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

(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 Det Europæiske Økonomiske og Sociale Udvalg ([1]),

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([2]), og

ud fra følgende betragtninger:

(1) Digitaliseringen af økonomien går stadig hurtigere. Informations- og kommunikationsteknologi er ikke længere en specifik sektor, men grundlaget for alle moderne innovative økonomiske systemer og samfund. Elektroniske data er kernen i disse systemer og kan skabe stor værdi, når de analyseres eller kombineres med tjenester og varer. Samtidig betyder den hastige udvikling af dataøkonomien og de fremspirende teknologier som f.eks. kunstig intelligens, produkter og tjenesteydelser med tilknytning til tingenes internet, autonome systemer og 5G, at der opstår nye retlige spørgsmål med hensyn til adgang til og genanvendelse af data, ansvarsforhold, etik og solidaritet. Der bør overvejes at iværksætte en arbejdsindsats vedrørende ansvarsforhold, navnlig ved gennemførelse af selvregulerende kodekser og andre former for bedste praksis, under hensyntagen til henstillinger, afgørelser og handlinger, der udføres uden menneskelig medvirken gennem hele databehandlingsværdikæden. Dette arbejde kan også omfatte passende mekanismer til ansvarsplacering, til overførsel af ansvar mellem samarbejdende tjenester, til forsikring og til audit.

(2) Dataværdikæder bygger på forskellige dataaktiviteter: frembringelse og indsamling af data; aggregering og organisation af data; behandling af data; analyse, markedsføring og distribution af data; anvendelse og genanvendelse af data. Formålstjenlig og effektiv behandling af data er en grundlæggende byggesten i dataværdikæden. Dog hæmmes den formålstjenlige og effektive databehandlings funktion og udviklingen af dataøkonomien i Unionen af navnlig to typer af hindringer for datamobilitet og for det indre marked: dataplaceringskrav fastsat af medlemsstaternes myndigheder og praksis med leverandørbinding i den private sektor.

(3) Etableringsfriheden og den frie udveksling af tjenesteydelser i henhold til traktaten om Den Europæiske Unions funktionsmåde (»TEUF«) gælder også for databehandlingstjenester. Imidlertid bliver leveringen af disse tjenester hæmmet eller forhindret af visse nationale, regionale eller lokale krav vedrørende datas placering i et bestemt område.

(4) Disse hindringer for fri udveksling af databehandlingstjenester og for etableringsretten for tjenesteleverandører skyldes krav i medlemsstaternes lovgivninger om, at data behandles inden for et bestemt geografisk område eller territorium. Andre regler eller anden administrativ praksis har en tilsvarende virkning ved at pålægge specifikke krav, som gør det vanskeligere at behandle data uden for et bestemt geografisk område eller territorium inden for Unionen, f.eks. krav om brug af teknologiske faciliteter, der er certificeret eller godkendt i en bestemt medlemsstat. Usikkerhed om retstilstanden med hensyn til rækkevidden af berettigede og uberettigede dataplaceringskrav begrænser yderligere markedsdeltagernes og den offentlige sektors valgmuligheder med hensyn til, hvor data behandles. Denne forordning begrænser på ingen måde virksomheder i at indgå kontrakter, der angiver, hvor data skal placeres. Denne forordning har blot som hensigt at garantere denne frihed ved at sikre, at en aftalt placering kan ligge overalt inden for Unionen.

([1]) EUT C 227 af 28.6.2018, s. 78.
([2]) Europa-Parlamentets holdning af 4.10.2018 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 6.11.2018.

(5) Samtidig hæmmes datamobilitet i Unionen også af begrænsninger i den private sektor: retlige, kontraktmæssige og tekniske hindringer gør det svært eller umuligt for brugere af databehandlingstjenester at få overført deres data fra én tjenesteleverandør til en anden eller tilbage til deres egne systemer til informationsteknologi (»IT«), ikke mindst efter udløbet af deres kontrakt med en tjenesteleverandør.

(6) Kombinationen af disse hindringer har ført til mangel på konkurrence mellem cloudtjenesteleverandører i Unionen, til forskellige problemer med leverandørbinding og til en alvorlig mangel på datamobilitet. Tilsvarende har dataplaceringspolitikker undergravet forsknings- og udviklingsvirksomheders mulighed for at fremme samarbejde mellem virksomheder, universiteter og andre forskningsinstitutioner med henblik på at fremme innovation.

(7) Hensynet til retssikkerheden og behovet for lige konkurrencevilkår inden for Unionen gør et fælles regelsæt for alle markedsaktører til en vigtig forudsætning for et velfungerende indre marked. For at fjerne de hindringer for samhandelen og de konkurrenceforvridninger, som forskelle mellem de nationale lovgivninger medfører, og for at forhindre, at der opstår yderligere hindringer for samhandelen og væsentlige konkurrenceforvridninger, er det nødvendigt at vedtage ensartede regler, der gælder i alle medlemsstaterne.

(8) De retlige rammer for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og for respekten for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation, og navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([1]), samt Europa-Parlamentets og Rådets direktiv (EU) 2016/680 ([2]) og 2002/58/EF ([3]) berøres ikke af nærværende forordning.

