EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2018/1807

av 14. november 2018

om en ramme for fri flyt av andre opplysninger enn personopplysninger i Den europeiske union

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité([1]),

etter samråd med Regionkomiteen,

etter den ordinære regelverksprosedyren([2]) og

ut fra følgende betraktninger:

1) Digitaliseringen av økonomien går stadig raskere. Informasjons- og kommunikasjonsteknologi er ikke lenger en egen sektor, men utgjør grunnlaget for alle moderne nyskapende økonomisystemer og samfunn. Elektroniske data er kjernen i disse systemene og kan skape stor verdi når de analyseres eller kombineres med tjenester og produkter. Samtidig reiser den raske utviklingen av dataøkonomien og nye teknologier, som for eksempel kunstig intelligens, produkter og tjenester knyttet til tingenes internett, autonome systemer og 5G nye juridiske spørsmål rundt tilgang til og viderebruk av data, ansvar, etikk og solidaritet. Det bør vurderes å igangsette arbeid rundt ansvarsforhold, særlig ved gjennomføring av atferdsregler for egenregulering og andre former for beste praksis. Dette arbeidet bør ta hensyn til anbefalinger, beslutninger og tiltak som iverksettes uten menneskelig medvirkning gjennom hele databehandlingsverdikjeden. Dette arbeidet kan også omfatte egnede ordninger for fastsettelse av ansvar, for overføring av ansvar mellom samarbeidende tjenester, for forsikring og for revisjon.

2) Dataverdikjeder bygger på forskjellige dataaktiviteter: oppretting og innsamling av data, aggregering og organisering av data, databehandling, dataanalyse, markedsføring og distribusjon av data, bruk og viderebruk av data. En formålstjenlig og effektiv databehandling er en grunnleggende byggestein i alle dataverdikjeder. Den formålstjenlige og effektive databehandlingen, samt utviklingen av dataøkonomien i Unionen, hemmes imidlertid særlig av to typer hindringer for datamobilitet og for det indre marked: datalokaliseringskrav som er fastsatt av medlemsstatenes myndigheter, samt mekanismer for innlåsing til leverandører i privat sektor.

3) Etableringsadgangen og adgangen til å yte tjenester i henhold til traktaten om Den europeiske unions virkemåte («TEUV») gjelder også for databehandlingstjenester. Imidlertid hemmes, og i noen tilfeller hindres, leveringen av disse tjenestene av visse nasjonale, regionale eller lokale krav om å lokalisere data innenfor et bestemt territorium.

4) Slike hindringer for den frie utvekslingen av databehandlingstjenester og for tjenesteyteres etableringsrett stammer fra kravene i medlemsstatenes lovgivning om at databehandling må skje innenfor et bestemt geografisk område eller territorium. Andre regler eller annen forvaltningspraksis har en tilsvarende virkning ved at de innfører særlige krav som gjør det vanskeligere å behandle data utenfor et bestemt geografisk område eller territorium i Unionen, som for eksempel krav om bruk av tekniske anlegg som er sertifisert eller godkjent i en bestemt medlemsstat. Rettslig usikkerhet når det gjelder omfanget av berettigede og uberettigede datalokaliseringskrav begrenser markedsaktørenes og den offentlige sektorens valgmuligheter ytterligere med hensyn til hvor data kan behandles. Denne forordningen begrenser ikke på noen måte virksomhetenes adgang til å inngå avtaler som angir hvor dataene skal lokaliseres. Denne forordning har bare til hensikt å verne denne friheten ved å sikre at et avtalt sted kan ligge hvor som helst i Unionen.

([1]) EUT C 227 av 28.6 2018, s. 78.

([2]) Europaparlamentets holdning av 4. oktober 2018 (ennå ikke offentliggjort i EUT) og Rådets beslutning av 6. november 2018.

