anvendelse, for så vidt som den vedrører Kommissionen, Den Europæiske Centralbank eller EU-organer. Hvor det er relevant, finder artikel 62 i forordning (EU) 2018/1725 tilsvarende anvendelse.

Tilsynsmyndighedernes opgaver og beføjelser omhandlet i dette stykke udøves i forbindelse med behandling af personoplysninger.

4. Uden at det berører denne artikels stk. 1:

a) skal sektormyndighedernes kompetence i forbindelse med specifikke sektorbestemte spørgsmål vedrørende dataadgang og -anvendelse i forbindelse med gennemførelsen af denne forordning respekteres

b) skal den kompetente myndighed, der er ansvarlig for anvendelsen og håndhævelsen af artikel 23-31, 34 og 3, have erfaring inden for områderne data og elektroniske kommunikationstjenester.

5. Medlemsstaterne sikrer, at opgaverne og beføjelserne for de kompetente myndigheder er klart definerede og omfatter at:

a) fremme datakompetence og -bevidsthed blandt brugere og enheder, der er omfattet af denne forordnings anvendelsesområde, om rettigheder og forpligtelser i henhold til denne forordning

b) behandle klager over påståede overtrædelser af denne forordning, herunder vedrørende forretningshemmeligheder, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og løbende

underrette klagerne, hvis det er relevant i henhold til national ret, om forløbet og resultatet af undersøgelsen inden for en rimelig frist, navnlig hvis yderligere undersøgelse eller koordinering med en anden kompetent myndighed er nødvendig

c) foretage undersøgelser om spørgsmål, der vedrører anvendelsen af denne forordning, herunder på grundlag af oplysninger, der er modtaget fra en anden kompetent myndighed eller en anden offentlig myndighed

d) pålægge økonomiske sanktioner, der er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning, og som kan omfatte periodiske sanktioner og sanktioner med tilbagevirkende kraft, eller indlede retsforfølgning med henblik på at pålægge bøder

e) overvåge den teknologiske og relevante kommercielle udvikling af relevans for tilrådighedsstillelsen og anvendelsen af data

f) samarbejde med andre medlemsstaters kompetente myndigheder og, hvis det er relevant, Kommissionen eller EDIB for at sikre ensartet og effektiv anvendelse af denne forordning, herunder udveksling af alle relevante oplysninger ad elektronisk vej uden unødigt ophold, herunder med hensyn til denne artikels stk. 10

g) samarbejde med de relevante kompetente myndigheder, der er ansvarlige for gennemførelsen af andre EU-retsakter eller nationale retsakter, herunder med myndigheder med kompetence inden for områderne data og elektroniske kommunikationstjenester, med den tilsynsmyndighed, der er ansvarlig for at overvåge anvendelsen af forordning (EU) 2016/679, eller med sektormyndigheder for at sikre, at nærværende forordning håndhæves i overensstemmelse med anden EU-ret og national ret

h) samarbejde med de relevante kompetente myndigheder for at sikre, at forpligtelserne i artikel 23-31, 34 og 35 håndhæves i overensstemmelse med anden EU-ret og selvregulering, der gælder for udbydere af databehandlingstjenester

i) sikre, at skiftegebyrer mellem udbydere af databehandlingstjenester fjernes i overensstemmelse med artikel 29

j) behandle anmodninger om data fremsat i henhold til kapitel V.

Hvis der er udpeget en datakoordinator, letter denne det i første afsnit, litra f), g) og h), omhandlede samarbejde og bistår de kompetente myndigheder på deres anmodning.

6. Datakoordinatoren skal, hvis en sådan kompetent myndighed er udpeget:

a) fungere som et enkelt kontaktpunkt for alle spørgsmål vedrørende denne forordnings anvendelse

b) sikre offentlig onlineadgang til offentlige myndigheders anmodninger om at stille data til rådighed i tilfælde af ekstraordinært behov i henhold til kapitel V og fremme frivillige aftaler om datadeling mellem offentlige myndigheder og dataindehavere

c) underrette Kommissionen hvert år om de afslag, der er meddelt i henhold til artikel 4, stk. 2 og 8, og artikel 5, stk. 11.

7. Medlemsstaterne underretter Kommissionen om navnene på de kompetente myndigheder og om deres opgaver og beføjelser samt, i givet fald, navnet på datakoordinatoren. Kommissionen fører et offentligt register over disse myndigheder.

8. De kompetente myndigheder skal ved udførelsen af deres opgaver og udøvelsen af deres beføjelser i henhold til denne forordning være upartiske og frie for udefrakommende indflydelse, det være sig direkte eller indirekte, og må hverken søge eller modtage instrukser med henblik på enkeltsager fra nogen anden offentlig myndighed eller nogen privat part.

9. Medlemsstaterne sikrer, at de kompetente myndigheder har tilstrækkelige menneskelige og tekniske ressourcer og relevant ekspertise til effektivt at kunne udføre deres opgaver i overensstemmelse med denne forordning.

10. Enheder, der er omfattet af denne forordnings anvendelsesområde, er underlagt kompetencen i den medlemsstat, hvor enheden er etableret. Hvis en enhed er etableret i mere end én medlemsstat, anses den for at høre under kompetencen i den medlemsstat, hvor den har sin hovedvirksomhed, dvs. hvor enheden har sit hovedkontor eller vedtægtsmæssige hjemsted, hvorfra de vigtigste finansielle funktioner og den operationelle kontrol udøves.

11. Enhver enhed, der er omfattet af denne forordnings anvendelsesområde, som stiller forbundne produkter til rådighed eller udbyder tjenester i Unionen, og som ikke er etableret i Unionen, udpeger en retlig repræsentant i en af medlemsstaterne.

12. For at sikre overholdelse af denne forordning bemyndiger en enhed, der er omfattet af denne forordnings anvendelsesområde, og som stiller forbundne produkter til rådighed eller udbyder tjenester i Unionen, en retlig repræsentant, som der skal rettes henvendelse til i tillæg til eller i stedet for enheden af de kompetente myndigheder med hensyn til alle spørgsmål vedrørende den pågældende enhed. Denne retlige repræsentant samarbejder med og dokumenterer udførligt på anmodning over for de kompetente myndigheder, hvilke tiltag der er iværksat, og hvilke bestemmelser der er indført af den enhed, der er omfattet af denne forordnings anvendelsesområde, og som stiller forbundne produkter til rådighed eller udbyder tjenester i Unionen, for at sikre, at denne forordning overholdes.

13. En enhed, der er omfattet af denne forordnings anvendelsesområde, og som stiller forbundne produkter til rådighed eller udbyder tjenester i Unionen, anses for at høre under den medlemsstats kompetence, hvor dens retlige repræsentant befinder sig. En sådan enheds udpegelse af en retlig repræsentant berører ikke en sådan enheds ansvar og eventuelle retlige skridt, som måtte blive taget over for en sådan enhed. Indtil en enhed udpeger en retlig repræsentant i overensstemmelse med denne artikel, hører den under alle medlemsstaternes kompetence med henblik på i givet fald at sikre anvendelse og håndhævelse af denne forordning. Enhver kompetent myndighed kan udøve sin kompetence, herunder ved at pålægge sanktioner, der er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning, forudsat at enheden ikke er genstand for håndhævelsesprocedurer i henhold til denne forordning vedrørende de samme forhold af en anden kompetent myndighed.

14. De kompetente myndigheder har beføjelse til at anmode brugere, dataindehavere eller datamodtagere eller deres retlige repræsentanter, der hører under deres medlemsstats kompetence, om alle oplysninger, som er nødvendige for at kontrollere efterlevelsen af denne forordning. Enhver anmodning om oplysninger skal stå i et rimeligt forhold til, hvad den underliggende opgave kræver, og være begrundet.

15. Hvis en kompetent myndighed i én medlemsstat anmoder om bistand eller håndhævelsesforanstaltninger fra en kompetent myndighed i en anden medlemsstat, indgiver den en begrundet anmodning. Ved modtagelsen af en sådan anmodning giver en kompetent myndighed uden unødigt ophold et svar med nærmere oplysninger om de tiltag, der er iværksat eller påtænkes iværksat.

16. De kompetente myndigheder overholder principperne om fortrolighed og om tavshedspligt og forretningshemmeligheder og beskytter personoplysninger i overensstemmelse med EU-retten eller national ret. Alle oplysninger, der udveksles i forbindelse med en anmodning om bistand, og som gives i henhold til denne artikel, må kun anvendes i forbindelse med den sag, hvortil der blev anmodet om oplysningerne.

Artikel 38

Ret til at indgive klage

1. Uden at det berører andre administrative klageadgange eller retsmidler, har fysiske og juridiske personer ret til at indgive en klage individuelt eller, hvor det er relevant, kollektivt til den relevante kompetente myndighed i den medlemsstat, hvor de har deres sædvanlige opholdssted, arbejdssted eller forretningssted, hvis de finder, at deres rettigheder i henhold til denne forordning er blevet krænket. Datakoordinatoren giver efter anmodning alle nødvendige oplysninger til fysiske og juridiske personer med henblik på indgivelsen af deres klage til den relevante kompetente myndighed.

2. Den kompetente myndighed, som klagen er indgivet til, underretter i overensstemmelse med national ret klageren om forløbet af sagen og om den trufne afgørelse.

3. De kompetente myndigheder samarbejder om at behandle og afgøre klager effektivt og rettidigt, herunder ved at udveksle alle relevante oplysninger ad elektronisk vej uden unødigt ophold. Dette samarbejde berører ikke de samarbejds mekanismer, der er fastsat i kapitel VI og VII i forordning (EU) 2016/679 og i forordning (EU) 2017/2394.

Artikel 39

Ret til effektive retsmidler

1. Uanset eventuelle administrative eller andre udenretslige midler har alle berørte fysiske og juridiske personer ret til effektive retsmidler med hensyn til juridisk bindende afgørelser truffet af kompetente myndigheder.

2. Hvis en kompetent myndighed undlader at reagere på en klage, har alle berørte fysiske og juridiske personer i overensstemmelse med national ret enten ret til effektive retsmidler eller adgang til prøvelse ved et uvildigt organ med passende ekspertise.

3. En sag i medfør af denne artikel anlægges ved domstolene eller retterne i medlemsstaten for den kompetente myndighed, mod hvem retsmidlet søges, enten enkeltvis eller, hvis det er relevant, i fællesskab af repræsentanter for én eller flere fysiske eller juridiske personer.

Artikel 40

Sanktioner

1. Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af denne forordning, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning.

2. Medlemsstaterne giver senest den 12. september 2025 Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om senere ændringer, der berører dem. Kommissionen ajourfører regelmæssigt og fører et lettilgængeligt offentligt register over disse foranstaltninger.

3. Medlemsstaterne tager hensyn til anbefalingerne fra EDIB og følgende ikkeudtømmende kriterier for pålæggelse af sanktioner for overtrædelser af denne forordning:

- a) overtrædelsens art, grovhed, omfang og varighed
- b) eventuelle tiltag, som den overtrædende part har truffet for at afbøde eller afhjælpe den skade, der er forårsaget af overtrædelserne
- c) den overtrædende parts eventuelle tidligere overtrædelser
- d) de økonomiske fordele eller tab, som den overtrædende part har opnået eller undgået som følge af overtrædelserne, for så vidt som disse fordele eller tab kan fastslås på en pålidelig måde
- e) eventuelle andre skærpende eller formildende faktorer i lyset af sagens omstændigheder
- f) den overtrædende parts årlige omsætning i det foregående regnskabsår i Unionen.

4. For så vidt angår overtrædelser af de forpligtelser, der er fastsat i denne forordnings kapitel II, III og V, kan de tilsynsmyndigheder, der er ansvarlige for overvågning af anvendelsen af forordning (EU) 2016/679, inden for rammerne af deres beføjelser pålægge administrative bøder i overensstemmelse med artikel 83 i forordning (EU) 2016/679 op til det beløb, der er omhandlet i artikel 83, stk. 5, i nævnte forordning.

5. For så vidt angår overtrædelser af de forpligtelser, der er fastsat i denne forordnings kapitel V, kan Den Europæiske Tilsynsførende for Databeskyttelse inden for rammerne af sine beføjelser pålægge administrative bøder i overensstemmelse med artikel 66 i forordning (EU) 2018/1725 op til det beløb, der er omhandlet i artikel 66, stk. 3, i nævnte forordning.

Artikel 41

Model for aftalevilkår og standardkontraktbestemmelser

Inden den 12. september 2025 udvikler og anbefaler Kommissionen en ikkebindende model for aftalevilkår for dataadgang og -anvendelse, herunder betingelser vedrørende rimelig godtgørelse og beskyttelse af forretningshemmeligheder, og ikkebindende standardkontraktbestemmelser for cloudcomputingaftaler for at bistå parterne med at udarbejde og forhandle aftaler med fair, rimelige og ikkeforskelsbehandlende kontraktlige rettigheder og forpligtelser.

Artikel 42

EDIB's rolle

EDIB, der af Kommissionen er oprettet som en ekspertgruppe i henhold til artikel 29 i forordning (EU) 2022/868, og hvori de kompetente myndigheder skal være repræsenteret, støtter en konsekvent anvendelse af nærværende forordning ved at:

a) rådgive og bistå Kommissionen med hensyn til at udvikle konsekvent praksis hos de kompetente myndigheder for håndhævelse af kapitel II, III, V og VII

b) lette samarbejde mellem de kompetente myndigheder gennem kapacitetsopbygning og udveksling af oplysninger, navnlig ved at fastlægge metoder til effektiv udveksling af oplysninger vedrørende håndhævelsen af rettigheder og forpligtelser i henhold til kapitel II, III og V i grænseoverskridende sager, herunder koordinering med hensyn til fastsættelse af sanktioner

c) rådgive og bistå Kommissionen med hensyn til:

i) om der skal anmodes om udarbejdelse af harmoniserede standarder, jf. artikel 33, stk. 4, artikel 35, stk. 4, og artikel 36, stk. 5

ii) udarbejdelse af de gennemførelsesretsakter, der er omhandlet i artikel 33, stk. 5, artikel 35, stk. 5 og 8, og artikel 36, stk. 6

iii) udarbejdelse af de delegerede retsakter, der er omhandlet i artikel 29, stk. 7, og artikel 33, stk. 2, og

iv) vedtagelse af de retningslinjer, der fastsætter interoperable rammer for fælles standarder og praksis for fælles europæiske dataområders funktion, jf. artikel 33, stk. 11.