(9) Det ekspanderende tingenes internet, kunstig intelligens og maskinindlæring udgør en vigtig kilde til andre data end personoplysninger, f.eks. som et resultat af, at de anvendes i automatiserede industrielle produktionsprocesser. Konkrete eksempler på andre data end personoplysninger omfatter aggregerede og anonymiserede datasæt, som indgår i big data-analyser, data om præcisionsdyrkning, der kan bidrage til at overvåge og optimere anvendelsen af pesticider og vand, eller data om industrielle maskiners vedligeholdelsesbehov. Hvis teknologiske udviklinger gør det muligt at omdanne anonymiserede data til personoplysninger, behandles sådanne data som personoplysninger, og forordning (EU) 2016/679 skal da finde tilsvarende anvendelse.

(10) I henhold til forordning (EU) 2016/679 må medlemsstaterne hverken indskrænke eller forbyde den frie udveksling af personoplysninger inden for Unionen af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger. Ved nærværende forordning fastsættes samme princip om fri udveksling inden for Unionen for andre data end personoplysninger, medmindre en indskrænkning eller et forbud er berettiget af hensyn til den offentlige sikkerhed. Ved forordning (EU) 2016/679 og nærværende forordning tilvejebringes et sammenhængende sæt af regler, der tager højde for fri bevægelighed for forskellige typer af data. Desuden indfører nærværende forordning ikke en forpligtelse til at lagre de forskellige typer af data hver for sig.

(11) For at skabe en ramme for fri udveksling af andre data end personoplysninger i Unionen og danne grundlag for at videreudvikle dataøkonomien og styrke Unionens industris konkurrenceevne er det nødvendigt at fastlægge en klar, dækkende og forudsigelig retlig ramme for behandling af andre data end personoplysninger på det indre marked. En principbaseret tilgang, der omfatter samarbejde mellem medlemsstaterne og selvregulering, bør sikre, at rammen er tilstrækkelig fleksibel, til at der tages hensyn til udviklingen i behovene hos brugere, tjenesteleverandører og nationale myndigheder i Unionen. For at undgå risikoen for overlap med eksisterende ordninger og dermed undgå at øge byrden for både medlemsstater og virksomheder bør der ikke fastlægges detaljerede tekniske regler.

(12) Denne forordning bør ikke berøre databehandling, for så vidt som den udføres som led i en aktivitet, der falder uden for EU-rettens anvendelsesområde. Navnlig bør det erindres, at den nationale sikkerhed i overensstemmelse med artikel 4 i traktaten om Den Europæiske Union (»TEU«) er den enkelte medlemsstats eneansvar.

([1]) 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).

([2]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89).

([3]) 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 (direktivet om privatlivets fred og elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

(13) Den fri udveksling af data inden for Unionen vil spille en vigtig rolle i forhold til at opnå datadreven vækst og innovation. I lighed med virksomheder og forbrugere vil medlemsstaternes offentlige myndigheder og offentligretlige organer kunne drage fordel af øget valgfrihed med hensyn til datadrevne tjenesteleverandører, af mere konkurrencedygtige priser og af en mere effektiv levering af tjenesteydelser til borgerne. I betragtning af de store mængder data, som offentlige myndigheder og offentligretlige organer håndterer, er det af største vigtighed, at de går foran med et godt eksempel med hensyn til anvendelse af tjenester for elektronisk databehandling, og at de afholder sig fra at lægge begrænsninger på dataplacering, når de gør brug af tjenester for databehandlingstjenester. Offentlige myndigheder og offentligretlige organer bør derfor være omfattet af denne forordning. I denne forbindelse bør princippet om fri udveksling af andre data end personoplysninger, der er fastsat i denne forordning, også finde anvendelse på almen og fast administrativ praksis og på andre dataplaceringskrav inden for offentlige udbud, uden at dette berører Europa-Parlamentets og Rådets direktiv 2014/24/EU ([1]).

(14) Som det er tilfældet med direktiv 2014/24/EU, berører denne forordning ikke love og administrative bestemmelser vedrørende medlemsstaternes interne organisation og fordeling blandt offentlige myndigheder og offentligretlige organer af beføjelser og ansvar vedrørende databehandling uden kontraktmæssig betaling til private parter og berører heller ikke medlemsstaternes love og administrative bestemmelser vedrørende gennemførelsen af disse beføjelser og ansvar. Selv om de offentlige myndigheder og offentligretlige organer tilskyndes til at overveje de økonomiske og andre fordele ved outsourcing til eksterne tjenesteleverandører, kan de have legitime grunde til at vælge selvforsyning med tjenesteydelser eller insourcing. Følgelig pålægger denne forordning på ingen måde medlemsstaterne en forpligtelse til at outsource eller eksternalisere levering af tjenesteydelser, som de ønsker selv at levere eller at organisere på anden vis end gennem offentlige kontrakter.

(15) Denne forordning bør finde anvendelse på fysiske og juridiske personer, der leverer databehandlingstjenester til brugere, som er bosiddende eller etableret i Unionen, herunder på fysiske og juridiske personer, der leverer databehandlingstjenester i Unionen uden at være etableret der. Denne forordning bør derfor ikke finde anvendelse på databehandlingstjenester, der finder sted uden for Unionen, og på dataplaceringskrav vedrørende sådanne data.