5) Samtidig hemmes også datamobiliteten i Unionen av private restriksjoner: rettslige, avtalemessige og tekniske hindringer som gjør det vanskelig eller umulig for brukerne av databehandlingstjenester å overføre sine data fra en tjenesteyter til en annen, eller tilbake til sine egne informasjonsteknologi (IT)-systemer, ikke minst ved oppsigelse av avtaler med tjenesteytere.

6) Kombinasjonen av disse hindringene har ført til manglende konkurranse mellom skytjenesteleverandører i Unionen, forskjellige problemer med innlåsing til leverandører og en alvorlig mangel på datamobilitet. På samme måte har regelverk og retningslinjer for datalokalisering undergravd muligheten for foretak innenfor forskning og utvikling til å fremme samarbeid mellom virksomheter, universiteter og andre forskningsinstitusjoner med sikte på å fremme innovasjon.

7) Av hensyn til rettssikkerheten og behovet for like konkurransevilkår i Unionen er et felles sett av regler for alle markedsdeltakere et viktig element for at det indre marked skal fungere på en tilfredsstillende måte. For å fjerne handelshindringer og den konkurransevridningen som følger av ulikheter i nasjonal rett, og for å hindre at det oppstår nye handelshindringer og betydelige konkurransevridninger, er det nødvendig å vedta ensartede regler som kommer til anvendelse i alle medlemsstater.

8) Den rettslig rammen for vern av fysiske personer i forbindelse med behandling av personopplysninger og for respekten for privatlivet og vern av personopplysninger i elektronisk kommunikasjon, særlig europaparlaments- og rådsforordning (EU) 2016/679([1]) og europaparlaments- og rådsdirektiv (EU) 2016/680([2]) og 2002/58/EF([3]), berøres ikke av denne forordning.

9) Det voksende tingenes internett, kunstig intelligens og maskinlæring er viktige kilder til andre opplysninger enn personopplysninger, for eksempel som følge av at de benyttes i automatiserte industriproduksjonsprosesser. Konkrete eksempler på andre opplysninger enn personopplysninger omfatter aggregerte og anonymiserte datasett som brukes til analyser av stordata, data om presisjonslandbruk som kan bidra til overvåking og optimalisering av bruken av pesticider og vann, eller opplysninger om industrimaskiners vedlikeholdsbehov. Dersom den teknologiske utviklingen gjør det mulig å konvertere anonymiserte data til personopplysninger, skal slike data behandles som personopplysninger, og forordning (EU) 2016/679 får i så fall anvendelse.

10) I henhold til forordning (EU) 2016/679 kan medlemsstatene verken begrense eller forby den frie utvekslingen av personopplysninger i Unionen begrunnet i vern av fysiske personer i forbindelse med behandling av personopplysninger. Denne forordning fastsetter det samme prinsippet om fri utveksling i Unionen for andre opplysninger enn personopplysninger, unntatt når en begrensning eller et forbud er begrunnet av hensyn til offentlige sikkerhet. Forordning (EU) 2016/679 og denne forordning danner et sammenhengende sett av regler som tar hensyn til fri utveksling av forskjellige typer data. Denne forordning pålegger ikke en plikt til å lagre forskjellige typer data hver for seg.

11) For å skape en ramme for fri flyt av andre opplysninger enn personopplysninger i Unionen og legge grunnlaget for å videreutvikle dataøkonomien og styrke konkurranseevnen til industrien i Unionen, er det nødvendig å fastsette en tydelig, omfattende og forutsigbar rettslig ramme for behandling av andre opplysninger enn personopplysninger i det indre marked. En prinsippbaserte metode som gir mulighet for samarbeid mellom medlemsstatene, samt egenregulering, bør sikre at rammen er fleksibel nok til å ta hensyn til utviklingen i behovene til brukere, tjenesteytere og nasjonale myndigheter i Unionen. For å unngå risikoen for overlapping med eksisterende ordninger, og dermed unngå større byrder for både medlemsstater og foretak, bør det ikke fastsettes nærmere tekniske forskrifter.