KAPITEL X

***SUI GENERIS*-RET I HENHOLD TIL DIREKTIV 96/9/EF**

Artikel 43

Databaser med visse data

Sui generis-retten fastsat i artikel 7 i direktiv 96/9/EF finder ikke anvendelse, når data er indhentet fra eller genereret af et forbundet produkt eller en relateret tjeneste, der er omfattet af denne forordnings anvendelsesområde, navnlig vedrørende denne forordnings artikel 4 og 5.

KAPITEL XI

AFSLUTTENDE BESTEMMELSER

Artikel 44

Andre EU-retsakter, hvorved rettigheder og forpligtelser vedrørende adgang til og anvendelse af data reguleres

1. De specifikke forpligtelser vedrørende tilgængeliggørelse af data mellem virksomheder, mellem virksomheder og forbrugere og undtagelsesvis mellem virksomheder og offentlige organer i EU-retsakter, der trådte i kraft senest den 11. januar 2024, og delegerede retsakter eller gennemførelsesretsakter i henhold til disse EU-retsakter, berøres ikke.

2. Denne forordning berører ikke EU-ret, der i lyset af behov i en sektor, et fælles europæisk dataområde eller på et område af offentlig interesse fastsætter yderligere krav, navnlig vedrørende:

- a) tekniske aspekter af adgang til data
- b) begrænsninger af dataindehaveres ret til at få adgang til eller anvende visse data leveret af brugere
- c) aspekter ud over adgang til og anvendelse af data.

3. Denne forordning berører med undtagelse af kapitel V ikke EU-ret eller national ret, der indeholder bestemmelser om adgang til og tilladelse til anvendelse af data til videnskabelige forskningsformål.

Artikel 45

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.
2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 29, stk. 7, og artikel 33, stk. 2, tillægges Kommissionen for en ubegrænset periode fra den 11. januar 2024.
3. Den i artikel 29, stk. 7, og artikel 33, stk. 2, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.
4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.
5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.
6. En delegeret retsakt vedtaget i henhold til artikel 29, stk. 7, eller artikel 33, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på tre måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med tre måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 46

Udvalgsprocedure

1. Kommissionen består af udvalget nedsat ved forordning (EU) 2022/868. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.
2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

*Artikel 47***Ændring af forordning (EU) 2017/2394**

I bilaget til forordning (EU) 2017/2394 tilføjes følgende punkt:

»29. Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserede regler om fair adgang til og anvendelse af data og om ændring af forordning (EU) 2017/2394 og direktiv (EU) 2020/1828 (dataforordningen) (EUT L 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).«

*Artikel 48***Ændring af direktiv (EU) 2020/1828**

I bilag I til direktiv (EU) 2020/1828 tilføjes følgende punkt:

»68. Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserede regler om fair adgang til og anvendelse af data og om ændring af forordning (EU) 2017/2394 og direktiv (EU) 2020/1828 (dataforordningen) (EUT L 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).«

*Artikel 49***Evaluering og revision**

1. Senest den 12. september 2028 foretager Kommissionen en evaluering af denne forordning og forelægger Europa-Parlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg en rapport om de vigtigste resultater. I denne evaluering vurderes navnlig:

a) situationer, der anses for at være situationer, hvor der er et ekstraordinært behov med henblik på denne forordnings artikel 15 og anvendelsen af denne forordnings kapitel V i praksis, navnlig offentlige myndigheders, Kommissionens, Den Europæiske Centralbanks og EU-organers erfaringer med anvendelse af denne forordnings kapitel V, antallet og resultatet af de sager, der er indbragt for den kompetente myndighed i henhold til artikel 18, stk. 5, om anvendelse af denne forordnings kapitel V, som indberettet af de kompetente myndigheder, indvirkningen af andre forpligtelser, der er fastsat i EU-retten eller national ret med henblik på at efterkomme anmodninger om adgang til oplysninger, indvirkningen af frivillige datadelingsmekanismer såsom dem, som dataaltruistiske organisationer, der er anerkendt i henhold til forordning (EU) 2022/868, har fastlagt, på opfyldelsen af målene i nærværende forordnings kapitel V og

personoplysningers rolle i forbindelse med nærværende forordnings artikel 15, herunder udviklingen af teknologier til beskyttelse af privatlivet

b) denne forordnings indvirkning på anvendelsen af data i økonomien, herunder på datainnovation, datamonetariseringsspraksis og dataformidlingstjenester samt på datadeling inden for de fælles europæiske dataområder

c) tilgængeligheden og anvendelsen af forskellige kategorier og typer af data

d) udelukkelsen af visse kategorier af virksomheder som berettigede i henhold til artikel 5

e) fraværet af enhver indvirkning på intellektuelle ejendomsrettigheder

f) indvirkningen på forretningshemmeligheder, herunder på beskyttelsen mod ulovlig erhvervelse, brug og videregivelse heraf, samt indvirkningen af den mekanisme, der gør det muligt for dataindehavere at afvise brugeres anmodninger i henhold til artikel 4, stk. 8, og artikel 5, stk. 11, så vidt muligt under hensyntagen til eventuel revision af direktiv (EU) 2016/943

g) om listen over urimelige aftalevilkår, jf. artikel 13, er ajourført i lyset af ny forretningspraksis og den hurtige markedsinnovation

h) ændringer i kontraktpraksis hos udbydere af databehandlingstjenester, og hvorvidt dette resulterer i tilstrækkelig overensstemmelse med artikel 25

i) nedsættelsen af de gebyrer, som udbydere af databehandlingstjenester pålægger for skifteprocessen, i overensstemmelse med den gradvise fjernelse af skiftegebyrer i henhold til artikel 29

j) samspillet mellem denne forordning og andre EU-retsakter af relevans for dataøkonomien

k) forebyggelsen af ulovlig statslig adgang til andre data end personoplysninger

l) effektiviteten af den håndhævelsesordning, der kræves i henhold til artikel 37

m) denne forordnings indvirkning på SMV'er med hensyn til deres innovationskapacitet og tilgængeligheden af databehandlingstjenester for brugere i Unionen og byrden ved at opfylde nye forpligtelser.

2. Senest den 12. september 2028 foretager Kommissionen en evaluering af denne forordning og forelægger EuropaParlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg en rapport om de vigtigste resultater. Denne evaluering skal vurdere indvirkningen af artikel 23-31, 34 og 35, navnlig med hensyn til prisfastsættelse og mangfoldigheden af databehandlingstjenester, der udbydes i Unionen, med særligt fokus på udbydere, der er SMV'er.

3. Medlemsstaterne forelægger Kommissionen de oplysninger, der er nødvendige for udarbejdelsen af de i stk. 1 og 2 omhandlede rapporter.

4. På grundlag af de i stk. 1 og 2 omhandlede rapporter kan Kommissionen, hvis det er relevant, forelægge EuropaParlamentet og Rådet et lovgivningsmæssigt forslag om ændring af denne forordning.

Artikel 50

Ikrafttræden og anvendelse

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den finder anvendelse fra den 12. september 2025.

Den forpligtelse, der følger af artikel 3, stk. 1, finder anvendelse på forbundne produkter og de hermed relaterede tjenester, der bringes i omsætning efter den 12. september 2026.

Kapitel III finder kun anvendelse i forbindelse med forpligtelser til at stille data til rådighed i henhold til EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten, som træder i kraft efter den 12. september 2025.

Kapitel IV finder anvendelse på aftaler, der indgås efter den 12. september 2025.

Kapitel IV finder anvendelse fra den 12. september 2027 på aftaler, der indgås senest den 12. september 2025, forudsat at de:

a) er af ubegrænset varighed, eller

b) udløber mindst ti år efter den 11. januar 2024.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Strasbourg, den 13. december 2023.

På Europa-Parlamentets vegne

R. METSOLA

Formand

På Rådets vegne

P. NAVARRO RÍOS

Formand

- (1) EUT C 402 af 19.10.2022, s. 5.
- (2) EUT C 365 af 23.9.2022, s. 18.
- (3) EUT C 375 af 30.9.2022, s. 112.
- (4) Europa-Parlamentets holdning af 9.11.2023 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 27.11.2023.
- (5) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).
- (6) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).
- (7) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).
- (8) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).
- (9) Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler (EFT L 95 af 21.4.1993, s. 29).
- (10) Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugerne på det indre mar-ked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF, 98/27/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (»direktivet om urimelig handelspraksis«) (EUT L 149 af 11.6.2005, s. 22).
- (11) Europa-Parlamentets og Rådets direktiv 2011/83/EU af 25. oktober 2011 om forbrugerrettigheder, om ændring af Rådets direktiv 93/13/EØF og Europa-Parlamentets og Rådets direktiv 1999/44/EF samt om ophævelse af Rådets direktiv 85/577/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF (EUT L 304 af 22.11.2011, s. 64).
- (12) Europa-Parlamentets og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af udbredelsen af terrorrelateret indhold online (EUT L 172 af 17.5.2021, s. 79).
- (13) Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT L 277 af 27.10.2022, s. 1).
- (14) Europa-Parlamentets og Rådets forordning (EU) 2023/1543 af 12. juli 2023 om europæiske editionskendelser og europæiske sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe idømt som led i en straffesag (EUT L 191 af 28.7.2023, s. 118).

- (15) Europa-Parlamentets og Rådets direktiv (EU) 2023/1544 af 12. juli 2023 om harmoniserede regler for udpegning af bestemte forretningssteder og udpegning af retlige repræsentanter med henblik på indsamling af elektronisk bevismateriale i straffesager (EUT L 191 af 28.7.2023, s. 181).
- (16) Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og om ophævelse af forordning (EF) nr. 1781/2006 (EUT L 141 af 5.6.2015, s. 1).
- (17) Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT L 141 af 5.6.2015, s. 73).
- (18) Europa-Parlamentets og Rådets direktiv (EU) 2019/882 af 17. april 2019 om tilgængelighedskrav for produkter og tjenester (EUT L 151 af 7.6.2019, s. 70).
- (19) Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (EFT L 167 af 22.6.2001, s. 10).
- (20) Europa-Parlamentets og Rådets direktiv 2004/48/EF af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder (EUT L 157 af 30.4.2004, s. 45).
- (21) Europa-Parlamentets og Rådets direktiv (EU) 2019/790 af 17. april 2019 om ophavsret og beslægtede rettigheder på det digitale indre marked og om ændring af direktiv 96/9/EF og 2001/29/EF (EUT L 130 af 17.5.2019, s. 92).
- (22) Europa-Parlamentets og Rådets forordning (EU) 2022/868 af 30. maj 2022 om europæisk datastyring og om ændring af forordning (EU) 2018/1724 (forordning om datastyring) (EUT L 152 af 3.6.2022, s. 1).
- (23) Europa-Parlamentets og Rådets direktiv (EU) 2016/943 af 8. juni 2016 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse (EUT L 157 af 15.6.2016, s. 1).
- (24) Europa-Parlamentets og Rådets direktiv 98/6/EF af 16. februar 1998 om forbrugerbeskyttelse i forbindelse med angivelse af priser på forbrugsvarer (EFT L 80 af 18.3.1998, s. 27).
- (25) Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (direktivet om elektronisk handel) (EFT L 178 af 17.7.2000, s. 1).
- (26) Europa-Parlamentets og Rådets forordning (EU) 2022/1925 af 14. september 2022 om åbne og fair markeder i den digitale sektor og om ændring af direktiv (EU) 2019/1937 og (EU) 2020/1828 (forordningen om digitale markeder) (EUT L 265 af 12.10.2022, s. 1).
- (27) Europa-Parlamentets og Rådets forordning (EF) nr. 223/2009 af 11. marts 2009 om europæiske statistikker og om ophævelse af forordning (EF, Euratom) nr. 1101/2008 om fremsendelse af fortrolige statistiske oplysninger til De Europæiske Fællesskabers Statistiske Kontor, Rådets forordning (EF) nr. 322/97 om EF-statistikker og Rådets afgørelse 89/382/EØF, Euratom om nedsættelse af et udvalg for De Europæiske Fællesskabers statistiske program (EUT L 87 af 31.3.2009, s. 164).
- (28) Europa-Parlamentets og Rådets direktiv (EU) 2019/1024 af 20. juni 2019 om åbne data og videreanvendelse af den offentlige sektors informationer (EUT L 172 af 26.6.2019, s. 56).

- (29) Europa-Parlamentet og Rådets direktiv 96/9/EF af 11. marts 1996 om retlig beskyttelse af databaser (EFT L 77 af 27.3.1996, s. 20).
- (30) Europa-Parlamentets og Rådets forordning (EU) 2018/1807 af 14. november 2018 om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union (EUT L 303 af 28.11.2018, s. 59).
- (31) Europa-Parlamentets og Rådets direktiv (EU) 2019/770 af 20. maj 2019 om visse aspekter om aftaler om levering af digitalt indhold og digitale tjenester (EUT L 136 af 22.5.2019, s. 1).
- (32) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).
- (33) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).
- (34) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).
- (35) Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF af 9. juli 2008 om fælles rammer for markedsføring af produkter og om ophævelse af Rådets afgørelse 93/465/EØF (EUT L 218 af 13.8.2008, s. 82).
- (36) Europa-Parlamentets og Rådets forordning (EU) 2017/2394 af 12. december 2017 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse og om ophævelse af forordning (EF) nr. 2006/2004 (EUT L 345 af 27.12.2017, s. 1).
- (37) Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 af 25. november 2020 om adgang til anlæggelse af gruppesøgsmål til beskyttelse af forbrugernes kollektive interesser og om ophævelse af direktiv 2009/22/EF (EUT L 409 af 4.12.2020, s. 1).
- (38) EUT L 123 af 12.5.2016, s. 1.
- (39) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Lovforslagets hovedpunkter
 - 2.1. Anvendelsesområde
 - 2.1.1. Gældende ret
 - 2.1.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
 - 2.2. Udpegning af kompetente myndigheder og samarbejde med andre myndigheder, herunder Datatilsynet
 - 2.2.1. Gældende ret
 - 2.2.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
 - 2.3. Certificering af tvistbilæggelsesorganer
 - 2.3.1. Gældende ret
 - 2.3.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
 - 2.4. De kompetente myndigheders opgaver og beføjelser m.v.
 - 2.4.1. Gældende ret
 - 2.4.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
 - 2.5. Sanktioner (kritik, påbud, offentliggørelse og bødestraf)
 - 2.5.1. Gældende ret
 - 2.5.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
3. Forholdet til databeskyttelsesretten
4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige
5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.
6. Administrative konsekvenser for borgerne
7. Klimamæssige konsekvenser
8. Miljø- og naturmæssige konsekvenser
9. Forholdet til EU-retten
10. Hørte myndigheder og organisationer m.v.
11. Sammenfattende skema

1. Indledning

Formålet med dette lovforslag er at supplere reglerne i dataforordningen. Forslaget fastsætter således supplerende nationale bestemmelser om kompetence, håndhævelse og straf inden for det nationale råderum, som dataforordningen giver mulighed for.