(16) Denne forordning fastlægger ikke lovvalgsregler på det handelsretlige område og berører derfor ikke Europa-Parlamentets og Rådets forordning (EF) nr. 593/2008 ([2]). Navnlig er en kontrakt om levering af tjenesteydelser i princippet underlagt loven i det land, hvor tjenesteleverandøren har sit sædvanlige opholdssted, for så vidt som der ikke er foretaget et lovvalg i overensstemmelse med nævnte forordning.

(17) Nærværende forordning bør gælde for databehandling i bredeste forstand og omfatte brugen af alle typer IT-systemer, uanset om de er placeret i brugerens lokaler eller outsourcet til en tjenesteleverandør. Den bør dække forskellige grader af databehandling, fra datalagring (Infrastructure-as-a-Service (IaaS)) til behandling af data på platforme (Platform-as-a-Service (PaaS)) eller i applikationer (Software-as-a-Service (SaaS)).

(18) Dataplaceringskrav udgør en klar hindring for fri udveksling af databehandlingstjenester i Unionen og for det indre marked. Sådanne krav bør forbydes, medmindre de er begrundet i hensynet til den offentlige sikkerhed som fastlagt i EU-retten, navnlig i den i artikel 52 i TEUF anvendte betydning, og overholder proportionalitetsprincippet, der er forankret i artikel 5 i TEU. For at gennemføre princippet om fri udveksling af andre data end personoplysninger på tværs af grænserne, sikre en hurtig afskaffelse af eksisterende dataplaceringskrav og gøre det muligt af driftsmæssige årsager at foretage databehandling flere steder i Unionen, og da der ved denne forordning indføres foranstaltninger til at sikre myndighederne adgang til data i regulerings- og tilsynsøjemed, bør medlemsstaterne kun kunne påberåbe sig hensynet til den offentlige sikkerhed som begrundelse for dataplaceringskrav.

(19) Begrebet »den offentlige sikkerhed«, som omhandlet i artikel 52 i TEUF og som fortolket af Domstolen, omfatter både den interne og eksterne sikkerhed i en medlemsstat samt spørgsmål vedrørende offentlig tryghed med henblik på navnlig at fremme efterforskning, afsløring og retsforfølgelse af strafbare handlinger. Det forudsætter, at der foreligger en reel og tilstrækkelig alvorlig trussel, der påvirker en af de grundlæggende samfundsinteresser, såsom en trussel for driften af institutionerne og de livsvigtige offentlige tjenester og for befolkningens overlevelse samt risikoen for en alvorlig forstyrrelse af de internationale relationer eller af nationers fredelige sameksistens, eller en trussel mod militære interesser. I overensstemmelse med proportionalitetsprincippet bør dataplaceringskrav, der er begrundet i hensynet til den offentlige sikkerhed, være egnede til at nå det tilsigtede mål og ikke gå ud over, hvad der er nødvendigt for at nå dette mål.

([1]) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

([2]) Europa-Parlamentets og Rådets forordning (EF) nr. 593/2008 af 17. juni 2008 om lovvalgsregler for kontraktlige forpligtelser (Rom I) (EUT L 177 af 4.7.2008, s. 6).

(20) For at sikre en effektiv anvendelse af princippet om fri udveksling af andre data end personoplysninger på tværs af grænserne og undgå, at der opstår nye hindringer på det indre marked, bør medlemsstaterne straks underrette Kommissionen om ethvert udkast til retsakt, der indfører nye dataplaceringskrav eller ændrer eksisterende krav. Disse udkast til retsakter bør forelægges og vurderes i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 ([1]).

(21) For at fjerne eventuelle eksisterende hindringer bør medlemsstaterne desuden i løbet af en overgangsperiode på 24 måneder fra denne forordnings anvendelsesdato, tage eksisterende love og administrative bestemmelser af generel karakter, der fastsætter dataplaceringskrav, op til revision og meddele Kommissionen eventuelle dataplaceringskrav, som de anser for at være i overensstemmelse med denne forordning, samt give en begrundelse herfor. Dette bør sætte Kommissionen i stand til at undersøge, om eventuelle resterende dataplaceringskrav er i overensstemmelse. Kommissionen bør have mulighed for, hvor det er hensigtsmæssigt, at fremsætte bemærkninger over for den pågældende medlemsstat. Disse bemærkninger kan omfatte en anbefaling om ændring eller ophævelse af et dataplaceringskrav.

(22) De forpligtelser til at underrette Kommissionen om eksisterende dataplaceringskrav og udkast til retsakter, der er fastsat ved denne forordning, bør finde anvendelse på reguleringsmæssige dataplaceringskrav og udkast til retsakter af generel karakter, men ikke på afgørelser, der retter sig til en konkret fysisk eller juridisk person.

(23) For at skabe klarhed om dataplaceringskravene i medlemsstaterne fastlagt ved lov og administrative bestemmelser af generel karakter for fysiske og juridiske personer, som f.eks. tjenesteleverandører og brugere af databehandlingstjenester, bør medlemsstaterne offentliggøre oplysninger om sådanne krav og jævnligt ajourføre oplysningerne om sådanne foranstaltninger på et nationalt centralt onlineinformationssted. Alternativt bør medlemsstaterne indgive ajourførte oplysninger om sådanne krav til et centralt informationssted, der er oprettet i henhold til en anden EU-retsakt. Med henblik på at sikre, at fysiske og juridiske personer informeres på passende vis om dataplaceringskrav overalt i Unionen, bør medlemsstaterne meddele Kommissionen adresserne på disse nationale centrale onlineinformationssteder. Kommissionen bør offentliggøre disse oplysninger på sit eget websted sammen med en regelmæssigt ajourført, konsolideret liste over samtlige gældende dataplaceringskrav i medlemsstaterne, herunder opsummerede oplysninger om disse krav.