12) Denne forordning bør ikke påvirke databehandling i den grad den utføres som en del av en aktivitet som ikke omfattes av unionsretten. Særlig bør det minnes om at i henhold til artikkel 4 i traktaten om Den europeiske union («TEU») er nasjonal sikkerhet hver enkelt medlemsstats eget ansvar.

([1]) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

([2]) Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, om fri utveksling av slike opplysninger og om oppheving av Rådets rammebeslutning 2008/977/JIS (EUT L 119 av 4.5.2016, s. 89).

([3]) Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon) (EFT L 201 av 31.7.2002, s. 37).

13) Fri flyt av data i Unionen vil spille en viktig rolle for å oppnå datadrevet vekst og innovasjon. I likhet med foretak og forbrukere vil også medlemsstatenes offentlige myndigheter og offentligrettslige organer kunne tjene på økt valgfrihet med hensyn til leverandører av datadrevne tjenester, av mer konkurransedyktige priser og av en mer effektiv måte å levere tjenester til borgerne på. På grunn av de store mengdene data som offentlige myndigheter og offentligrettslige organer håndterer, er det ytterst viktig at de går foran med et godt eksempel, for eksempel ved at de tar i bruk databehandlingstjenester, og at de avstår fra å legge begrensninger på datalokalisering når de gjør bruk av databehandlingstjenester. Offentlige myndigheter og offentligrettslige organer bør derfor omfattes av denne forordning. I denne forbindelse bør prinsippet om fri flyt av andre opplysninger enn personopplysninger, som er fastsatt i denne forordning, også få anvendelse på forvaltningspraksis og på datalokaliseringskrav innenfor offentlige innkjøp, uten at det berører europaparlaments- og rådsdirektiv 2014/24/EU([1]).

14) På samme måte som for direktiv 2014/24/EU berører denne forordning ikke lover og forskrifter som gjelder den interne organiseringen av medlemsstatene, og som fordeler myndighet og ansvar for databehandling blant offentlige myndigheter og offentligrettslige organer uten kontraktsregulert godtgjøring til private parter. Forordningen berører heller ikke lover og forskrifter i medlemsstatene som omfatter gjennomføringen av slik myndighet og slikt ansvar. Samtidig som de offentlige myndighetene og de offentligrettslige organene oppmuntres til å vurdere økonomiske og andre fordeler ved utkontraktering til eksterne tjenesteytere, kan de ha rettmessige grunner til å velge egenforsyning av tjenester eller å bruke egne ressurser. Dermed er det ikke noe i denne forordning som pålegger medlemsstatene å konkurranseutsette eller benytte underleverandører til levering av tjenester som de ønsker å levere selv, eller å organisere på annen måte enn ved hjelp av offentlige kontrakter.

15) Denne forordning bør få anvendelse på fysiske eller juridiske personer som leverer databehandlingstjenester til brukere som er bosatt i eller har en virksomhet i Unionen, herunder de som leverer databehandlingstjenester i Unionen uten å ha en virksomhet i Unionen. Denne forordning bør derfor ikke få anvendelse på databehandlingstjenester som finner sted utenfor Unionen, og på datalokaliseringskrav knyttet til slike data.

16) Denne forordning fastsetter ikke regler for valg av gjeldende lovgiving på det handelsrettslige området, og den berører derfor ikke europaparlaments- og rådsforordning (EF) nr. 593/2008([2]). En avtale om tjenesteyting er i prinsippet underlagt lovgivningen i det landet der tjenesteyteren har sitt vanlige bosted, særlig dersom gjeldende lovgivning for avtalen ikke er blitt valgt i samsvar med nevnte forordning.

17) Denne forordning bør gjelde for databehandling i videste forstand. Dette omfatter bruken av alle typer IT-systemer, uansett om de finnes i brukerens lokaler eller er utkontraktert til en tjenesteyter. Den bør omfatte ulike nivåer av databehandling, fra datalagring (infrastruktur som en tjeneste [Infrastructure-as-a-Service – IaaS]) til behandling av data på plattformer (plattform som en tjeneste [Platform-as-a-Service – PaaS]) eller i applikasjoner (programvare som en tjeneste [Software-as-a-Service – SaaS]).