Dataforordningen blev vedtaget den 13. december 2023 og finder anvendelse fra den 12. september 2025, dog er der visse undtagelser hertil.

Dataforordningen udgør et led i den europæiske datastrategi,

og den supplerer Europa-Parlamentets og Rådets forordning (EU) 2022/868 af 30. maj 2022 om europæisk datastyring (forordning om datastyring). Datastyringsforordningen og dataforordningen vil tilsammen skulle bidrage til oprettelsen af et indre marked for data i EU samt skulle bidrage til, at Europa bliver førende inden for dataøkonomien ved at udnytte potentialet i de stadigt stigende datamængder, navnlig industrielle data, til gavn for både den europæiske økonomi og det europæiske samfund.

Dataforordningen har til formål at styrke dataøkonomien i EU og fremme et konkurrencedygtigt datamarked ved at gøre data mere tilgængelige og anvendelige samt tilskynde

til datadreven innovation. For at opnå dette har dataforordningen til hensigt at skabe retfærdighed i fordelingen af den værdi, der hidrører fra data, blandt aktører i dataøkonomien.

Dataforordningen fastsætter en harmoniseret ramme, der definerer, hvem der kan anvende data fra forbundne produkter eller relaterede tjenester, og på hvilke betingelser. Desuden omfatter dataforordningen foranstaltninger til at øge retfærdigheden og konkurrencen på markedet for databehandlingstjenester (blandt andet på cloudmarkedet) i Europa samt til at beskytte virksomheder mod urimelige kontraktvilkår i forbindelse med datadeling, der pålægges af aktører, som er stærkere end dem. Yderligere indfører dataforordningen en mekanisme, hvorigennem offentlige myndigheder kan anmode om data fra en virksomhed, hvor der er et ekstraordinært behov, f.eks. i offentlige nødsituationer, og fastsætter klare regler for, hvordan sådanne anmodninger bør fremsættes. Endvidere indføres der sikkerhedsforanstaltninger for at undgå, at statslige organer fra tredjelande kan få adgang til andre data end personoplysninger, hvis dette ville være i strid med EU-retten eller national ret. Endelig fastsætter dataforordningen væsentlige krav vedrørende interoperabilitet for at sikre, at data kan flyde frit uden problemer mellem sektorer og medlemsstater. Oprettelsen af fælles europæiske dataområder for strategiske sektorer i økonomien og områder af offentlig interesse vil bidrage til et reelt indre marked for data, hvor det er muligt at dele og anvende data på tværs af sektorer.

For at formålet med dataforordningen kan opnås, er det grundlæggende at etablere velfungerende og effektive tilsyn. Som følge heraf skal hver medlemsstat udpege én eller flere myndigheder, der skal påse overholdelsen af dataforordningen.

Lovforslaget har til formål at supplere dataforordningen, hvor dette er påkrævet, med henblik på at sikre nødvendige og tilstrækkelige gennemførelsesforanstaltninger for så vidt angår tilsyn og håndhævelse.

Med lovforslaget foreslås således bestemmelser, der tillægger den kompetente myndighed nærmere håndhævelsesbeføjelser, herunder bestemmelser om undersøgelsesbeføjelser og muligheder for sanktionering i overensstemmelse med artikel 40, stk. 1, i dataforordningen.

2. Lovforslagets hovedpunkter

2.1. Anvendelsesområde

2.1.1. Gældende ret

Det følger af dataforordningens artikel 1, stk. 2, at dataforordningen både omfatter personoplysninger og andre data end personoplysninger.

I forhold til personoplysninger følger det af artikel 1, stk. 5, 1. pkt., at dataforordningen ikke berører EU-retten og national ret om beskyttelse af personoplysninger, privatlivets fred og kommunikationshemmigheden samt integriteten

af terminaludstyr, som finder anvendelse på personoplysninger, der behandles i forbindelse med de rettigheder og forpligtelser, der er fastsat i dataforordningen, navnlig forordning (EU) 2016/679 (databeskyttelsesforordningen) og (EU) 2018/1725 (forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unions institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger) og direktiv 2002/58/EF (direktiv om beskyttelse inden for elektronisk kommunikation), herunder tilsynsmyndighedernes beføjelser og kompetencer og de registreredes rettigheder. For så vidt angår brugere, som er registrerede, supplerer de rettigheder, der er fastsat i dataforordningens kapitel II, registreredes indsigtret og retten til dataportabilitet i henhold til artikel 15 og 20 i databeskyttelsesforordningen, jf. artikel 1, stk. 5, 2. pkt., i dataforordningen. I tilfælde af uoverensstemmelse mellem dataforordningen og EU-retten om beskyttelse af personoplysninger eller privatlivets fred eller national ret vedtaget i overensstemmelse med EU-retten har den relevante EU-ret eller nationale ret om beskyttelse af personoplysninger eller privatlivets fred forrang, jf. artikel 1, stk. 5, sidste pkt., i dataforordningen.

De enkelte kapitler i dataforordningen regulerer en række særskilte områder og situationer, som skal læses i sammenhæng med dataforordningens artikel 1, stk. 2. I dataforordningens kapitel II reguleres datadeling mellem virksomheder og mellem virksomheder og forbrugere i forbindelse med tingenes internet (IoT). I kapitel III reguleres nærmere betingelserne for datadeling i den private sektor, når der er en lovbestemt forpligtelse til at dele data. I kapitel IV reguleres urimelige aftalevilkår. Reglerne i kapitel IV finder anvendelse på data fra den private sektor, der tilgås og anvendes på grundlag af aftaler mellem virksomheder. I kapitel V reguleres datadeling med fokus på andre data end personoplysninger mellem virksomheder og myndigheder, når der foreligger et ekstraordinært behov. I kapitel VI reguleres skift mellem databehandlingstjenester. Reglerne i kapitel VI finder anvendelse på data og tjenester, der behandles af udbydere af databehandlingstjenester. I kapitel VII reguleres tredjelandes adgang til oplysninger. Reglerne i kapitel VII finder alene anvendelse på andre data end personoplysninger, som udbydere af databehandlingstjenester er i besiddelse af i EU. Endelig regulerer kapitel VIII særlige regler om interoperabilitet, herunder kriterier som deltagere i dataområder skal opfylde.

Det følger af artikel 1, stk. 3, i dataforordningen, at dataforordningen finder anvendelse på

- producenter af forbundne produkter, som bringes i om sætning i Unionen, og udbydere af relaterede tjenester, uanset disse producenters og udbyderes etableringssted,
- brugere i Unionen af forbundne produkter eller relaterede tjenester, jf. litra a),
- dataindehavere, uanset deres etableringssted, der stiller data til rådighed for datamodtagere i Unionen,
- datamodtagere i Unionen, som dataene stilles til rådighed for,

- e) offentlige myndigheder, Kommissionen, Den Europæiske Centralbank og EU-organer, der anmoder dataindehavere om at stille data til rådighed, hvis der er et ekstraordinært behov for de pågældende data med henblik på udførelse af en specifik opgave i offentlighedens interesse, og de dataindehavere, der leverer disse data som følge af en sådan anmodning,
- f) udbydere af databehandlingstjenester, uanset deres etableringssted, der udbyder sådanne tjenester til kunder i Unionen, og
- g) deltagere i dataområder og leverandører af applikationer, der anvender intelligente kontrakter, og personer, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre i forbindelse med gennemførelsen af en aftale.

Oplistningen i artikel 1, stk. 3, i dataforordningen, er ikke udtømmende.

I dataforordningens artikel 1, stk. 4-10, er der fastsat regler, der angiver, hvornår og hvordan dataforordningen finder anvendelse inden for en række nærmere angivne områder og situationer.

2.1.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Dataforordningen kræver indførelse af supplerende bestemmelser om tilsynskompetence (blandt andet i form af beføjelser i relation til håndtering af klager og undersøgelser af overtrædelser af dataforordningen) og sanktionering i national lovgivning. Derfor har lovforslaget til formål at indføre supplerende regler i forbindelse med tilsynet med og håndhævelsen af dataforordningen.

Den foreslåede lov vil have samme anvendelsesområde som dataforordningen. Der henvises i øvrigt til lovforslagets § 1 og bemærkningerne hertil.

2.2. Udpegning af kompetente myndigheder og samarbejde med andre myndigheder, herunder Datatilsynet

2.2.1. Gældende ret

Det følger af dataforordningens artikel 37, stk. 1, at hver medlemsstat skal udpege én eller flere kompetente myndigheder til at have ansvaret for anvendelsen og håndhævelsen af dataforordningen. Dette gælder blandt andet i forhold til at udføre de opgaver, der er beskrevet i dataforordningens artikel 37, stk. 5.

Det følger videre af dataforordningens artikel 37, stk. 3, 1. og 2. pkt., at de tilsynsmyndigheder, der er ansvarlige for at overvåge anvendelsen af databeskyttelsesforordningen, er ansvarlige for at overvåge anvendelsen af dataforordningen for så vidt angår beskyttelse af personoplysninger, og at kapitel VI og VII i databeskyttelsesforordningen tilsvarende finder anvendelse.

Såfremt der udpeges flere kompetente myndigheder, er det

i henhold til dataforordningens artikel 37, stk. 2, et krav, at der også udpeges en datakoordinator for at lette samarbejdet mellem de kompetente myndigheder. Datakoordinatorens opgaver er beskrevet i dataforordningens artikel 37, stk. 5 og 6. Det fremgår af præambelbetragtning nr. 107, at såfremt der ikke er udpeget en datakoordinator, bør den kompetente myndighed påtage sig de opgaver, som datakoordinatoren pålægges i dataforordningen.

Det følger derudover af dataforordningens artikel 37, stk. 8, at kompetente myndigheder ved udførelsen af deres opgaver og udøvelsen af deres beføjelser i henhold til dataforordningen skal være upartiske og frie for udefrakommende indflydelse, både direkte og indirekte, og at de hverken må søge eller modtage instrukser med henblik på enkeltsager fra nogen anden offentlig myndighed eller nogen privat part.

2.2.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Digitaliseringsministeriet finder det hensigtsmæssigt, at Digitaliseringsstyrelsen med lovforslaget formelt bliver udpeget som kompetent myndighed i henhold til dataforordningens artikel 37, stk. 1.

Dataforordningen regulerer digitale tjenester samt har til formål at fremme datakompetence og bevidsthed for brugere og enheder omfattet af dataforordningen. Dataforordningen etablerer en mulighed for at klage over overtrædelser af dataforordningen samt en mulighed for, at myndigheder af egen drift kan påse overholdelsen af dataforordningen, jf. artikel 37, stk. 5, i dataforordningen. Behandlingen af sager om overtrædelser af dataforordningen forventes at kræve ekspertise og forståelse for digitaliseringsområdet, herunder de tekniske aspekter. Dertil kommer, at der vil være behov for at foretage en vægtning af de hensyn, der gør sig gældende inden for data- og digitaliseringsområdet, som dataforordningen tilsigter at regulere, herunder blandt andet at styrke det europæiske indre digitale marked og økonomi. Digitaliseringsstyrelsen vurderes at have den nødvendige erfaring med og indsigt i området, og opgaverne lægger sig i naturlig forlængelse af styrelsens eksisterende tilsynsområder og kompetencer.

I forhold til data i form af personoplysninger, fremgår det af dataforordningens artikel 37, stk. 3, at tilsynsmyndigheder, der er ansvarlige for at overvåge anvendelsen af databeskyttelsesforordningen, vil være ansvarlige for at overvåge anvendelsen af dataforordningen for så vidt angår beskyttelse af personoplysninger. Samtidig fremgår det, at kapitel VI og VII i databeskyttelsesforordningen tilsvarende finder anvendelse. Dataforordningen stiller ikke krav om, at Datatilsynet skal udpeges som kompetent myndighed i relation til dataforordningen.

Den foreslåede ordning vil medføre, at det alene er Digitaliseringsstyrelsen, der vil skulle varetage tilsynsopgaverne efter dataforordningen, som tilfalder kompetente myndigheder. Datatilsynet vil alene skulle føre tilsyn med overholdel-

sen af de eksisterende regler om beskyttelse af personoplysninger, og der er derfor ikke behov for at tildele Datatilsynet særskilte beføjelser i relation til dataforordningen.

Som følge af samarbejdsforpligtelsen i dataforordningens artikel 37, stk. 5, litra g, vil Digitaliseringsstyrelsen i praksis skulle arbejde tæt sammen med andre myndigheder, navnlig i relation til behandlingen af klager om overtrædelser af dataforordningen. Dette gælder særligt i relation til Datatilsynet som følge af samspillet mellem dataforordningen og de eksisterende regler om beskyttelse af personoplysninger, jf. blandt andet artikel 1, stk. 5, og artikel 37, stk. 3, i dataforordningen.

Ordnningen afspejler den politiske beslutning om at udpege Digitaliseringsstyrelsen som central myndighed i relation til dataforordningen.

Som følge af at Digitaliseringsstyrelsen bliver den eneste kompetente myndighed, er der ikke behov for at udpege en datakoordinator, idet Digitaliseringsstyrelsen vil varetage de opgaver, som pålægges datakoordinatoren i dataforordningen, jf. dataforordningens præambelbetragtning nr. 107.

Det foreslås derfor med lovforslagets § 2, stk. 1, at Digitaliseringsstyrelsen bliver kompetent myndighed i overensstemmelse med dataforordningens artikel 37, stk. 1.

Der henvises til lovforslagets § 2 og bemærkningerne hertil.

Digitaliseringsministeriet foreslår, at dataforordningens artikel 37, stk. 8, gengives i den foreslåede § 4, dog således at indholdet af artiklen udvides til også at omfatte loven. Dataforordningen stiller krav til myndigheders upartiskhed i relation til at undgå udefrakommende indflydelse. Ordningen vil medføre, at Digitaliseringsstyrelsen bliver uafhængig i håndteringen af sager efter dataforordningen samt loven. Det bemærkes, at der af dataforordningens ordlyd ikke stilles særlige krav i forhold til kompetente myndigheders funktionelle uafhængighed. Da dataforordningen ikke stiller krav til, hvordan kompetente myndigheder organisatorisk skal indrettes, vurderes det som unødigt indgribende at pålægge specifikke rammer herfor. Den foreslåede bestemmelse skal sikre overensstemmelse med kravene i dataforordningens artikel 37, stk. 8, herunder ved at afskære ministeren for digitaliserings instruktionsbeføjelser i relation til Digitaliseringsstyrelsens behandling af sager efter dataforordningen samt loven.