(24) Dataplaceringskrav beror ofte på manglende tillid til databehandling i andre lande, der udspringer af en formodning om, at dataene ikke er tilgængelige for medlemsstaternes kompetente myndigheder, når de f.eks. skal foretage inspektion og audit i regulerings- eller tilsynsøjemed. Sådan manglende tillid kan ikke overvindes udelukkende ved at erklære kontraktvilkår, som forhindrer kompetente myndigheder i at få lovlig adgang til data med henblik på varetagelse af deres officielle opgaver, ugyldige. Denne forordning bør derfor klart fastslå, at den ikke berører de kompetente myndigheders beføjelser til at anmode om eller få adgang til data i overensstemmelse med EU-retten eller national ret, og at kompetente myndigheder ikke kan nægtes adgang til data med den begrundelse, at dataene behandles i en anden medlemsstat. De kompetente myndigheder kan pålægge funktionelle krav for at understøtte adgang til data, såsom krav om, at systembeskrivelser opbevares i den berørte medlemsstat.

(25) Fysiske og juridiske personer, der er underlagt forpligtelser til at indberette data til de kompetente myndigheder, kan opfylde disse forpligtelser ved at give og garantere de kompetente myndigheder effektiv og rettidig elektronisk adgang til dataene, uanset i hvilken medlemsstat dataene behandles. Sådan adgang kan sikres gennem konkrete vilkår og betingelser i kontrakten mellem den fysiske eller juridiske person, der er underlagt forpligtelsen til at give adgang, og tjenesteleverandøren.

(26) Når en fysisk eller juridisk person er underlagt en forpligtelse til at indberette data og ikke opfylder denne forpligtelse, bør den kompetente myndighed kunne søge bistand hos de kompetente myndigheder i andre medlemsstater. I sådanne tilfælde bør de kompetente myndigheder, alt afhængigt af emnet i det pågældende tilfælde, gøre brug af særlige samarbejdsinstrumenter i EU-retten eller internationale aftaler, f.eks., inden for

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

henholdsvis politisamarbejde og samarbejde i strafferetlige, civilretlige og administrative anliggender, Rådets rammeafgørelse 2006/960/RIA ([1]), Europa-Parlamentets og Rådets direktiv 2014/41/EU ([2]), Europarådets konvention om IT-kriminalitet ([3]), Rådets forordning (EF) nr. 1206/2001 ([4]), Rådets direktiv 2006/112/EF ([5]) henholdsvis Rådets forordning (EU) nr. 904/2010 ([6]). I mangel af sådanne særlige samarbejdsordninger bør de kompetente myndigheder samarbejde med hinanden gennem udpegede centrale kontaktpunkter med henblik på at give adgang til de ønskede data.

(27) Hvis en anmodning om bistand indebærer, at den adspurgte myndighed skal have adgang til en fysisk eller juridisk persons lokaler, herunder til udstyr og midler til databehandling, skal en sådan adgang være i overensstemmelse med EU-retten eller national procesret, herunder eventuelle krav om, at der indhentes forudgående retskendelse.

(28) Denne forordning bør ikke gøre det muligt for brugerne at forsøge at unddrage sig anvendelsen af national ret. Den bør derfor fastsætte bestemmelser, som gør det muligt for medlemsstaterne at pålægge brugerne effektive, forholdsmæssige og afskrækkende sanktioner, såfremt de forhindrer de kompetente myndigheder i at få adgang til de nødvendige data med henblik på varetagelsen af de kompetente myndigheders officielle opgaver i henhold til EU-retten eller national ret. I hastende tilfælde, hvor en bruger misbruger sine rettigheder, bør medlemsstaterne have mulighed for at pålægge strengt forholdsmæssige foreløbige foranstaltninger. Foreløbige foranstaltninger, der kræver relokalisering af data i længere tid end 180 dage efter relokaliseringen, ville indebære en tilsidesættelse af princippet om fri udveksling af data i et væsentligt tidsrum, og Kommissionen bør derfor underrettes herom med henblik på en kontrol af deres forenelighed med EU-retten.

(29) Muligheden for at portere data uden hindringer er en afgørende faktor, der øger brugernes valgmuligheder og fremmer effektiv konkurrence på markederne for databehandlingstjenester. De reelle eller formodede problemer med at portere data på tværs af grænserne undergraver også professionelle brugeres tillid til tilbud i andre lande og dermed deres tillid til det indre marked. Mens fysiske personer og forbrugere nyder godt af eksisterende EU-ret, fremmer den ikke mulighederne for at skifte tjenesteleverandør for brugere, der handler i forbindelse med deres forretnings- eller erhvervsmæssige aktiviteter. Ensartede tekniske krav i Unionen, uanset om det drejer sig om teknisk harmonisering, gensidig anerkendelse eller frivillig harmonisering, bidrager også til at udvikle et konkurrencedygtigt indre marked for databehandlingstjenester.