18) Datalokaliseringskrav innebærer en klar hindring for fri tilgang til databehandlingstjenester i hele Unionen og for det indre marked. Slike krav bør derfor forbys med mindre de er begrunnet ut fra hensynet til offentlig sikkerhet, som definert i unionsretten, særlig som definert i artikkel 52 i TEUV, og oppfyller forholdsmessighetsprinsippet som er nedfelt i artikkel 5 i TEU. Ettersom denne forordning fastsetter tiltak for å sikre tilgang til data for regulerings- og tilsynsformål, bør medlemsstatene bare kunne påberope seg hensynet til offentlig sikkerhet som begrunnelse for datalokaliseringskrav. Dette skal sikre prinsippet om fri flyt av andre opplysninger enn personopplysninger på tvers av landegrensene, en rask fjerning av eksisterende datalokaliseringskrav og gjøre det mulig, av driftsmessige hensyn, å behandle data på flere steder i Unionen.

19) Begrepet «offentlig sikkerhet», som definert i artikkel 52 i TEUV, og som fortolket av Domstolen, dekker både den interne og den eksterne sikkerheten i en medlemsstat, samt spørsmål om samfunnssikkerhet, særlig for å lette etterforskning, avsløring og rettslig forfølging av straffbare forhold. «Offentlig sikkerhet» forutsetter at det foreligger en reell og tilstrekkelig alvorlig trussel som påvirker en av de grunnleggende samfunnsinteressene, for eksempel en trussel mot institusjoners og grunnleggende offentlige tjenesters virkemåte og befolkningens overlevelse, samt risikoen for en alvorlig forstyrrelse av internasjonale relasjoner eller nasjoners fredelige sameksistens, eller en trussel mot militære interesser. I samsvar med forholdsmessighetsprinsippet bør datalokaliseringskrav som er begrunnet ut fra hensynet til offentlig sikkerhet, være egnet til å sikre at det fastsatte målet nås, og ikke gå lenger enn det som er nødvendig for å nå dette målet.

([1]) Europaparlaments- og rådsdirektiv 2014/24/EU av 26. februar 2014 om offentlige innkjøp og om oppheving av direktiv 2004/18/EF (EUT L 94 av 28.3.2014, s. 65).

([2]) Europaparlaments- og rådsforordning (EF) nr. 593/2008 av 17. juni 2008 om hvilken lovgivning som får anvendelse på avtaleforpliktelser (Roma I) (EUT L 177 av 4.7.2008, s. 6).

20) Medlemsstatene bør umiddelbart oversende Kommisjonen ethvert utkast til lovgivning som innfører et nytt datalokaliseringskrav eller foretar endringer i et eksisterende datalokaliseringskrav. Dette skal sikre en effektiv anvendelse av prinsippet om fri flyt av andre opplysninger enn personopplysninger på tvers av landegrensene, og hindre at det oppstår nye hindringer for et velfungerende indre marked. Utkastene til lovgivning bør oversendes og vurderes i samsvar med europaparlaments- og rådsforordning (EU) nr. 2015/1535([1]).

21) For å fjerne eventuelle eksisterende hindringer bør medlemsstatene dessuten, i en overgangsperiode på 24 måneder fra anvendelsesdatoen for denne forordning, foreta en gjennomgåelse av gjeldende lover eller forskrifter av allmenn art som fastsetter datalokaliseringskrav. Kommisjonen bør underrettes om alle slike datalokaliseringskrav som medlemsstatene anser å være i samsvar med denne forordning, sammen med en begrunnelse. Begrunnelsen bør gjøre det mulig for Kommisjonen å undersøke om eventuelle gjenstående datalokaliseringskrav er i samsvar med forordningen. Kommisjonen bør, når det er relevant, kunne framlegge merknader til den berørte medlemsstaten. Slike merknader kan omfatte en anbefaling om endring eller oppheving av et datalokaliseringskrav.