Der henvises i øvrigt til lovforslagets § 4 og bemærkningerne hertil.

2.3. Certificering af tvistbilæggesorganer

2.3.1. Gældende ret

Dataforordningens artikel 10 indeholder bestemmelser vedrørende tvistbilæggesorganer, herunder om adgang til tvistbilæggesorganer for brugere, dataindehavere og datamodtagere samt kunder og udbydere af databehandlingstje-

nester, jf. artikel 10, stk. 1 og 4, i dataforordningen, og om betingelser for certificering, jf. artikel 10, stk. 5, i dataforordningen.

Medlemsstater, hvor et tvistbilæggesorgan er etableret, pålægges i dataforordningens artikel 10, stk. 5, at kunne certificere et sådant organ efter anmodning, hvis følgende betingelser er opfyldt

- a) det er upartisk og uafhængigt, og det skal træffe sine afgørelser i overensstemmelse med klare, ikkeforskelsbehandlende og fair procedureregler,
- b) det har den nødvendige ekspertise, navnlig med hensyn til fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser, herunder godtgørelse, og om at stille data til rådighed på en gennemsigtig måde, således at organet effektivt kan fastsætte disse vilkår og betingelser,
- c) det er let at kontakte ved hjælp af elektronisk kommunikation, og
- d) det er i stand til at vedtage sine afgørelser på en hurtig og omkostningseffektiv måde på mindst ét af Unionens officielle sprog.

Af præambelbetragtning nr. 52 i dataforordningen følger, at det står medlemsstaterne frit for at vedtage eventuelle særlige regler for certificeringsproceduren, herunder certificeringens udløb eller tilbagekaldelse, og at bestemmelserne i dataforordningen om tvistbilægges ikke bør forpligte medlemsstaterne til at oprette tvistbilæggesorganer.

Dataforordningens artikel 10 giver således medlemsstaterne mulighed for at fastsætte nærmere regler vedrørende certificering, men den indebærer ikke en forpligtelse til at oprette et tvistbilæggesorgan.

2.3.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Dataforordningens artikel 10 pålægger medlemsstater at kunne certificere et tvistbilæggesorgan efter anmodning, såfremt tvistbilæggesorganet er etableret i den pågældende medlemsstat. Forpligtelsen til at kunne certificere pålægges i dataforordningen ikke de kompetente myndigheder. Da Digitaliseringsstyrelsen ikke har erfaring med etablering eller certificering af tvistbilæggesorganer, vil det være nærliggende, at Digitaliseringsstyrelsen i samarbejde med myndigheder, der har erfaring hermed, udarbejder regler, der blandt andet etablerer en certificeringsordning og nærmere specificerer, hvem der kan certificere et tvistbilæggesorgan, hvordan ansøgning skal indgives, samt hvordan betingelserne i dataforordningens artikel 10 skal forstås.

Det foreslås derfor med lovforslagets § 3, at ministeren for digitalisering kan fastsætte nærmere regler vedrørende certificering af tvistbilæggesorganer i henhold til dataforordningens artikel 10, og at ministeren for digitalisering derudover kan fastsætte sådanne regler på andre ministres ressortområder efter aftale med vedkommende ministre.

Der henvises til lovforslagets § 3 og bemærkningerne hertil.

2.4. De kompetente myndigheders opgaver og beføjelser m.v.

2.4.1. Gældende ret

Det fremgår af dataforordningens artikel 37, stk. 1, at kompetente myndigheder har ansvaret for anvendelsen og håndhævelsen af dataforordningen.

Dataforordningens artikel 37, stk. 5, indeholder en nærmere oplysning af, hvilke opgaver, som kompetente myndigheder skal varetage, samt hvilke beføjelser, som de skal have.

Såfremt der ikke er udpeget en datakoordinator, bør den kompetente myndighed påtage sig de opgaver, som datakoordinatoren pålægges i dataforordningen, jf. præambelbetragtning nr. 107 i dataforordningen. Datakoordinatorens opgaver er nærmere beskrevet i dataforordningens artikel 37, stk. 5, sidste pkt. og stk. 6.

Ifølge dataforordningens artikel 37, stk. 14, skal kompetente myndigheder have beføjelse til at anmode brugere, dataindhavere eller datamodtagere samt deres retlige repræsentanter, der hører under deres medlemsstats kompetence, om alle oplysninger, som er nødvendige for at kontrollere efterlevelsen af dataforordningen. Enhver anmodning om oplysninger skal stå i rimeligt forhold til, hvad den underliggende opgave kræver, og være begrundet.

Bestemmelsen suppleres af præambelbetragtning nr. 107 i dataforordningen, hvorefter kompetente myndigheder gennem udøvelsen af deres beføjelser i overensstemmelse med gældende nationale procedurer bør kunne søge efter og opnå oplysninger, navnlig vedrørende enheders aktiviteter inden for deres kompetence. Det følger af dataforordningens artikel 37, stk. 10, 1. pkt., at enheder, der er omfattet af dataforordningens anvendelsesområde, er underlagt kompetencen i den medlemsstat, hvor enheden er etableret. Hvis en enhed er etableret i mere end én medlemsstat, anses den for at høre under kompetencen i den medlemsstat, hvor den har sin hovedvirksomhed, jf. artikel 37, stk. 10, sidste pkt., i dataforordningen. Såfremt en enhed ikke er etableret i Unionen, anses enheden for at høre under den medlemsstats kompetence, hvor dens retlige repræsentant befinder sig, jf. artikel 37, stk. 13, 1. pkt., i dataforordningen.

Ifølge dataforordningens artikel 37, stk. 5, litra f, skal kompetente myndigheder samarbejde med andre medlemsstats kompetente myndigheder og Kommissionen eller European Data Innovation Board (EDIB) for at sikre ensartet og effektiv anvendelse af dataforordningen, herunder udveksling af alle relevante oplysninger ad elektronisk vej uden unødigt ophold.

2.4.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Digitaliseringsstyrelsen vil som eneste kompetente myndighed efter dataforordningen skulle varetage de opgaver, der

nærmere er angivet i dataforordningens artikel 37, stk. 5 og 6.

Den foreslåede ordning vil medføre, at Digitaliseringsstyrelsen blandt andet vil skulle behandle alle klagesager i relation til påståede overtrædelser af dataforordningen, jf. artikel 37, stk. 5, litra b, i dataforordningen. Derudover vil Digitaliseringsstyrelsen kunne tage sager op af egen drift for at undersøge, om dataforordningen overholdes, jf. artikel 37, stk. 5, litra c og i, i dataforordningen. I overensstemmelse med dataforordningens artikel 39, stk. 2, og dansk rets almindelige principper om domstolsprøvelse, vil Digitaliseringsstyrelsens undladelse af at behandle en klage kunne indbringes for domstolene.

Idet Digitaliseringsstyrelsen bliver den eneste kompetente myndighed, er der ikke behov for at udpege en datakoordinator. De opgaver, som datakoordinatoren skal varetage efter dataforordningens artikel 37, stk. 6, vil blive varetaget af Digitaliseringsstyrelsen i overensstemmelse med præambelbetragtning nr. 107 i dataforordningen.

Dataforordningens artikel 37, stk. 14, og præambelbetragtning nr. 107 understreger et behov for, at kompetente myndigheder i forbindelse med håndhævelsen af forordningen bør kunne opnå oplysninger fra relevante retssubjekter i relation til dataforordningen. Derudover fastsættes der ikke yderligere specifikke krav til, hvilke nærmere bestemte undersøgelsesbeføjelser, som kompetente myndigheder skal have.

For at kunne påse overholdelsen af dataforordningen, herunder gennem klagesagsbehandling samt egen drift-sager, finder Digitaliseringsministeriet det nødvendigt, at Digitaliseringsstyrelsen får mulighed for at indhente oplysninger, f.eks. i form af relevante dokumenter, tekniske specifikationer, data, oplysninger om overensstemmelse og oplysninger om tekniske aspekter. For at kunne håndhæve dataforordningen i sin helhed vil det være nødvendigt at kunne anmode om oplysninger fra alle retssubjekter, der er forpligtede i henhold til forordningen. Oplysningerne vil i overensstemmelse med dataforordningens artikel 37, stk. 14, og almindelig dansk forvaltningsret alene kunne indhentes, såfremt indhentelsen af oplysningerne er sagligt begrundet og proportional i forhold til formålet. Desuden afgrænses muligheden for at indhente oplysninger af det almindelige forbud mod at udsætte nogen for selvinkriminering, som det blandt andet kan udledes af Den Europæiske Menneskerettighedskonventions artikel 6 og § 10 i retssikkerhedsloven.

Digitaliseringsministeriet finder det desuden nødvendigt, at Digitaliseringsstyrelsen i forbindelse med sagsbehandling kan videregive oplysninger til andre forvaltningsmyndigheder i Danmark såvel som andre kompetente myndigheder i Den Europæiske Union samt Europa-Kommissionen, herunder oplysninger undergivet tavshedspligt, dvs. fortrolige oplysninger. Videregivelse af oplysninger til andre forvaltningsmyndigheder i Danmark, til andre kompetente myndigheder i Den Europæiske Union samt til Europa-Kommissio-

nen er påkrævet af hensyn til opfyldelsen af de samarbejdsforpligtelser, der følger af dataforordningens artikel 37, stk. 5, litra f-h. Videregivelse af personoplysninger reguleres af de databeskyttelsesretlige regler, mens oplysninger, som ikke udgør personoplysninger, og som ikke er fortrolige, som udgangspunkt kan videregives frit. Hvad angår videregivelse af fortrolige oplysninger, der ikke udgør personoplysninger, reguleres dette af forvaltningslovens regler om videregivelse, for så vidt der er tale om videregivelse til andre forvaltningsmyndigheder i Danmark. Da videregivelse af fortrolige oplysninger, der ikke udgør personoplysninger, til andre forvaltningsmyndigheder i Danmark er reguleret i forvaltningsloven, findes der ikke at være behov for at indføre en hjemmel hertil med lovforslaget. Forvaltningslovens regler regulerer dog ikke videregivelse af fortrolige oplysninger, der ikke udgør personoplysninger, til andre kompetente myndigheder i Den Europæiske Union eller til Europa-Kommissionen. På baggrund heraf og henset til, at det følger af dataforordningens artikel 37, stk. 5, litra f, at samarbejdsforpligtelsen i forhold til andre kompetente myndigheder i Den Europæiske Union og Europa-Kommissionen omfatter udveksling af alle relevante oplysninger ad elektronisk vej, findes det nødvendigt at indføre en særskilt hjemmel til videregivelse af oplysninger til andre kompetente myndigheder i Den Europæiske Union samt til Europa-Kommissionen, idet dette vil sikre, at også fortrolige oplysninger kan videregives.

Det bemærkes, at videregivelse af oplysninger i henhold til loven og dataforordningen skal ske i overensstemmelse med gældende lovgivning, herunder reglerne i databeskyttelsesforordningen, databeskyttelsesloven samt forvaltningsloven.

Der henvises til lovforslagets §§ 2, 5 og 6 og bemærkningerne hertil.

2.5. Sanktioner (kritik, påbud, offentliggørelse og bødestraf)

2.5.1. Gældende ret

Det fremgår af dataforordningens artikel 40, stk. 1, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af dataforordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning. Bestemmelsen suppleres af præambelbetragtning nr. 109, hvorefter kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i dataforordningen, er underlagt sanktioner, og at sådanne sanktioner kan omfatte økonomiske sanktioner, advarsler, irettesættelser eller påbud om at bringe forretningspraksis i overensstemmelse med forpligtelserne pålagt ved dataforordningen.

Ved pålæggelse af sanktioner for overtrædelser af dataforordningen er det i dataforordningens artikel 40, stk. 3, angivet, at der skal tages hensyn til anbefalingerne fra EDIB, samt følgende ikkeudtømmende kriterier:

- a) Overtrædelsens art, grovhed, omfang og varighed.
- b) Eventuelle tiltag, som den overtrædende part har truffet for at afbøde eller afhjælpe den skade, der er forårsaget af overtrædelserne.
- c) Den overtrædende parts eventuelle tidligere overtrædelser.
- d) De økonomiske fordele eller tab, som den overtrædende part har opnået eller undgået som følge af overtrædelserne, for så vidt som disse fordele eller tab kan fastslås på en pålidelig måde.
- e) Eventuelle andre skærpende eller formildende faktorer i lyset af sagens omstændigheder.
- f) Den overtrædende parts årlige omsætning i det foregående regnskabsår i Unionen.

Endelig er det nærmere angivet i dataforordningens artikel 37, stk. 5, litra d, at kompetente myndigheder skal kunne pålægge økonomiske sanktioner eller indlede retsforfølgning med henblik på at pålægge bøder.

2.5.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Digitaliseringsministeriet vurderer, at det, med henblik på at sikre at der leves op til forpligtelsen i dataforordningens artikel 40, stk. 1, er nødvendigt, at der fastsættes bestemmelser om kritik, påbud, offentliggørelse samt bøder.

Det foreslås som følge heraf i lovforslagets § 7, at Digitaliseringsstyrelsen vil kunne udtale kritik af fysiske og juridiske personer omfattet af dataforordningen. Muligheden for at udtale kritik vil navnlig være relevant, hvor en overtrædelse efter en samlet vurdering anses for at udgøre en mindre alvorlig overtrædelse. Det kunne f.eks. være i sager om manglende efterlevelse af en underretningspligt. Herudover vil muligheden for at udtale kritik kunne være relevant i forhold til overtrædelser, hvor det konkret vurderes, at meddelelse af et påbud efter § 9 ikke vil kunne rette op på forholdet. Det bemærkes, at udtalelsen vil kunne blive offentliggjort af Digitaliseringsstyrelsen i medfør af den foreslåede § 8, jf. nedenstående.