(30) For at høste det fulde udbytte af et konkurrencepræget miljø bør professionelle brugere kunne træffe informerede valg og nemt kunne sammenligne de enkelte elementer i de forskellige databehandlingstjenester, der udbydes på det indre marked, herunder af kontraktvilkår og -betingelser for dataportering ved opsigelse af en kontrakt. På baggrund af innovationspotentialet på markedet samt erfaringerne og ekspertisen hos tjenesteleverandører og professionelle brugere af databehandlingstjenester bør markedsdeltagerne ved selvregulering fastlægge detaljerede informationskrav og operationelle krav vedrørende dataportering, og selvreguleringen bør fremmes og overvåges af Kommissionen og tage form af EU-adfærdskodekser, som kan omfatte standardkontraktvilkår og -betingelser.

(31) For at være effektive og gøre leverandørskift og dataportering lettere bør sådanne adfærdskodekser være omfattende og dække mindst de centrale aspekter, som er vigtige under dataporteringsprocessen, såsom procedurerne, der finder anvendelse for, og placeringen af databackup, de dataformater og -medier, der er til rådighed, den krævede IT-konfiguration og minimumsbåndbredde, hvor lang tid der går, inden porteringsprocessen kan sættes i gang, og hvor lang tid dataene forbliver tilgængelige til portering, samt garantierne for adgang til data, såfremt tjenesteleverandøren går konkurs. Adfærdskodekserne bør også gøre det klart, at leverandørbinding ikke er acceptabel forretningspraksis, de bør fastsætte bestemmelser om tillidsfremmende teknologier og bør ajourføres regelmæssigt for at holde trit med den teknologiske udvikling. Kommissionen bør sikre, at alle berørte interessenter, herunder sammenslutninger af små og mellemstore virksomheder (SMV'er) og nystartede virksomheder, brugere og cloudtjenesteleverandører høres igennem hele processen. Kommissionen bør evaluere udviklingen og effektiviteten af gennemførelsen af sådanne adfærdskodekser.

([1]) Rådets rammeafgørelse 2006/960/RIA af 18. december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder (EUT L 386 af 29.12.2006, s. 89).
([2]) Europa-Parlamentets og Rådets direktiv 2014/41/EU af 3. april 2014 om den europæiske efterforskningskendelse i straffesager (EUT L 130 af 1.5.2014, s. 1).
([3]) Europarådets konvention om IT-kriminalitet, CETS nr. 185.
([4]) Rådets forordning (EF) nr. 1206/2001 af 28. maj 2001 om samarbejde mellem medlemsstaternes retter om bevisoptagelse på det civil- og handelsretlige område (EFT L 174 af 27.6.2001, s. 1).
([5]) Rådets direktiv 2006/112/EF af 28. november 2006 om det fælles merværdiafgiftssystem (EUT L 347 af 11.12.2006, s. 1).
([6]) Rådets forordning (EU) nr. 904/2010 af 7. oktober 2010 om administrativt samarbejde og bekæmpelse af svig vedrørende merværdiafgift (EUT L 268 af 12.10.2010, s. 1).

(32) Når en kompetent myndighed i en medlemsstat anmoder om bistand fra en anden medlemsstat til at få adgang til data i henhold til denne forordning, bør den gennem et centralt kontaktpunkt indgive en behørigt begrundet anmodning til sidstnævntes centrale kontaktpunkt, herunder en skriftlig redegørelse for begrundelsen og retsgrundlaget for at søge adgang til dataene. Det centrale kontaktpunkt, der er udpeget af den medlemsstat, der anmodes om bistand, bør lette videresendelsen af anmodningen til den relevante kompetente myndighed i den anmodede medlemsstat. For at sikre et effektivt samarbejde bør den myndighed, som anmodningen er sendt til, uden unødigt ophold yde den bistand, der anmodes om i en given anmodning, eller oplyse om opståede vanskeligheder med at imødekomme anmodningen eller om begrundelsen for at afvise den.

(33) Hvis tilliden til sikkerheden i forbindelse med databehandling i andre medlemsstater styrkes, bør det mindske tilbøjeligheden hos markedsdeltagerne og i den offentlige sektor til at bruge placeringen af data som substitut for datasikkerhed. Det bør også forbedre retssikkerheden for virksomhederne med hensyn til overholdelse af gældende sikkerhedskrav, når de outsourcer deres databehandling til tjenesteleverandører, herunder sådanne i andre medlemsstater.

(34) Ethvert sikkerhedskrav vedrørende databehandling, der anvendes på en berettiget og forholdsmæssig måde på grundlag af EU-retten eller national ret i overensstemmelse med EU-retten i den medlemsstat, hvor den fysiske eller juridiske person, hvis data er berørt, er bosiddende eller etableret, bør fortsat finde anvendelse på behandling af disse data i en anden medlemsstat. Disse fysiske og juridiske personer bør kunne opfylde sådanne krav egenhændigt eller i kraft af bestemmelser i kontrakter med tjenesteleverandørerne.

(35) Sikkerhedskrav, der fastsættes på nationalt plan, bør være nødvendige og stå i et rimeligt forhold til de sikkerhedsrisici i forbindelse med databehandling, der er omfattet af den nationale lovgivning, hvori disse krav fastsættes.