22) Plikten til å underrette Kommisjonen om eksisterende datalokaliseringskrav og utkast til lovgivning, som er fastsatt ved denne forordning, bør få anvendelse på regelverksbaserte datalokaliseringskrav og utkast til lovgivning av allmenn art, men ikke på beslutninger som er rettet mot en bestemt fysisk eller juridisk person.

23) Fysiske og juridiske personer, som for eksempel tjenesteytere og brukere av databehandlingstjenester, bør sikres innsyn i de datalokaliseringskravene i medlemsstatene som er fastsatt ved lov eller forskrift av allmenn art. Medlemsstatene bør derfor offentliggjøre informasjon om slike krav på et nasjonalt nettbasert felles informasjonssted, og regelmessig oppdatere denne informasjonen. Alternativt bør medlemsstatene legge fram oppdatert informasjon om slike krav på et sentralt informasjonssted som er opprettet i henhold til en annen unionsrettsakt. For å underrette fysiske og juridiske personer på behørig måte om datalokaliseringskrav i hele Unionen bør medlemsstatene underrette Kommisjonen om adressene til disse felles informasjonsstedene. Kommisjonen bør offentliggjøre denne informasjonen på sitt eget nettsted, sammen med en regelmessig oppdatert og konsolidert liste over alle datalokaliseringskrav som gjelder i medlemsstatene, herunder sammenfattende opplysninger om disse kravene.

24) Datalokaliseringskravene kan ofte tilbakeføres til manglende tillit til databehandling på tvers av landegrensene, basert på en antakelse om at dataene ikke vil være tilgjengelige for vedkommende myndigheter i medlemsstatene, for eksempel når de skal utføre inspeksjon og revisjon i forbindelse med kontroll eller tilsyn. Slik manglende tillit kan ikke overvinnes utelukkende ved å erklære avtalevilkårene som forhindrer vedkommende myndigheter å få lovlig tilgang til data når de utfører sine offisielle oppgaver, ugyldige. Denne forordning bør derfor klart fastslå at den ikke påvirker vedkommende myndigheters rett til å anmode om og få tilgang til data i samsvar med Unionsretten eller nasjonal rett, og at vedkommende myndigheter ikke kan nektes tilgang til data på grunnlag av at dataene behandles i en annen medlemsstat. Vedkommende myndigheter kan pålegge funksjonskrav for å støtte tilgangen til data, for eksempel kreve at systembeskrivelser skal oppbevares i den berørte medlemsstaten.

25) Fysiske eller juridiske personer som er underlagt plikt til å innberette data til vedkommende myndigheter, kan oppfylle slike forpliktelser ved å gi og garantere vedkommende myndigheter rask og effektiv elektronisk tilgang til dataene, uansett på hvilken medlemsstats territorium dataene behandles. Slik tilgang kan sikres gjennom konkrete vilkår i avtaler som inngås mellom den fysiske eller juridiske personen som er underlagt plikten til å gi tilgang, og tjenesteyteren.

26) Dersom en fysisk eller juridisk person som er underlagt plikt til å innberette data, ikke oppfyller denne plikten, bør vedkommende myndighet kunne søke bistand fra vedkommende myndigheter i andre medlemsstater. I slike tilfeller bør vedkommende myndigheter bruke spesifikke samarbeidsinstrumenter i unionsretten eller internasjonale avtaler, avhengig av sak i det aktuelle tilfellet, for eksempel innenfor henholdsvis politisamarbeid, strafferettslige eller sivilrettslige

([1]) Europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske forskrifter og regler for informasjonssamfunnstjenester (EUT L 241 av 17.9.2015, s. 1).

saker eller i administrative spørsmål, Rådets rammebeslutning 2006/960/JIS([1]), europaparlaments- og rådsdirektiv 2014/41/EU([2]), Europarådets konvensjon om datakriminalitet([3]), rådsforordning (EF) nr. 1206/2001([4]), rådsdirektiv 2006/112/EF([5]) og rådsforordning (EU) nr. 904/2010([6]). I mangel av slike spesifikke samarbeidsordninger bør vedkommende myndigheter samarbeide gjennom utpekte felles kontaktpunkter, med sikte på å gi tilgang til de ønskede dataene.