Desuden foreslås det i lovforslagets § 9, at Digitaliseringsstyrelsen vil kunne meddele påbud. Det er Digitaliseringsministeriets vurdering, at det er hensigtsmæssigt, at Digitaliseringsstyrelsen som kompetent myndighed skal kunne udstede påbud til retssubjekter, som dataforordningen pålægger forpligtelser, for at sikre overholdelsen af dataforordningen. Påbud vil både kunne angå, at retssubjekter skal udføre en handling eller bringe en handling til ophør, som dataforordningen forpligter retssubjekter til. Påbud vil blandt andet kunne omhandle nedsættelse af gebyr i overensstemmelse med den gradvise fjernelse af skiftegebyrer efter dataforordningens artikel 29 eller nedsættelse af godtgørelse for at stille data til rådighed i overensstemmelse med dataforordningens artikel 9.

Det foreslås herudover i lovforslagets § 8, at Digitaliseringsstyrelsen som en nødvendig og effektiv sanktion kan of-

fentliggøre sine udtalelser og afgørelser i sager om overtrædelser af dataforordningen eller loven, når samfundsmæssige hensyn taler for offentliggørelse. Offentliggørelse kan, udover at fungere som sanktion, indgå som led i Digitaliseringsstyrelsens opgave med at fremme datakompetence og -bevidsthed, jf. artikel 37, stk. 5, litra a, i dataforordningen. Offentliggørelse kan tjene som vejledning, idet offentligheden bliver oplyst om, at en praksis, handling eller undladelse udgør en overtrædelse af dataforordningen eller loven. Det vurderes på den baggrund, at den foreslåede bestemmelse i § 8 både tjener et formål i relation til dataforordningens artikel 37, stk. 5, litra a, og artikel 40, stk. 1. Det bemærkes, at der ikke vil være tale om systematisk offentliggørelse, men alene offentliggørelse baseret på en konkret afvejning af hensynet til de fysiske eller juridiske personer, som oplysningerne vedrører, over for de hensyn til samfundsmæssige interesser, der søges varetaget ved offentliggørelse. Det bemærkes desuden, at der forud for offentliggørelse skal foretages en konkret vurdering af, om der er oplysninger, der skal anonymiseres, og om der skal ske offentliggørelse af hele eller dele af udtalelsen eller afgørelsen, herunder om offentliggørelse alene skal ske i form af et resumé.

I den forbindelse bemærkes det, at visse fortrolige oplysninger ikke vil kunne offentliggøres som led i offentliggørelse af Digitaliseringsstyrelsens afgørelser eller udtalelser. Dette gælder blandt andet oplysninger om tekniske indretninger, fremgangsmåder, drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, som oplysningerne angår, at oplysningerne ikke videregives. Offentliggørelse vil desuden være underlagt fortrolighedsreglerne fastlagt i dataforordningens artikel 37, stk. 16.

For så vidt angår strafferetlige sanktioner, er det med udgangspunkt i dansk ret Digitaliseringsministeriets vurdering, at en passende strafferetlig sanktion vil være bøde.

Det foreslås, at det i lovens § 10, stk. 1, nr. 1 angives, hvilke bestemmelser i dataforordningen der er strafbelagt ved overtrædelse. Der vil på den måde kunne skabes et overblik over, hvilke bestemmelser, der er strafferetligt sanktioneret. På den baggrund foreslås det, at overtrædelse af følgende bestemmelser i dataforordningen skal kunne sanktioneres med bøde, medmindre højere straf er forskyldt efter anden lovgivning: artikel 3, artikel 4, stk. 1, 2, 4-8, 10, 11, 13 eller 14, artikel 5, stk. 1, 3-6 eller 9-11, artikel 6, stk. 1 eller 2, artikel 8, stk. 4, artikel 11, 14, 23, 25-28, artikel 29, stk. 1, 3, 5 eller 6, artikel 30, stk. 1-5, artikel 31, stk. 3, eller artikel 32, stk. 1, 4 eller 5.

Herudover foreslås det i lovforslagets § 10, stk. 1, nr. 2-3, at overtrædelse af følgende også vil skulle kunne sanktioneres med bøde, medmindre højere straf er forskyldt efter anden lovgivning:

- Undladelse af at efterkomme Digitaliseringsstyrelsens krav efter § 5 eller afgivelse af ukorrekte, ufuldstændige

eller vildledende oplysninger eller fortielse af oplysninger i forbindelse med sådanne krav.

- Undladelse af at efterkomme et påbud udstedt efter § 9.

I forhold til forældelsesfristen følger det af straffelovens § 93, stk. 1, at de nærmere forældelsesfrister skal beregnes efter det strafmaksimum, der er foreskrevet for forbrydelsen. Det er således strafferammen for den pågældende forbrydelse og ikke den konkrete forskyldte straf, som er afgørende for beregningen af forældelsesfristen. Forældelsesfristen er efter straffelovens § 93, stk. 11, 2 år, når der ikke er hjemlet højere straf end fængsel i 1 år for overtrædelsen.

Straffesager for overtrædelse af dataforordningen og loven vil efter omstændighederne kunne antage en vis størrelse og kompleksitet. Hertil kommer, at efterforskningen af sager, der f.eks. først henvises til politiet efter at have været undergivet forudgående sagsbehandling hos Digitaliseringsstyrelsen, eller som omfatter forhold, bevissikring m.v. uden for dansk jurisdiktion, må forventes at have en vis tidsmæssig udstrækning. I sådanne sager vil det kunne være vanskeligt at gennemføre de nødvendige strafforfølgningsskridt med henblik på at afbryde sagens forældelse inden for 2 år.

På denne baggrund er det Digitaliseringsministeriets vurdering, at det er mest hensigtsmæssigt, hvis forældelsesfristen for overtrædelser af loven eller dataforordningen fastsættes til 5 år.

Der henvises til lovforslagets §§ 7-10 og bemærkningerne hertil.

3. Forholdet til databeskyttelsesretten

Digitaliseringsstyrelsens behandling af personoplysninger er reguleret af databeskyttelsesforordningen samt lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) med senere ændringer. Det forudsættes med den foreslåede ordning, at Digitaliseringsstyrelsen som led i sagsbehandlingen vil skulle behandle personoplysninger. Digitaliseringsstyrelsen er dataansvarlig for den del af behandlingen af personoplysninger, der foregår i Digitaliseringsstyrelsen.

Det foreslås i lovforslagets § 5, at Digitaliseringsstyrelsen kan anmode om alle oplysninger, som er nødvendige for Digitaliseringsstyrelsens tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under Digitaliseringsstyrelsens kompetence, fra de fysiske og juridiske personer omfattet af dataforordningen samt retlige repræsentanter omfattet af artikel 37, stk. 11, i dataforordningen.

Ifølge databeskyttelsesforordningens artikel 6, stk. 2 og 3, er det muligt at implementere mere specifikke bestemmelser, der tilpasser anvendelsen af artikel 6, stk. 1, litra c, og artikel 6, stk. 1, litra e. Den foreslåede bestemmelse i § 5 udgør således supplerende retsgrundlag til databeskyttelsesforordningens artikel 6, stk. 1 litra e.

Det vurderes, at den foreslåede bestemmelse er proportional i forhold til de legitime mål og respekterer det væsentligste indhold af de databeskyttelsesretlige regler, da behandlingen er betinget af nødvendighed.

Yderligere foreslås det i lovforslagets § 6, at Digitaliseringsstyrelsen kan videregive oplysninger til Europa-Kommissionen og andre kompetente myndigheder i Den Europæiske Union, i det omfang det er nødvendigt for at påse overholdelsen af bestemmelserne i loven, dataforordningen eller den pågældende medlemsstats datadelingslovgivning. Adgangen til at videregive oplysninger kan i nogle tilfælde medføre, at personoplysninger videregives til kompetente myndigheder i Den Europæiske Union eller til Europa-Kommissionen.

Af artikel 37, stk. 5, litra f, i dataforordningen, følger at kompetente myndigheder skal samarbejde med andre medlemsstaters kompetente myndigheder og, hvis det er relevant, Europa-Kommissionen eller EDIB for at sikre ensartet og effektiv anvendelse af forordningen, herunder udveksling af alle relevante oplysninger ad elektronisk vej uden unødigt ophold, herunder med hensyn til dataforordningens artikel 37, stk. 10.

Ifølge databeskyttelsesforordningens artikel 6, stk. 2 og 3, er det muligt at implementere mere specifikke bestemmelser, der tilpasser anvendelsen af artikel 6, stk. 1, litra c, og artikel 6, stk. 1, litra e. Den foreslåede bestemmelse i § 6 udgør således supplerende retsgrundlag til databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Det vurderes, at den foreslåede bestemmelse er inden for rammerne af dataforordningen samt respekterer det væsentligste indhold af de databeskyttelsesretlige regler, da videregivelsen er betinget af nødvendighed.

Det bemærkes i forhold til lovforslagets § 6 og § 8, at i det omfang Digitaliseringsstyrelsen undtagelsesvist vil komme til at behandle følsomme oplysninger omfattet af databeskyttelsesforordningens artikel 9, vil behandlingen i sådanne tilfælde være nødvendig af hensyn til væsentlige samfundsinteresser, som angivet i databeskyttelsesforordningens artikel 9, stk. 2, litra g. Behandlingen vurderes hertil nødvendig for, at Digitaliseringsstyrelsen kan løfte sine tilsyns- og samarbejdsforpligtelser i henhold til artikel 37, stk. 1 og 5, i dataforordningen.

Det foreslås endvidere i lovforslagets § 8, at Digitaliseringsstyrelsen kan offentliggøre sine udtalelser efter § 7 og afgørelser efter § 9 i sager om overtrædelser af dataforordningen eller loven.

Offentliggørelsesordningen kan i nogle tilfælde medføre, at oplysninger om strafbare forhold, som omfattes af databeskyttelsesforordningens artikel 10, offentliggøres. Den foreslåede bestemmelse udgør således supplerende retsgrundlag til databeskyttelsesforordningens artikel 10.

Digitaliseringsministeriet vurderer, at de samfundsmæssige

hensyn bag offentliggørelse er tilstrækkeligt tungtvejende til at etablere en offentliggørelsesordning. Offentliggørelse i henhold til den foreslåede § 8 vil dog kun være nødvendig, når offentliggørelsen sker af hensyn til varetagelsen af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse af oplysningerne. Det bemærkes, at der ikke vil være tale om systematisk offentliggørelse, men alene offentliggørelse baseret på en konkret vurdering af sagens omstændigheder.

Digitaliseringsstyrelsen er endvidere berettiget – og efter omstændighederne også forpligtet – til at undlade at offentliggøre oplysninger fra sager, som tilsynet har behandlet, hvis offentlighedens interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private og offentlige interesser. I tvivlstilfælde vil det være naturligt at indhente en udtalelse herom fra den dataansvarlige, som er part i sagen, og eventuelt tillige fra den registrerede.

Digitaliseringsministeriet skal afslutningsvist bemærke, at det forudsættes, at de øvrige bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven, herunder de grundlæggende principper i databeskyttelsesforordningens artikel 5, også iagttages, når der behandles personoplysninger i medfør af de foreslåede bestemmelser.

Der henvises i øvrigt til lovforslagets §§ 5, 6 og 8 samt bemærkningerne hertil.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Det bemærkes overordnet, at lovforslaget supplerer dataforordningen, som har økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget forventes på den baggrund ikke i sig selv at have økonomiske konsekvenser eller implementeringskonsekvenser for det offentlige af betydning. Lovforslaget har ikke i sig selv i øvrigt økonomiske konsekvenser eller implementeringskonsekvenser af betydning for kommunerne eller regionerne.

For så vidt angår lovforslagets bemyndigelsesbestemmelser vil der i forbindelse med udstedelsen af eventuelle bekendtgørelser blive foretaget en vurdering af eventuelle økonomiske konsekvenser og implementeringskonsekvenser for det offentlige.

Digitaliseringsministeriet har herudover overvejet, hvorvidt lovforslaget følger de syv principper for digitaliseringsklar lovgivning. Da lovforslaget fastsætter supplerende regler til dataforordningen, har det ikke selvstændig relevans i forbindelse med de syv principper. Der er heller ikke foreslået yderligere supplerende bestemmelser, som kunne være relevante i denne sammenhæng. Det bemærkes dog, at lovforslaget er udformet således, at de syv principper for digitaliseringsklar lovgivning iagttages i videst muligt omfang.

5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Det bemærkes overordnet, at lovforslaget supplerer dataforordningen, som har økonomiske og administrative konsekvenser for erhvervslivet m.v.

For så vidt angår lovforslagets bemyndigelsesbestemmelser vil der i forbindelse med udstedelsen af eventuelle bekendtgørelser blive foretaget en vurdering af eventuelle økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget har været sendt til Erhvervsstyrelsens Område for Bedre Regulering (OBR), der på det foreliggende grundlag har vurderet, at lovforslaget medfører administrative konsekvenser i form af omkostninger for erhvervslivet. De løbende administrative konsekvenser knytter sig til lovforslagets § 5 om anmodning om oplysninger i tilfælde af tilsyn med regelefterlevende virksomheder.

På baggrund af ovenstående vurderes det, at de samlede administrative konsekvenser ikke overstiger bagatelgrænsen for forelæggelsen for Regeringens økonomiudvalg på 4 mio. kr., hvorfor de ikke kvantificeres nærmere.

6. Administrative konsekvenser for borgerne

Lovforslaget forventes ikke at have administrative konsekvenser for borgerne.

7. Klimamæssige konsekvenser

Lovforslaget medfører ikke klimamæssige konsekvenser.

8. Miljø- og naturmæssige konsekvenser

Lovforslaget medfører ikke miljø- og naturmæssige konsekvenser.

9. Forholdet til EU-retten

Lovforslaget fastsætter supplerende bestemmelser til Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair ad-

gang til og anvendelse af data (dataforordningen). Da forordningen, med forbehold af en række nærmere, specifikke undtagelser, finder anvendelse i Danmark fra den 12. september 2025, vil fastsættelsen af de supplerende bestemmelser, der foreslås med dette lovforslag, være forsinket.

10. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 30. april til den 30. maj 2025 (30 dage) været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatsamfundet, AE – Arbejderbevægelsens Erhvervsråd, Alexandra Instituttet, ATP, Autig, BL – Danmarks almene boliger, Danish Cloud Community, Danmarks Nationalbank, Danmarks Statistik, Dansk Arbejdsgiverforening, Danske Advokater, Danske A-Kasser, Danske Annoncører og Markedsførere, Danske Handicaporganisationer, Danske Regioner, Dansk Erhverv, Danske Universiteter, Dansk Industri, Dansk IT, Dansk Metal, Dataetisk Råd, Datatilsynet, Den Danske Dommerforening, Det Centrale Handicapråd, DI Digital, Digital Lead, DKCERT, Domstolsstyrelsen, Energinet, Energistyrelsen, Erhvervshus Fyn, Erhvervshus Hovedstaden, Erhvervshus Midtjylland, Erhvervshus Nordjylland, Erhvervshus Sjælland, Erhvervshus Sydjylland, Finans Danmark, Finanstilsynet, FOA, Fonden Dansk Standard, Forbrugerombudsmanden, Forbrugerrådet Tænk, Foreningen Danske Revisorer, Forsikring og Pension, FSR – danske revisorer, Green Power Denmark, GTS-foreningen, HK Danmark, Ingeniørforeningen IDA, Institut for menneskerettigheder, IT-Branchen, IT-Politisk Forening, KL – Kommunernes Landsforening, KMD, KOMBIT, Konkurrence- og Forbrugerstyrelsen, Landbrug & Fødevarer, LOS – Landsorganisationen for sociale tilbud, MADE, Nets Danmark A/S, Patent- og Varemærkestyrelsen, Prosa, Forbundet af IT-Professionelle, Psykiatrifonden, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rigsrevisionen, Rådet for Digital Sikkerhed, Rådet for Socialt Udsatte, SMVDanmark, Teleindustrien, Ældre Sagen og 3F – Fagligt Fælles Forbund.

11. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet m.v.	Ingen	De administrative konsekvenser knytter sig til lovforslagets § 5 om anmodning om oplysninger i tilfælde af tilsyn med regelefterlevende virksomheder. De samlede administrative konsekvenser overstiger ikke bagatelgrænsen for forelæggelsen for Regeringens økonomiudvalg

		på 4. mio. kr., hvorfor de ikke kvantificeres nærmere.
Administrative konsekvenser for erhvervslivet m.v.	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Klimamæssige konsekvenser	Ingen	Ingen
Miljø- og naturmæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget fastsætter supplerende bestemmelser til Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair adgang til og anvendelse af data (dataforordningen).	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Det foreslås i § 1, at loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair adgang til og anvendelse af data (dataforordningen), jf. bilag 1.

Med den foreslåede bestemmelse tydeliggøres det, at loven vil supplere dataforordningen.

Til § 2

Det følger af artikel 37, stk. 1, i dataforordningen, at hver medlemsstat udpeger én eller flere kompetente myndigheder til at have ansvaret for anvendelsen og håndhævelsen af dataforordningen, og at medlemsstaterne kan oprette en eller flere nye myndigheder eller forlade sig på eksisterende myndigheder.

For så vidt angår personoplysninger følger det af dataforordningens artikel 37, stk. 3, 1. og 2. pkt., at de tilsynsmyndigheder, der er ansvarlige for at overvåge anvendelsen af databeskyttelsesforordningen, er ansvarlige for at overvåge anvendelsen af dataforordningen for så vidt angår beskyttelse af personoplysninger, og at kapitel VI og VII i databeskyttelsesforordningen tilsvarende finder anvendelse.

Det følger endvidere af dataforordningens artikel 37, stk. 2, 1. pkt., at hvis en medlemsstat udpeger mere end én kompetent myndighed, udpeger den en datakoordinator blandt dem for at lette samarbejdet mellem de kompetente myndigheder og for at bistå enheder inden for dataforordningens anvendelsesområde i forbindelse med alle spørgsmål vedrørende dataforordningens anvendelse og håndhævelse. Ved udøvelsen af de opgaver og beføjelser, som de kompetente myndig-

heder er tillagt, samarbejder de kompetente myndigheder med hinanden, jf. artikel 37, stk. 2, sidste pkt., i dataforordningen.

Desuden følger det af artikel 37, stk. 5, i dataforordningen, at medlemsstaterne sikrer, at opgaverne og beføjelserne for de kompetente myndigheder er klart definerede og omfatter at

- fremme datakompetence og -bevidsthed blandt brugere og enheder, der er omfattet af dataforordningens anvendelsesområde, om rettigheder og forpligtelser i henhold til dataforordningen,
- behandle klager over påståede overtrædelser af dataforordningen, herunder vedrørende forretningshemmeligheder, og, for så vidt det er hensigtsmæssigt, undersøge genstanden for klagen og løbende underrette klagerne, hvis det er relevant i henhold til national ret, om forløbet og resultatet af undersøgelsen inden for en rimelig frist, navnlig hvis yderligere undersøgelse eller koordinering med en anden kompetent myndighed er nødvendig,
- foretage undersøgelser om spørgsmål, der vedrører anvendelsen af dataforordningen, herunder på grundlag af oplysninger, der er modtaget fra en anden kompetent myndighed eller en anden offentlig myndighed,
- pålægge økonomiske sanktioner, der er effektive, står i et rimeligt forhold til overtrædelserne og har afskrækkende virkning, og som kan omfatte periodiske sanktioner og sanktioner med tilbagevirkende kraft, eller indlede retsforfølgning med henblik på at pålægge bøder,
- overvåge den teknologiske og relevante kommercielle udvikling af relevans for tilrådighedsstillelsen og anvendelsen af data,
- samarbejde med andre medlemsstaters kompetente myndigheder og, hvis det er relevant, Europa-Kommisjonen eller EDIB for at sikre ensartet og effektiv an-

vendelse af dataforordningen, herunder udveksling af alle relevante oplysninger ad elektronisk vej uden unødigt ophold, herunder med hensyn til dataforordningens artikel 37, stk. 10,

- g) samarbejde med de relevante kompetente myndigheder, der er ansvarlige for gennemførelsen af andre EU-retsakter eller nationale retsakter, herunder med myndigheder med kompetence inden for områderne data og elektroniske kommunikationstjenester, med den tilsynsmyndighed, der er ansvarlig for at overvåge anvendelsen af forordning (EU) 2016/679, eller med sektormyndigheder for at sikre, at dataforordningen håndhæves i overensstemmelse med anden EU-ret og national ret,
- h) samarbejde med de relevante kompetente myndigheder for at sikre, at forpligtelserne i dataforordningens artikel 23-31, 34 og 35 håndhæves i overensstemmelse med anden EU-ret og selvregulering, der gælder for udbydere af databehandlingstjenester,
- i) sikre, at skiftegebyrer mellem udbydere af databehandlingstjenester fjernes i overensstemmelse med dataforordningens artikel 29, og
- j) behandle anmodninger om data fremsat i henhold til dataforordningens kapitel V.

Yderligere følger det af artikel 37, stk. 5, sidste pkt., at hvis der er udpeget en datakoordinator, letter denne det i litra f, g og h, omhandlede samarbejde og bistår de kompetente myndigheder på deres anmodning.

Herudover følger det af dataforordningens artikel 37, stk. 6, at datakoordinatoren skal

- a) fungere som et enkelt kontaktpunkt for alle spørgsmål vedrørende dataforordningens anvendelse,
- b) sikre offentlig onlineadgang til offentlige myndigheders anmodninger om at stille data til rådighed i tilfælde af ekstraordinært behov i henhold til dataforordningens kapitel V og fremme frivillige aftaler om datadeling mellem offentlige myndigheder og dataindehavere, og
- c) underrette Kommissionen hvert år om de afslag, der er meddelt i henhold til dataforordningens artikel 4, stk. 2 og 8, og artikel 5, stk. 11.

Af præambelbetragtning nr. 107 i dataforordningen, følger derudover, at hvis der ikke er udpeget nogen datakoordinator, bør den kompetente myndighed påtage sig de opgaver, som datakoordinatoren pålægges i henhold til dataforordningen.

Det foreslås i *stk. 1*, at Digitaliseringsstyrelsen er kompetent myndighed i overensstemmelse med artikel 37, stk. 1, i dataforordningen.

Med den foreslåede bestemmelse vil Digitaliseringsstyrelsen formelt blive udpeget som kompetent myndighed.

Den foreslåede bestemmelse vil medføre, at Digitaliseringsstyrelsen som kompetent myndighed vil blive ansvarlig for

at udføre opgaverne, der er oplistet i dataforordningens artikel 37, stk. 5 og 6.

Kommissionen vil skulle underrettes om udpegningen af Digitaliseringsstyrelsen som kompetent myndighed, og om Digitaliseringsstyrelsens opgaver og beføjelser, jf. artikel 37, stk. 7, 1. pkt., i dataforordningen.

Det foreslås i *stk. 2*, at Digitaliseringsstyrelsen påser overholdelsen af dataforordningen, jf. artikel 37, stk. 1, i dataforordningen, og varetager de opgaver, der er oplistet i dataforordningens artikel 37, stk. 5 og 6.

Den foreslåede bestemmelse indebærer, at Digitaliseringsstyrelsen både vil skulle varetage samtlige af de opgaver, der i henhold til dataforordningen tilfalder kompetente myndigheder, og de opgaver, der i henhold til dataforordningen tilfalder en datakoordinator, idet Digitaliseringsstyrelsen bliver den eneste kompetente myndighed.

Digitaliseringsstyrelsen vil som følge heraf blandt andet kunne foretage egen drift-undersøgelser, behandle klagesager samt anmodninger fra Kommissionen og andre kompetente myndigheder.

Det foreslås i *stk. 3*, at ministeren for digitalisering kan fastsætte nærmere regler om indgivelse af klager efter dataforordningen, herunder formkrav til sådanne klager.

Den foreslåede bestemmelse har til hensigt at give ministeren for digitalisering mulighed for i en bekendtgørelse at fastsætte regler om f.eks. anvendelse af en bestemt digital klageløsning og krav om, at klageren i klageløsningen skal oplyse sit navn, give oplysning om, hvilken fysisk eller juridisk person, som klagen drejer sig om, samt hvori den påståede overtrædelse består og relevant dokumentation herfor.

Til § 3

Det følger af dataforordningens artikel 10, stk. 1, at brugere, dataindehavere og datamodtagere skal have adgang til et tvistbilæggesorgan, der er certificeret i overensstemmelse med dataforordningens artikel 10, stk. 5, til at bilægge tvister i henhold til dataforordningens artikel 4, stk. 3 og 9, og artikel 5, stk. 12, samt tvister vedrørende de fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser for og en gennemsigtig måde at stille data til rådighed på i overensstemmelse med dataforordningens kapitel III og kapitel IV.

Det følger videre af dataforordningens artikel 10, stk. 4, at kunder og udbydere af databehandlingstjenester skal have adgang til et tvistbilæggesorgan, der er certificeret i overensstemmelse med dataforordningens artikel 10, stk. 5, til at bilægge tvister i forbindelse med overtrædelse af kunders rettigheder og de forpligtelser, der påhviler udbydere af databehandlingstjenester, i overensstemmelse med dataforordningens artikel 23-31.

Desuden følger det af dataforordningens artikel 10, stk. 5, at

den medlemsstat, hvori tvistbilæggesorganet er etableret, certificerer det pågældende organ efter dettes anmodning, hvis det har godtgjort, at det opfylder alle følgende betingelser

- a) det er upartisk og uafhængigt, og det skal træffe sine afgørelser i overensstemmelse med klare, ikkeforskelsbehandlende og fair procedureregler,
- b) det har den nødvendige ekspertise, navnlig med hensyn til fair, rimelige og ikkeforskelsbehandlende vilkår og betingelser, herunder godtgørelse, og om at stille data til rådighed på en gennemsigtig måde, således at organet effektivt kan fastsætte disse vilkår og betingelser,
- c) det er let at kontakte ved hjælp af elektronisk kommunikation, og
- d) det er i stand til at vedtage sine afgørelser på en hurtig og omkostningseffektiv måde på mindst ét af Unionens officielle sprog.

Herudover følger det af dataforordningens artikel 10, stk. 6, at medlemsstaterne underretter Kommissionen om de tvistbilæggesorganer, der er certificeret i overensstemmelse dataforordningens artikel 10, stk. 5, og at Kommissionen offentliggør en liste over disse organer på et særligt websted og holder den ajour.

Endvidere følger det af præambelbetragtning nr. 52 i dataforordningen, at det står medlemsstaterne frit for at vedtage eventuelle særlige regler for certificeringsproceduren, herunder certificeringens udløb eller tilbagekaldelse, og at bestemmelserne i dataforordningen om tvistbilæggesorganer ikke bør forpligte medlemsstaterne til at oprette tvistbilæggesorganer.

Det foreslås i § 3, 1. pkt., at ministeren for digitalisering kan fastsætte nærmere regler vedrørende certificering af tvistbilæggesorganer i henhold til artikel 10 i dataforordningen.

Den foreslåede bestemmelse vil medføre, at ministeren for digitalisering får mulighed for at kunne fastsætte nærmere regler vedrørende certificering af tvistbilæggesorganer, såfremt der viser sig at være behov herfor. Der gives dermed mulighed for, at der f.eks. kan fastsættes regler om etablering af certificeringsordning samt proceduren for certificering, herunder hvilken myndighed inden for ministeren for digitaliserings eget ressortområde, der skal forestå certificering, og hvordan ansøgninger om certificering skal indgives, certificeringens udløb og tilbagekaldelse af certificeringer.

Det bemærkes, at opgaven med certificering vil kunne placeres inden for såvel som uden for ministeren for digitaliserings eget ressortområde, jf. bemærkningerne til § 3, 2. pkt.

Det foreslås i § 3, 2. pkt., at ministeren for digitalisering derudover kan fastsætte sådanne regler på andre ministres ressortområder efter aftale med vedkommende minister.

Den foreslåede bestemmelse vil medføre, at ministeren for digitalisering får mulighed for at kunne fastsætte nærmere regler vedrørende certificering af tvistbilæggesorganer inden for andre ministres ressortområde, såfremt der viser

sig at være behov herfor. Sådanne nærmere regler vil dog alene kunne fastsættes efter aftale med vedkommende minister. Med den foreslåede bestemmelse gives der i lighed med det foreslåede 1. pkt. mulighed for, at der f.eks. kan fastsættes regler om etablering af certificeringsordning samt proceduren for certificering, herunder hvilken myndighed uden for ministeren for digitaliserings eget ressortområde, der skal forestå certificering, og hvordan ansøgninger om certificering skal indgives, certificeringens udløb og tilbagekaldelse af certificeringer.

Til § 4

Det følger af dataforordningens artikel 37, stk. 8, at kompetente myndigheder ved udførelsen af deres opgaver og udøvelsen af deres beføjelser i henhold til dataforordningen skal være upartiske og frie for udefrakommende indflydelse, det være sig direkte eller indirekte, og at kompetente myndigheder ikke må søge eller modtage instrukser med henblik på enkeltsager fra nogen anden offentlig myndighed eller nogen privat part.