(36) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([1]) indeholder bestemmelser om retlige foranstaltninger, der skal øge det samlede cybersikkerhedsniveau i Unionen. Databehandlingstjenester er blandt de digitale tjenester, der er omfattet af nævnte direktiv. I henhold til nævnte direktiv skal medlemsstaterne sikre, at tjenesteleverandører af digitale tjenester identificerer og træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i net- og informationssystemer, som de anvender. Disse foranstaltninger bør garantere et sikkerhedsniveau, der står i forhold til risikoen, idet der tages hensyn til systemers og faciliteters sikkerhed, håndtering af hændelser, styring af driftskontinuitet, overvågning, audit og testning og overholdelse af internationale standarder. Disse elementer skal specificeres yderligere i gennemførelsesretsakter, som Kommissionen vedtager i henhold til direktivet.

(37) Kommissionen bør forelægge en rapport om gennemførelsen af denne forordning, særlig med henblik på at afgøre, om der er behov for ændringer i lyset af udviklingen i de teknologiske betingelser og markedsvilkårene. Denne rapport bør navnlig evaluere denne forordning, særlig anvendelsen heraf i forhold til datasæt bestående af både personoplysninger og andre data end personoplysninger, samt gennemførelsen af undtagelsen med hensyn til den offentlige sikkerhed. Inden denne forordning begynder at finde anvendelse, bør Kommissionen ligeledes offentliggøre retningslinjer for håndtering af datasæt bestående af både personoplysninger og andre data end personoplysninger, således at virksomheder, herunder SMV'er, bedre forstår samspillet mellem denne forordning og forordning (EU) 2016/679, og det sikres, at begge forordninger overholdes.

(38) Nærværende forordning respekterer de grundlæggende rettigheder og overholder de principper, som anerkendes i bl.a. Den Europæiske Unions charter om grundlæggende rettigheder, og bør fortolkes og anvendes i overensstemmelse med disse rettigheder og principper, herunder retten til beskyttelse af personoplysninger, ytrings- og informationsfriheden og friheden til at oprette og drive egen virksomhed.

(39) Målet for denne forordning, nemlig at sikre fri udveksling af andre data end personoplysninger i Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af dets omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i TEU. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål —

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Formålet med denne forordning er at sikre fri udveksling af andre data end personoplysninger inden for Unionen ved at fastsætte bestemmelser om dataplaceringskrav, kompetente myndigheders adgang til data og dataportering for professionelle brugere.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på behandling i Unionen af elektroniske andre data end personoplysninger, når denne behandling:

a) leveres som en tjeneste til brugere, der er bosiddende eller etableret i Unionen, uanset om tjenesteleverandøren er etableret i Unionen eller ej, eller

b) foretages af en fysisk eller juridisk person, der er bosiddende eller etableret i Unionen, til eget behov.

2. I tilfælde af datasæt bestående af både personoplysninger og andre data end personoplysninger finder denne forordning anvendelse på den del af sættet, der omfatter andre data end personoplysninger. Når personoplysninger og andre data end personoplysninger i et datasæt er knyttet uløseligt sammen, berører nærværende forordning ikke anvendelsen af forordning (EU) 2016/679.

3. Nærværende forordning finder ikke anvendelse på aktiviteter, der falder uden for EU-rettens anvendelsesområde.

Denne forordning berører ikke love og administrative bestemmelser, som vedrører medlemsstaternes interne organisation, og som fordeler beføjelser og ansvar med hensyn til databehandling blandt offentlige myndigheder og offentligretlige organer, som defineret i artikel 2, stk. 1, nr. 4), i direktiv 2014/24/EU, uden kontraktmæssig betaling til private parter, og berører heller ikke medlemsstaternes love og administrative bestemmelser vedrørende gennemførelsen af disse beføjelser og ansvar.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) »data«: andre data end personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679

2) »behandling«: enhver aktivitet eller række af aktiviteter, med eller uden brug af automatisk behandling, som data eller datasæt i elektronisk format gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

3) »udkast til retsakt«: en tekst, der er udarbejdet med henblik på vedtagelse som en lov eller administrativ bestemmelse af generel karakter, og som befinder sig på det forberedende stadium, hvor det stadig er muligt at foretage væsentlige ændringer

4) »tjenesteleverandør«: en fysisk eller juridisk person, der leverer databehandlingstjenester

5) »dataplaceringskrav«: enhver forpligtelse, betingelse og begrænsning og ethvert forbud eller andet krav, der er fastsat i en medlemsstats love og administrative bestemmelser, eller som følger af almen og fast administrativ praksis i en medlemsstat og i offentligretlige organer, herunder inden for offentlige udbud, uden at dette berører direktiv 2014/24/EU, og som indebærer, at databehandling skal finde sted i en bestemt medlemsstat, eller forhindrer databehandling i enhver anden medlemsstat

6) »kompetent myndighed«: en myndighed i en medlemsstat eller enhver anden enhed, der i henhold til national ret er bemyndiget til at udføre en offentlig funktion eller udøve offentlig myndighed, der med henblik på varetagelse af sine officielle opgaver har beføjelse til at få adgang til data, der behandles af en fysisk eller juridisk person i henhold til EU-retten eller national ret

7) »bruger«: en fysisk eller juridisk person, herunder en offentlig myndighed eller et offentligretligt organ, der benytter eller anmoder om en databehandlingstjeneste

8) »professionel bruger«: en fysisk eller juridisk person, herunder en offentlig myndighed eller et offentligretligt organ, der benytter eller anmoder om en databehandlingstjeneste i forbindelse med sit erhverv, sin forretning, sit håndværk, sin profession eller sine opgaver.