27) Dersom en anmodning om bistand innebærer at den anmodede myndighet skal skaffe seg tilgang til en fysisk eller juridisk persons lokaler, herunder databehandlingsutstyr og -midler, skal slik tilgang være i samsvar med unionsretten eller nasjonal prosessrett, herunder eventuelle krav om at det innhentes rettslig forhåndsgodkjenning.

28) Denne forordning bør ikke gjøre det mulig for brukerne å forsøke å unndra seg anvendelsen av nasjonal rett. Den bør derfor fastsette bestemmelser som gjør det mulig for medlemsstatene å pålegge sanksjoner som er virkningsfulle, står i forhold til overtredelsen og virker avskrekkende, mot brukere som hindrer vedkommende myndigheter i å få tilgang til de dataene som er nødvendige for å utføre vedkommende myndigheters offisielle oppgaver i henhold til unionsretten og nasjonal rett. I hastetilfeller bør medlemsstatene, når en bruker misbruker sin rett, kunne pålegge strengt forholdsmessige midlertidige tiltak. Ethvert midlertidig tiltak som krever relokalisering av data i mer enn 180 dager etter relokaliseringen, vil innebære et avvik fra prinsippet om fri utveksling av opplysninger i et vesentlig tidsrom, og bør derfor meddeles Kommisjonen med henblikk på undersøkelse av dets forenlighet med unionsretten.

29) Muligheten til å overføre data uten hindringer er et viktig element for å øke brukernes valgmuligheter og fremme effektiv konkurranse på markedene for databehandlingstjenester. De reelle eller formodede problemene med å overføre data på tvers av landegrensene svekker også forbrukernes tillit til tilbud over landegrensene, og dermed også deres tillit til det indre marked. Mens de enkelte forbrukere nyter godt av gjeldende unionsrett, legges det ikke til rette for bytte mellom tjenesteyterne for de brukerne som opptrer innenfor rammen av sin nærings- eller yrkesvirksomhet. Ensartede tekniske krav i hele Unionen, uansett om de handler om teknisk harmonisering, gjensidig anerkjennelse eller frivillig harmonisering, bidrar også til utviklingen av et konkurransedyktig indre marked for databehandlingstjenester.

30) For å dra full nytte av konkurransesituasjonen bør yrkesbrukere kunne foreta velbegrunnede valg og lett kunne sammenligne de enkelte elementene av ulike databehandlingstjenester som tilbys på det indre marked, også avtalevilkårene for overføring av data ved oppsigelse av en avtale. Detaljert informasjon om og driftskrav for overføring av data mellom databehandlingstjenester bør defineres av markedsaktørene gjennom egenregulering. Slik kan man holde tritt med innovasjonspotensialet i markedet og ta hensyn til erfaringen og sakkunnskapen til tjenesteytere og yrkesbrukere av databehandlingstjenester. Egenreguleringen bør oppmuntres, tilrettelegges og overvåkes av Kommisjonen gjennom Unionens atferdsregler, som kan omfatte standard avtalevilkår.