Det foreslås i *stk. 1*, at Digitaliseringsstyrelsen ved udførelsen af sine opgaver og udøvelsen af sine beføjelser i henhold til dataforordningen og denne lov skal være upartisk og fri for udefrakommende indflydelse, det være sig direkte eller indirekte, og hverken må søge eller modtage instrukser med henblik på enkeltsager fra nogen anden offentlig myndighed eller nogen privat part i overensstemmelse med artikel 37, stk. 8, i dataforordningen.

Den foreslåede bestemmelse fastsætter et bredere anvendelsesområde for artikel 37, stk. 8, i dataforordningen, således at bestemmelsen også omfatter loven. Desuden lovfæster den foreslåede bestemmelse, at Digitaliseringsstyrelsen i enkeltsager ikke vil kunne modtage eller søge instrukser fra andre myndigheder, herunder fra ministeren for digitalisering, uanset at Digitaliseringsstyrelsen i øvrigt er underlagt Digitaliseringsministeriets organisatorisk. I enkeltsager vil Digitaliseringsstyrelsen f.eks. hverken af egen drift kunne søge en instruks fra ministeren for digitalisering eller kunne handle på baggrund af en instruks, som er modtaget fra ministeren for digitalisering. Det bemærkes, at der af dataforordningens ordlyd ikke stilles særlige krav i forhold til kompetente myndigheders funktionelle uafhængighed.

Digitaliseringsstyrelsen vil i forbindelse med sit øvrige arbejde kunne være underlagt instruktioner fra Digitaliseringsministeriet, uden at det vil påvirke, at Digitaliseringsstyrelsen vil være upartisk og fri for udefrakommende indflydelse på området omfattet af dataforordningen og loven.

Bestemmelsen skal ses i sammenhæng med forslagets § 4, stk. 2, hvorefter administrativ rekurs afskæres.

For enkelte sager eller på enkelte områder vil der kunne være behov for særegen fagspecifik ekspertise med henblik på at sikre, at sagerne afgøres på en måde, der stemmer overens med praksis på tilgrænsende fagområder, som henhører under andre myndigheders ressort. I disse tilfælde vil kravet

om uafhængighed ikke forhindre muligheden for, at Digitaliseringsstyrelsen vil kunne rådføre sig eller regelmæssigt udveksle synspunkter med andre myndigheder, herunder datatilsynsmyndigheder, samt indhente teknisk bistand m.v.

Det foreslås i *stk. 2*, at Digitaliseringsstyrelsens afgørelser efter dataforordningen og denne lov ikke kan indbringes for anden administrativ myndighed.

Bestemmelsen vil indebære, at Digitaliseringsstyrelsens afgørelser ikke vil kunne blive undergivet administrativ rekurs. Digitaliseringsstyrelsens afgørelser vil efter de generelle regler kunne indbringes for domstolene.

Den foreslåede bestemmelse skal sikre overensstemmelse med kravene i dataforordningens artikel 37, stk. 8, således at instruktionsbeføjelser afskæres i relation til Digitaliseringsstyrelsens behandling af sager efter dataforordningen.

Til § 5

Det følger af dataforordningens artikel 37, stk. 11, at enhver enhed, der er omfattet af dataforordningens anvendelsesområde, som stiller forbundne produkter til rådighed eller udbyder tjenester i Unionen, og som ikke er etableret i Unionen, udpeger en retlig repræsentant i en af medlemsstaterne.

Desuden følger det af dataforordningens artikel 37, stk. 14, at kompetente myndigheder skal have beføjelse til at anmode brugere, dataindehavere eller datamodtagere samt deres retlige repræsentanter, der hører under deres medlemsstats kompetence, om alle oplysninger, som er nødvendige for at kontrollere efterlevelsen af dataforordningen, og at enhver anmodning om oplysninger skal stå i et rimeligt forhold til, hvad den underliggende opgave kræver, og være begrundet.

Desuden følger det af præambelbetragtning nr. 107 i dataforordningen, at kompetente myndigheder gennem udøvelsen af deres beføjelser i overensstemmelse med gældende nationale procedurer bør kunne søge efter og opnå oplysninger, navnlig vedrørende enheders aktiviteter inden for deres kompetence. Det følger af dataforordningens artikel 37, stk. 10, 1. pkt., at enheder, der er omfattet af dataforordningens anvendelsesområde, er underlagt kompetencen i den medlemsstat, hvor enheden er etableret. Hvis en enhed er etableret i mere end én medlemsstat, anses den for at høre under kompetencen i den medlemsstat, hvor den har sin hovedvirksomhed, jf. artikel 37, stk. 10, sidste pkt., i dataforordningen. Såfremt en enhed ikke er etableret i Unionen, anses enheden for at høre under den medlemsstats kompetence, hvor dens retlige repræsentant befinder sig, jf. artikel 37, stk. 13, 1. pkt., i dataforordningen.

Det foreslås i § 5, at Digitaliseringsstyrelsen kan anmode om alle oplysninger fra fysiske og juridiske personer omfattet af dataforordningen samt retlige repræsentanter omfattet af artikel 37, stk. 11, i dataforordningen, som er nødvendige for Digitaliseringsstyrelsens tilsynsvirksomhed, herunder til

fastlæggelse af, om et forhold hører under Digitaliseringsstyrelsens kompetence.

Bestemmelsen supplerer artikel 37, stk. 14, i dataforordningen.

Personkredsen i den foreslåede bestemmelse er bredere end personkredsen, der fremgår af artikel 37, stk. 14, i dataforordningen, idet den foreslåede oplysningspligt omfatter samtlige fysiske og juridiske personer, som er omfattet af dataforordningen, samt retlige repræsentanter. Der vil som følge heraf kunne kræves oplysninger fra f.eks. producenter, dataindehavere, datamodtagere, brugere, tredjeparter og udbydere af databehandlingstjenester.

Den bredere personkreds skyldes, at effektiv håndhævelse af dataforordningen nødvendiggør, at Digitaliseringsstyrelsen som kompetent myndighed skal have mulighed for at kunne anmode om oplysninger fra alle retssubjekter, der forpligtes af forordningen. Der vil eksempelvis kunne være behov for at få oplysninger fra en producent af forbundne produkter i forbindelse med sager vedrørende dataforordningens artikel 3, stk. 1, hvor producenten har outsourcet dataindehaverrollen. Det bemærkes, at såfremt et retssubjekt er udpeget som gatekeeper i henhold til artikel 3 i forordning (EU) 2022/1925 af 14. september 2022 om åbne og fair markeder i den digitale sektor (forordningen om digitale markeder), forudsættes den foreslåede bestemmelse fortolket i overensstemmelse med forordningen om digitale markeder, navnlig forordningens artikel 5, stk. 1.

Hensigten med den foreslåede bestemmelse er at sikre Digitaliseringsstyrelsen tilstrækkelig mulighed for at søge en sag oplyst. Dette vil blandt andet være af afgørende betydning for vurderingen af, hvor indgribende en foranstaltning der skal træffes samt for at sikre proportionalitet.

Oplysningspligten vil være af væsentlig betydning for, at Digitaliseringsstyrelsen vil kunne håndhæve forordningen. Vurderingen af, hvilke oplysninger der vil blive indhentet, vil altid bero på en proportionalitetsvurdering, og karakteren af den dokumentation, der vil kunne kræves, vil variere fra sag til sag. Oplysningspligten vil blandt andet kunne anvendes til, at Digitaliseringsstyrelsen vil kunne pålægge fysiske og juridiske personer at forelægge relevante dokumenter, tekniske specifikationer, data eller oplysninger om overensstemmelse og tekniske aspekter af produktet eller tjenesten i det omfang en sådan adgang vil være nødvendig for at vurdere overensstemmelsen med dataforordningen.

De oplysninger, som Digitaliseringsstyrelsen vil kunne anmode om, skal være relevante for det, som kontrollen skal belyse, og være tilgængelige for den pågældende. Dette skal ses i sammenhæng med, at Digitaliseringsstyrelsen kun vil kunne anmode om oplysninger, som er nødvendige for at vurdere en potentiel overtrædelse af dataforordningen.

Den foreslåede bestemmelse afgrænses af det almindelige forbud mod at udsætte nogen for selvinkriminering, som det blandt andet kan udledes af Den Europæiske Menneske-

rettighedskonventions artikel 6 og § 10 i retssikkerhedsloven. Er der konkret mistanke om, at det af oplysningerne vil fremgå, at den pågældende har begået noget strafbart, vil det således ikke kunne kræves, at oplysningerne udleveres. I et sådant tilfælde må sagen overlades til politiets efterforskning.

Til § 6

Af dataforordningens artikel 37, stk. 5, litra f, fremgår, at medlemsstaterne sikrer, at opgaverne og beføjelserne for de kompetente myndigheder er klart definerede og omfatter samarbejde med andre medlemsstats kompetente myndigheder og, hvis det er relevant, Europa-Kommissionen eller EDIB for at sikre ensartet og effektiv anvendelse af dataforordningen, herunder udveksling af alle relevante oplysninger ad elektronisk vej uden unødigt ophold, herunder med hensyn til dataforordningens artikel 37, stk. 10.

Det foreslås i § 6, at Digitaliseringsstyrelsen kan videregive oplysninger til Europa-Kommissionen og andre kompetente myndigheder i Den Europæiske Union, i det omfang det er nødvendigt for at påse overholdelsen af bestemmelserne i denne lov, dataforordningen eller den pågældende medlemsstats datadelingslovgivning.

Med »datadelingslovgivning« forstår lovgivning om supplerende bestemmelser til dataforordningen.

Bestemmelsen supplerer artikel 37, stk. 5, litra f, i dataforordningen, idet den sikrer, at der kan leves op til samarbejdsforpligtelsen, der følger heraf.

Bestemmelsen indebærer, at der vil kunne ske videregivelse af oplysninger til Europa-Kommissionen og andre kompetente myndigheder i Den Europæiske Union, selv om oplysningerne måtte være undergivet tavshedspligt. Det gælder dog kun i det omfang, at en sådan videregivelse må anses for nødvendig.

Videregivelse af oplysninger vil skulle ske i overensstemmelse med gældende lovgivning, herunder reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Der henvises til afsnit 2.4 i lovforslagets almindelige bemærkninger.

Til § 7

Det følger af artikel 40, stk. 1, 1. pkt., i dataforordningen, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af dataforordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Af artikel 40, stk. 1, sidste pkt., i dataforordningen, følger, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning.

Desuden følger det af præambelbetragtning nr. 109 i dataforordningen, at kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i dataforordnin-

gen, er underlagt sanktioner, og at sådanne sanktioner kan omfatte irettesættelser.

Det foreslås i § 7, at Digitaliseringsstyrelsen kan udtale kritik af fysiske og juridiske personer omfattet af dataforordningen for overtrædelser af dataforordningen eller denne lov.

Bestemmelsen supplerer artikel 40, stk. 1, i dataforordningen.

Bestemmelsen skal tydeliggøre, at Digitaliseringsstyrelsen kan udtale kritik af fysiske og juridiske personer omfattet af dataforordningen. Kritik vil alene kunne udtales for overtrædelser af dataforordningen eller denne lov.

Muligheden for at udtale kritik vil eksempelvis kunne anvendes ved en overtrædelse, som efter en samlet vurdering anses for at udgøre en mindre alvorlig overtrædelse. Dette kunne f.eks. være i sager om manglende efterlevelse af en underretningspligt. Herudover vil muligheden for at udtale kritik kunne være relevant i forhold til overtrædelser, hvor det konkret vurderes, at meddelelse af et påbud efter § 9 ikke vil kunne rette op på forholdet.

Til § 8

Det følger af artikel 37, stk. 5, litra a, i dataforordningen, at medlemsstaterne sikrer, at opgaverne og beføjelserne for de kompetente myndigheder er klart definerede og omfatter at fremme datakompetence og -bevidsthed blandt brugere og enheder, der er omfattet af dataforordningens anvendelsesområde, om rettigheder og forpligtelser i henhold til dataforordningen.

Desuden følger det af præambelbetragtning nr. 19 i dataforordningen, at der ved datakompetence forstås færdigheder, viden og forståelse, der gør det muligt for brugere, forbrugere og virksomheder, navnlig SMV'er, der falder ind under dataforordningen anvendelsesområde, at få kendskab til den potentielle værdi af de data, som de har genereret, producerer og deler, og som de er motiverede til at tilbyde og give adgang til i overensstemmelse med relevante retsregler. Datakompetence bør være mere end blot læring om værktøjer og teknologier og bør sigte mod at give borgere og virksomheder evne og myndighed til at drage fordel af et inklusivt og retfærdigt datamarked.

Det følger yderligere af artikel 40, stk. 1, 1. pkt., i dataforordningen, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af dataforordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Af artikel 40, stk. 1, sidste pkt., i dataforordningen, følger, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning.

Endvidere følger det af præambelbetragtning nr. 109 i dataforordningen, at kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i dataforordnin-

gen, er underlagt sanktioner, og at sådanne sanktioner kan omfatte økonomiske sanktioner, advarsler, irettesættelser eller påbud om at bringe forretningspraksis i overensstemmelse med forpligtelserne pålagt ved dataforordningen.

Det foreslås i § 8, at Digitaliseringsstyrelsen kan offentliggøre sine udtalelser efter § 7 og afgørelser efter § 9 om overtrædelser af dataforordningen eller denne lov.

Begrebet sanktioner i artikel 40, stk. 1, i dataforordningen, dækker over en række forskellige reaktioner, hvilket kommer til udtryk i den ikkeudtømmende opstilling af eksempler på sanktioner i dataforordningens præambelbetragtning nr. 109, som omfatter både økonomiske og ikke-økonomiske sanktioner.

Bestemmelsen supplerer artikel 37, stk. 5, litra a, og artikel 40, stk. 1, i dataforordningen.

Bestemmelsen skal sikre, at Digitaliseringsstyrelsen, som en nødvendig og effektiv sanktion samt som led i varetagelsen af opgaven med at fremme datakompetence og -bevidsthed, vil kunne offentliggøre udtalelser og afgørelser i sager om overtrædelser af dataforordningen, når samfundsmæssige hensyn taler for offentliggørelse.