Artikel 4

Fri bevægelighed af data inden for Unionen

1. Dataplaceringskrav er forbudt, medmindre de er begrundet i hensynet til den offentlige sikkerhed og i overensstemmelse med proportionalitetsprincippet.

Dette stykkes første afsnit berører ikke stk. 3 eller dataplaceringskrav, som er fastsat på grundlag af eksisterende EU-ret.

2. Medlemsstaterne underretter straks Kommissionen om ethvert udkast til retsakt, der indebærer nye dataplaceringskrav eller ændringer af eksisterende dataplaceringskrav, i overensstemmelse med de procedurer, der er fastsat i artikel 5, 6 og 7 i direktiv (EU) 2015/1535.

3. Senest den 30. maj 2021 sikrer medlemsstaterne, at ethvert eksisterende dataplaceringskrav, som er fastsat i en lov eller administrativ bestemmelse af generel karakter, og som ikke er i overensstemmelse med nærværende artikels stk. 1, ophæves.

Senest den 30. maj 2021 skal en medlemsstat, der finder, at en eksisterende foranstaltning, som indeholder et dataplaceringskrav, er i overensstemmelse med nærværende artikels stk. 1 og derfor kan forblive i kraft, underrette Kommissionen om den pågældende foranstaltning, idet den giver en begrundelse for at opretholde foranstaltningen. Uden at det berører artikel 258 i TEUF, undersøger Kommissionen inden for en frist på seks måneder fra datoen for modtagelsen af en sådan underretning, om den pågældende foranstaltning er i overensstemmelse med nærværende artikels stk. 1, og den fremsætter, hvis det er relevant, bemærkninger over for den pågældende medlemsstat, herunder om nødvendigt en anbefaling om, at foranstaltningen ændres eller ophæves.

4. Medlemsstaterne gør de nærmere oplysninger om eventuelle dataplaceringskrav, som er fastsat i en lov eller administrativ bestemmelse af generel karakter, og som er gældende på deres område, offentligt tilgængelige via et nationalt centralt onlineinformationssted, som de ajourfører, eller indgiver ajourførte oplysninger om sådanne dataplaceringskrav til et centralt informationssted, som er oprettet i henhold til en anden EU-retsakt.

5. Medlemsstaterne meddeler Kommissionen adressen på deres centrale onlineinformationssted som omhandlet i stk. 4. Kommissionen offentliggør linkene til disse informationssteder på sit websted sammen med en regelmæssigt ajourført konsolideret liste over alle dataplaceringskrav som omhandlet i stk. 4, herunder opsummerede oplysninger om disse krav.

Artikel 5

Kompetente myndigheders adgang til data

1. Denne forordning berører ikke de kompetente myndigheders beføjelser til at anmode om eller få adgang til data med henblik på udførelse af deres officielle opgaver i overensstemmelse med EU-retten eller national ret. De kompetente myndigheder kan ikke nægtes adgang til data med den begrundelse, at dataene behandles i en anden medlemsstat.

2. Hvis en kompetent myndighed efter at have anmodet om adgang til en brugers data ikke får adgang, og hvis der ikke findes nogen specifikke samarbejdsmekanismer i henhold til EU-retten eller internationale aftaler med henblik på udveksling af data mellem kompetente myndigheder i forskellige medlemsstater, kan den pågældende kompetente myndighed anmode om bistand fra en kompetent myndighed i en anden medlemsstat i overensstemmelse med proceduren fastlagt i artikel 7.

3. Hvis en anmodning om bistand indebærer, at den adspurgte myndighed skal have adgang til en fysisk eller juridisk persons lokaler, herunder til udstyr og midler til databehandling, skal en sådan adgang være i overensstemmelse med EU-retten eller national procesret.

4. Medlemsstaterne kan pålægge effektive, forholdsmæssige og afskrækkende sanktioner i overensstemmelse med EU-retten og national ret for manglende opfyldelse af en forpligtelse til at indberette data.

I tilfælde af misbrug af rettigheder fra en brugers side kan en medlemsstat, når det er berettiget på grund af et hastende behov for at få adgang til de pågældende data og under hensyntagen til de berørte parters interesser, pålægge den pågældende bruger strengt forholdsmæssige foreløbige foranstaltninger. Når foreløbige foranstaltninger kræver relokalisering af data i længere tid end 180 dage efter relokaliseringen, underrettes Kommissionen inden for dette tidsrum af 180 dage. Kommissionen foretager hurtigst muligt en kontrol af foranstaltningen og dens forenelighed med EU-retten og træffer, hvis det er relevant, de nødvendige foranstaltninger. Kommissionen udveksler oplysninger med medlemsstaternes centrale kontaktpunkter som omhandlet i artikel 7 om de erfaringer, der er opnået i den forbindelse.