31) For at slike atferdsregler skal være effektive, og for å gjøre bytting av tjenesteytere og overføring av data enklere, bør reglene være omfattende og minst dekke de hovedaspektene som er viktige under prosessen for overføring av data. Eksempler på slike aspekter er: prosessene for, og lokaliseringen av, sikkerhetskopiering av data; tilgjengelige dataformater og datastøtte; påkrevd IT-konfigurasjon og minste båndbredde i nettet; påkrevd tid før overføringsprosessen kan settes i gang og hvor lenge data vil være tilgjengelige for overføring; samt garantier for tilgang til data dersom tjenesteyter går konkurs. Atferdsreglene bør også gjøre det klart at innlåsing ikke er en akseptabel forretningspraksis, de bør tilrettelegge for tillitsfremmende teknologier og de bør oppdateres regelmessig for å holde tritt med den teknologiske utviklingen. Kommisjonen bør sørge for at alle berørte parter, herunder sammenslutninger av små og mellomstore bedrifter (SMB) og nystartede foretak, brukere og skytjenesteleverandører rådspørres under hele prosessen. Kommisjonen bør evaluere utarbeidingen av slike atferdsregler, og hvor effektiv gjennomføringen av dem er.

([1]) Rådets rammebeslutning 2006/960/JIS av 18. desember 2006 om forenkling av utvekslingen av informasjon og etterretningsopplysninger mellom rettshåndhevende myndigheter i medlemsstatene i Den europeiske union (EUT L 386 av 29.12.2006, s. 89).

([2]) Europaparlaments- og rådsdirektiv 2014/41/EU av 3. april 2014 om den europeiske etterforskningsordren i straffesaker (EUT L 130 av 1.5.2014, s. 1).

([3]) Europarådets konvensjonen om datakriminalitet, CETS nr. 185.

([4]) Rådsforordning (EF) nr. 1206/2001 av 28. mai 2001 om samarbeid mellom medlemsstatenes domstoler om bevisopptak på det sivilrettslige eller handelsrettslige område (EFT L 174 av 27.6.2001, s. 1).

([5]) Rådsdirektiv 2006/112/EF av 28. november 2006 om det felles merverdiavgiftssystem (EUT L 347 av 11.12.2006, s. 1).

([6]) Rådsforordning (EU) nr. 904/2010 av 7. oktober 2010 om forvaltningssamarbeid og bedrageribekjempelse på området merverdiavgift (EUT L 268 av 12.10.2010, s. 1).

32) Dersom en vedkommende myndighet i en medlemsstat ber om bistand fra en annen medlemsstat for å få tilgang til data i henhold til denne forordning, bør den gjennom et utpekt felles kontaktpunkt framlegge en behørig begrunnet anmodning til sistnevnte medlemstats utpekte felles kontaktpunkt. Anmodningen bør omfatte en skriftlig forklaring av grunnene og det rettslige grunnlaget for å søke tilgang til dataene. Det felles kontaktpunktet utpekt av den medlemsstaten hvis bistand ønskes, bør legge til rette for overføringen av anmodningen til vedkommende myndighet i den anmodede medlemsstaten. For å sikre effektivt samarbeid bør den myndigheten som anmodningen er sendt til, uten unødig opphold gi bistand som svar på en gitt anmodning eller opplyse om problemer med å oppfylle en slik anmodning eller dens grunner til å avslå den.

33) Dersom tilliten til sikkerheten i databehandling på tvers av landegrensene styrkes, bør det kunne redusere markedsaktørenes og offentlig sektors tilbøyelighet til å bruke datalokalisering som erstatning for datasikkerhet. Det bør også forbedre rettssikkerheten for foretak med hensyn til om gjeldende sikkerhetskrav oppfylles når databehandlingsvirksomhet utkontrakteres til tjenesteytere, herunder tjenesteytere i andre medlemsstater.

34) Alle sikkerhetskrav knyttet til databehandling som benyttes på en berettiget og forholdsmessig måte på grunnlag av unionsretten eller nasjonal rett i samsvar med unionsretten i den medlemsstaten der de fysiske eller juridiske personene hvis data berøres, er bosatt eller etablert, bør fortsatt få anvendelse på behandlingen av disse dataene i en annen medlemsstat. Disse fysiske eller juridiske personene bør kunne oppfylle slike krav, enten selv eller gjennom kontraktsvilkår i avtaler med tjenesteytere.

35) Sikkerhetskrav som er fastsatt på nasjonalt plan, bør være nødvendige og stå i forhold til sikkerhetsrisiko ved databehandlingen innenfor virkeområdet for den delen av nasjonal rett der disse kravene er fastsatt.