Offentliggørelse i henhold til den foreslåede § 8 vil kunne omfatte navnet på den juridiske eller fysiske person, som er adressat for udtalelsen eller afgørelsen, samt oplysninger om overtrædelser af dataforordningen eller loven, herunder oplysninger om forhold omfattet af § 10. Digitaliseringsstyrelsen vil blandt andet kunne vælge at offentliggøre udtalelser eller afgørelser i henhold til den foreslåede § 8 for at afværge betydelige formuetab. Offentliggørelse vil endvidere kunne ske, hvis offentliggørelsen er nødvendig for, at blandt andet forbrugere og erhvervsdrivende kan varetage deres interesser i forhold til de fysiske eller juridiske personer, som der offentliggøres oplysninger om. Offentliggørelse vil dog aldrig kunne ske, hvis offentliggørelsen vil medføre uforholdsmæssig stor skade for den juridiske eller fysiske person i forhold til de hensyn, som taler for offentliggørelse. Det afgørende vil være, om offentlighedens interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private og offentlige interesser. I tvivlstilfælde vil det være naturligt at indhente en udtalelse fra de pågældende fysiske eller juridiske personer, som berøres af Digitaliseringsstyrelsens udtalelse eller afgørelse om overtrædelse af dataforordningen.

Det bemærkes, at der ikke er tale om en generel hjemmel til systematisk offentliggørelse, men udelukkende om en mulighed for offentliggørelse baseret på en konkret vurdering, hvor hensynet til de fysiske eller juridiske personer, som oplysningerne vedrører, afvejes over for de hensyn til samfundsmæssige interesser, der søges varetaget ved offentliggørelse.

Det bemærkes desuden, at der i den enkelte sag vil blive foretaget en konkret vurdering af, om udtalelsen eller afgørelsen indeholder oplysninger, der skal anonymiseres, lige-

som der vil blive foretaget en konkret vurdering af, om hele eller dele af udtalelsen eller afgørelsen skal offentliggøres, herunder om offentliggørelse alene skal ske i form af et resumé. Offentliggørelse i ikke anonymiseret form eller i begrænset anonymiseret form, dvs. hvor blot enkelte oplysninger ikke offentliggøres, vil være af særlig relevans i de tilfælde, hvor offentliggørelse særligt tjener en sanktionsmæssig funktion og foretages med henblik på f.eks. at afværge betydelige formuetab, eller for at forbrugere og erhvervsdrivende kan varetage deres interesser i forhold de fysiske eller juridiske personer, som der offentliggøres oplysninger om. Hvor offentliggørelse i stedet foretages med henblik på f.eks. at yde mere generel vejledning vedrørende dataforordningen og Digitaliseringsstyrelsens praksis, vil offentliggørelse i anonymiseret form imidlertid være af særlig relevans.

Til § 9

Det følger af artikel 40, stk. 1, 1. pkt., i dataforordningen, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af dataforordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Af artikel 40, stk. 1, sidste pkt., i dataforordningen, følger, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning.

Det følger desuden af præambelbetragtning nr. 109 i dataforordningen, at kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i dataforordningen, er underlagt sanktioner, og at sådanne sanktioner kan omfatte påbud om at bringe forretningspraksis i overensstemmelse med forpligtelserne pålagt ved dataforordningen.

Det foreslås i § 9, at Digitaliseringsstyrelsen kan udstede påbud til fysiske og juridiske personer omfattet af dataforordningen med henblik på at sikre overholdelsen af forpligtelser i medfør dataforordningen.

Bestemmelsen supplerer artikel 40, stk. 1, i dataforordningen.

Påbud vil kunne rettes mod fysiske og juridiske personer omfattet af dataforordningen.

Påbud vil kunne gives for at få en fysisk eller en juridisk person til at opfylde en forpligtelse, som denne har i henhold til dataforordningen, eller til at afstå fra at udføre visse handlinger. Påbud vil f.eks. kunne omfatte krav om foretagelse af ændringer, ophør af handlinger, opfyldelse af standarder, deling af data, nedsættelse af godtgørelse eller nedsættelse af skiftegebyrer.

Manglende efterkommelse af påbud udstedt efter § 9 vil kunne straffes med bøde, jf. lovforslagets § 10, stk. 1, nr. 3. Digitaliseringsstyrelsen vil dog kun kunne foretage politianmeldelse med henblik på at opnå dom for forholdet, såfremt der i påbuddet er blevet fastsat en frist for efterkommelse af påbuddet, dvs. en frist for, hvornår påbuddet

senest skal opfyldes, og denne frist er sprunget. Ved fristfastsættelsen vil Digitaliseringsstyrelsen skulle lægge vægt på karakteren og omfanget af den pligt, som den pågældende påbydes at opfylde.

Til § 10

Det følger af artikel 37, stk. 5, litra d, i dataforordningen, at medlemsstater sikrer, at opgaverne og beføjelserne for de kompetente myndigheder er klart definerede og omfatter at pålægge økonomiske sanktioner, der er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning, og som kan omfatte periodiske sanktioner og sanktioner med tilbagevirkende kraft, eller indlede retsforfølgning med henblik på at pålægge bøder.

Af artikel 40, stk. 1, 1. pkt., i dataforordningen følger desuden, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af dataforordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Af artikel 40, stk. 1, sidste pkt., i dataforordningen, følger videre, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Herudover følger det af præambelbetragtning nr. 109 i dataforordningen, at kompetente myndigheder bør sikre, at overtrædelser af de forpligtelser, der er fastsat i dataforordningen, er underlagt sanktioner, og at sådanne sanktioner kan omfatte økonomiske sanktioner.

Yderligere følger det af dataforordningens artikel 40, stk. 3, at medlemsstaterne ved sanktionering tager hensyn til anbefalingerne fra EDIB og følgende ikkeudtømmende kriterier for pålæggelse af sanktioner for overtrædelse af dataforordningen:

- a) Overtrædelsens art, grovhed, omfang og varighed.
- b) Eventuelle tiltag, som den overtrædende part har truffet for at afbøde eller afhjælpe den skade, der er forårsaget af overtrædelsen.
- c) Den overtrædende parts eventuelle tidligere overtrædelser.
- d) De økonomiske fordele eller tab, som den overtrædende part har opnået eller undgået som følge af overtrædelsen, for så vidt som disse fordele eller tab kan fastslås på en pålidelig måde.
- e) Eventuelle andre skærpende eller formildende faktorer i lyset af sagens omstændigheder.
- f) Den overtrædende parts årlige omsætning i det foregående regnskabsår i Unionen.

Det foreslås i § 10, at det fastsættes, hvilke bestemmelser i forordningen og loven der er straffelagt med bøder.

Det foreslås i *stk. 1, nr. 1*, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der uagtsomt eller forsætligt overtræder dataforordningens artikel 3, artikel 4, stk. 1, 2, 4-8, 10, 11, 13 eller 14, artikel 5, stk. 1, 3-6 eller 9-11, artikel 6, stk. 1 eller 2, artikel 8, stk. 4, artikel 11, 14, 23, 25-28, artikel 29, stk. 1, 3, 5 eller 6,

artikel 30, stk. 1-5, artikel 31, stk. 3, eller artikel 32, stk. 1, 4 eller 5.

Med den foreslåede bestemmelse sikres det, at overtrædelse af visse af dataforordningens artikler vil kunne sanktioneres med bøder. De oplyste artikler i den foreslåede bestemmelse omfatter navnlig:

- Forpligtelser vedrørende tilgængeliggørelse, tilrådighedsstillelse og anvendelse af produktdata og relaterede tjenstedata. (artikel 3, stk. 1, artikel 4, stk. 1, 2, 4-8, 10, 11, 13 og 14, artikel 5, stk. 1, 3-6 og 9-11, artikel 6, stk. 1 og 2, og artikel 8, stk. 4, i dataforordningen)
- Oplysningspligter vedrørende forbundne produkter og relaterede tjenester. (artikel 3, stk. 2 og 3, i dataforordningen)
- Forpligtelser vedrørende tekniske beskyttelsesforanstaltninger om uautoriseret anvendelse eller videregivelse af data. (artikel 11, i dataforordningen)
- Forpligtelser vedrørende tilrådighedsstillelse af data på grundlag af et ekstraordinært behov. (artikel 14, i dataforordningen)
- Forpligtelser vedrørende skift mellem databehandlingstjenester. (artikel 23, 25-28, artikel 29, stk. 1, 3, 5 og 6, artikel 30, stk. 1-5, og artikel 31, stk. 3, i dataforordningen)
- Forpligtelser vedrørende adgang til og overførsel af andre data end personoplysninger til tredjelande. (artikel 32, stk. 1, 4 og 5, i dataforordningen)

Den foreslåede bestemmelse fraviger ikke udgangspunktet i straffelovens § 19, 2. pkt., hvorfor det vil være tilstrækkeligt, at overtrædelsen er blevet begået af uagtsomhed.

Det foreslås herudover i *stk. 1, nr. 2*, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der uagtsomt eller forsætligt undlader at efterkomme Digitaliseringsstyrelsens krav efter § 5, eller som i forbindelse med sådanne krav afgiver ukorrekte, ufuldstændige eller vildledende oplysninger eller fortier oplysninger.

Med den foreslåede bestemmelse sikres det, at det vil kunne sanktioneres, hvis fysiske og juridiske personer undlader at imødekomme krav fra Digitaliseringsstyrelsen om at afgive oplysninger, som er nødvendige for Digitaliseringsstyrelsens tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under Digitaliseringsstyrelsens kompetence. Ligeledes sikres det med den foreslåede bestemmelse, at det vil kunne sanktioneres, hvis fysiske eller juridiske personer som svar på krav fra Digitaliseringsstyrelsen giver oplysninger, der er ukorrekte, ufuldstændige eller vildledende, eller fortier oplysninger, som er nødvendige for Digitaliseringsstyrelsens tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under Digitaliseringsstyrelsens kompetence.

Den foreslåede bestemmelse fraviger ikke udgangspunktet i straffelovens § 19, 2. pkt., hvorfor det vil være tilstrækkeligt, at overtrædelsen er blevet begået af uagtsomhed.

Den foreslåede bestemmelse afgrænses af det almindelige forbud mod at udsætte nogen for selvinkriminering, som det blandt andet kan udledes af Den Europæiske Menneskerettighedskonventions artikel 6 og § 10 i retssikkerhedsloven.

Desuden foreslås det i *stk. 1, nr. 3*, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der uagtsomt eller forsætligt undlader at efterkomme et påbud udstedt efter § 9.

Med den foreslåede bestemmelse sikres det, at det vil kunne sanktioneres, hvis fysiske og juridiske personer undlader at efterkomme Digitaliseringsstyrelsens påbud.

Den foreslåede bestemmelse fraviger ikke udgangspunktet i straffelovens § 19, 2. pkt., hvorfor det vil være tilstrækkeligt, at overtrædelsen er blevet begået af uagtsomhed.

Forbeholdet i lovforslagets § 10, stk. 1, om, at højere straf kan være forskyldt efter den øvrige lovgivning, har til formål at sikre, at handlinger, der tillige indebærer en overtrædelse af bestemmelser, der vil kunne medføre højere straf, vil kunne henføres under sådanne bestemmelser. Hvis det strafbare forhold f.eks. omfattes af § 10, stk. 1, nr. 2, samt straffelovens §§ 162 og 163 om afgivelse af urigtige oplysninger til offentlige myndigheder, henhører forholdet således under den bestemmelse, hvorefter den højeste straf er forskyldt.

Ved fastsættelse af bødestørrelsen vil der i sager omfattet af § 10, stk. 1, skulle tages hensyn til de ikkeudtømmende kriterier i artikel 40, stk. 3, litra a-f, i dataforordningen, samt anbefalinger fra EDIB, såfremt sådanne anbefalinger måtte foreligge på tidspunktet for fastsættelsen af bødens størrelse.

Herudover foreslås det i *stk. 2*, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Den foreslåede bestemmelse vil medføre, at der kan pålægges juridiske personer strafansvar for overtrædelse af de strafbelagte bestemmelser i § 10, stk. 1.

Endvidere foreslås det i *stk. 3*, at forældelsesfristen for overtrædelse af dataforordningen eller denne lov er 5 år.

Den foreslåede bestemmelse vil medføre, at forældelsesfristen for overtrædelser af dataforordningen eller denne lov er 5 år.

Der henvises til afsnit 2.5 i lovforslagets almindelige bemærkninger.

Til § 11

Det foreslås i § 11, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Den foreslåede bestemmelse vil medføre, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende. Det skyldes, at de foreslåede bestemmelser bør træde i kraft hurtigt henset til, at dataforordningen finder anvendelse fra den 12. september 2025, dog med en række nærmere, specifikke undtagelser, jf. nedenstående. Der er derfor behov for hurtigt at give Digitaliseringsstyrelsen beføjelser til at understøtte effektiv håndhævelse af dataforordningen.

For så vidt angår undtagelser til anvendelsesdatoen, jf. ovenstående, bemærkes, at forpligtelsen, der følger af dataforordningens artikel 3, stk. 1, finder anvendelse på forbundne produkter og de hermed relaterede tjenester, der bringes i omsætning efter den 12. september 2026. Hertil kommer, at dataforordningens kapitel III kun finder anvendelse i forbindelse med forpligtelser til at stille data til rådighed i henhold til EU-ret eller national lovgivning vedtaget i overensstemmelse med EU-retten, som træder i kraft efter den 12. september 2025. Dataforordningens kapitel IV finder anvendelse på aftaler, der indgås efter den 12. september 2025. På aftaler, der indgås senest den 12. september 2025, finder dataforordningens kapitel IV anvendelse fra den 12. september 2027, forudsat at de er af ubegrænset varighed, eller at de udløber mindst 10 år efter 11. januar 2024. Det bemærkes i forhold til skiftegebyrer, at det følger af artikel 29, stk. 1, i dataforordningen, at udbydere af databehandlingstjenester ikke må pålægge kunder skiftegebyrer for skifteprocessen fra den 12. januar 2027. Endvidere følger det af dataforordningens artikel 29, stk. 2, at udbydere af databehandlingstjenester i perioden 11. januar 2024 til 12. januar 2027 alene kan pålægge kunder nedsatte skiftegebyrer for skifteprocessen. For så vidt angår perioden fra den 11. januar 2024 og frem til lovens ikrafttræden vil det ikke være muligt strafferetligt at sanktionere overtrædelser af dataforordningens artikel 29, stk. 2.

Til § 12

Det foreslås i § 12, at loven ikke skal gælde for Færøerne og Grønland.