Artikel 6

Dataportering

1. Kommissionen tilskynder til og fremmer udvikling af adfærdskodekser for selvregulering på EU-plan (»adfærdskodekser«) med henblik på at bidrage til en konkurrencedygtig dataøkonomi baseret på principperne om gennemsigtighed og interoperabilitet og under behørig hensyntagen til åbne standarder, herunder bl.a. følgende aspekter:

a) bedste praksis i forbindelse med tjenesteleverandørskift og dataportering i et struktureret, almindeligt anvendt og maskinlæsbart format, herunder åbne standardiserede formater, hvis det er nødvendigt, eller hvis den tjenesteleverandør, der modtager dataene, anmoder derom

b) minimumsoplysningskrav for at sikre, at professionelle brugere, inden der indgås kontrakt om databehandling, får tilstrækkeligt detaljerede, klare og gennemskuelige oplysninger om de procedurer, tekniske krav, tidsfrister og gebyrer, der gælder, når en professionel bruger vil skifte tjenesteleverandør eller føre data tilbage til sine egne IT-systemer

c) strategier med hensyn til certificeringsordninger, som gør det lettere at sammenligne databehandlingsprodukter og -tjenester til professionelle brugere under hensyntagen til fastsatte nationale eller internationale standarder, med henblik på at forbedre sammenligneligheden af disse produkter og tjenesteydelser. Sådanne strategier kan bl.a. omfatte kvalitetsstyring, forvaltning af informationssikkerhed, forvaltning af driftskontinuitet og miljøforvaltning

d) kommunikationskøreplaner med en tværfaglig tilgang for at skabe større bevidsthed om adfærdskodekserne blandt de relevante interessenter.

2. Kommissionen sikrer, at adfærdskodekserne udvikles i tæt samarbejde med alle relevante interessenter, herunder sammenslutninger af SMV'er og nystartede virksomheder, brugere og cloudtjenesteleverandører.

3. Kommissionen tilskynder tjenesteleverandørerne til at afslutte udarbejdelsen af adfærdskodekserne senest den 29. november 2019 og til at gennemføre dem i praksis senest den 29. maj 2020.

Artikel 7

Procedure for samarbejde mellem myndigheder

1. Hver medlemsstat udpeger et centralt kontaktpunkt, som skal varetage forbindelserne med de centrale kontaktpunkter i andre medlemsstater og Kommissionen, for så vidt angår anvendelsen af denne forordning. Medlemsstaterne underretter Kommissionen om de udpegede kontaktpunkter og om eventuelle senere ændringer af de meddelte oplysninger.

2. Når en kompetent myndighed i en medlemsstat ønsker bistand fra en anden medlemsstat i henhold til artikel 5, stk. 2, med henblik på at få adgang til data, indgiver den en behørigt begrundet anmodning til sidstnævntes centrale kontaktpunkt. Denne anmodning skal omfatte en skriftlig redegørelse for begrundelsen og retsgrundlaget for at søge adgang til dataene.

3. Det centrale kontaktpunkt identificerer den relevante kompetente myndighed i sin medlemsstat og sender den anmodning, der er modtaget i medfør af stk. 2, til den pågældende myndighed.

4. Den relevante kompetente myndighed skal uden unødigt ophold og inden for en tidsramme, som står i forhold til, hvor meget anmodningen haster, give et svar med de ønskede data eller underrette den anmodende kompetente myndighed om, at den ikke finder, at betingelserne for at anmode om bistand i henhold til denne forordning er opfyldt.

5. Alle oplysninger, der udveksles i forbindelse med bistand, som der anmodes om og ydes i henhold til artikel 5, stk. 2, må kun anvendes i forbindelse med den sag, hvortil der blev anmodet om oplysningerne.

6. De centrale kontaktpunkter giver brugerne generel information om denne forordning, herunder om adfærdskodekser.

Artikel 8

Evaluering og retningslinjer

1. Senest den 29. november 2022 forelægger Kommissionen Europa-Parlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg en rapport med en evaluering af gennemførelsen af denne forordning, navnlig med hensyn til:

a) anvendelsen af denne forordning, navnlig anvendelsen heraf på datasæt bestående af både personoplysninger og andre data end personoplysninger, i lyset af udviklingen på markedet og den teknologiske udvikling, som kan udvide mulighederne for at fjerne anonymisering af data

b) medlemsstaternes gennemførelse af artikel 4, stk. 1, og navnlig undtagelsen vedrørende den offentlige sikkerhed og

c) udviklingen og den praktiske gennemførelse af adfærdskodekserne samt tjenesteleverandørernes formidling af oplysninger.

2. Medlemsstaterne forelægger Kommissionen de oplysninger, der er nødvendige for udarbejdelsen af den rapport, der er omhandlet i stk. 1.

3. Senest den 29. maj 2019 offentliggør Kommissionen retningslinjer om samspillet mellem denne forordning og forordning (EU) 2016/679 med hensyn til datasæt bestående af både personoplysninger og andre data end personoplysninger.

Artikel 9

Afsluttende bestemmelser

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

Denne forordning finder anvendelse seks måneder efter offentliggørelsen.

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

Udfærdiget i Strasbourg, den 14. november 2018.

På Europa-Parlamentets vegne	*På Rådets vegne*
A. TAJANI	K. EDTSTADLER
Formand	*Formand*