36) Europaparlaments- og rådsdirektiv (EU) 2016/1148([1]) fastsetter rettslige tiltak for å forbedre det generelle informasjonssikkerhetsnivået i Unionen. Databehandlingstjenester utgjør en av de digitale tjenestene som omfattes av nevnte direktiv. I henhold til nevnte direktiv skal medlemsstatene sikre at leverandører av digitale tjenester treffer hensiktsmessige og forholdsmessige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer som de bruker. Slike tiltak bør garantere et sikkerhetsnivå som står i forhold til den risikoen som foreligger, og bør ta hensyn til sikkerheten i systemer og anlegg, hendelseshåndtering, håndtering av kontinuitet i virksomheten, overvåking, revisjon og testing, og at internasjonale standarder overholdes. Disse elementene skal angis nærmere av Kommisjonen i gjennomføringsrettsakter i henhold til nevnte direktiv.

37) Kommisjonen bør framlegge en rapport om gjennomføringen av denne forordning, særlig for å kunne beslutte om det er behov for endringer i lys av den teknologiske eller markedsmessige utviklingen. Rapporten bør særlig vurdere denne forordning, særlig dens anvendelse på datasett som består av både personopplysninger og andre opplysninger enn personopplysninger, samt gjennomføringen av unntaket med hensyn til offentlig sikkerhet. Før denne forordning får anvendelse, bør Kommisjonen også offentliggjøre retningslinjer om hvordan datasett som består av både personopplysninger og andre opplysninger enn personopplysninger, bør håndteres. Dette skal sikre at foretak, herunder SMB-er, bedre forstår samspillet mellom denne forordning og forordning (EU) 2016/679, og at begge forordningene overholdes.

38) Denne forordning er forenlig med de grunnleggende rettighetene og de prinsippene som er anerkjent særlig i Den europeiske unions pakt om grunnleggende rettigheter. Denne forordning bør derfor fortolkes og anvendes i samsvar med disse rettighetene og prinsippene, herunder retten til vern av personopplysninger, ytrings- og informasjonsfrihet og frihet til å drive næringsvirksomhet.

39) Ettersom målet for denne forordning, som er å sikre fri flyt av andre opplysninger enn personopplysninger i Unionen, ikke kan nås i tilstrekkelig grad av medlemsstatene, og derfor på grunn av tiltakets omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i TEU. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel går denne forordning ikke lenger enn det som er nødvendig for å nå dette målet.

([1]) Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (EUT L 194 av 19.7.2016, s. 1).

VEDTATT DENNE FORORDNING:

Artikkel 1

Formål

Denne forordning har som mål å sikre fri flyt av andre opplysninger enn personopplysninger i Unionen ved å fastsette regler for datalokaliseringskrav, vedkommende myndigheters tilgang til data og overføring av data for yrkesbrukere.

Artikkel 2

Virkeområde

1. Denne forordning får anvendelse på behandling av andre elektroniske data enn personopplysninger i Unionen, som

a) leveres som en tjeneste til brukere som er bosatt i eller har en virksomhet i Unionen, uansett om tjenesteyteren er etablert i Unionen eller ikke, eller

b) utføres av en fysisk eller juridisk person som er bosatt i eller har en virksomhet i Unionen, for eget behov.

2. Når det gjelder et datasett som består av både personopplysninger og andre opplysninger enn personopplysninger, får denne forordning anvendelse på den delen av datasettet som omfatter andre opplysninger enn personopplysninger. Dersom personopplysninger og andre opplysninger enn personopplysninger i et datasett er uløselig knyttet til hverandre, skal denne forordning ikke berøre anvendelsen av forordning (EU) 2016/679.

3. Denne forordning får ikke anvendelse på aktiviteter som ikke omfattes av unionsretten.

Denne forordning berører ikke lover og forskrifter som gjelder den interne organiseringen av medlemsstatene, og som fordeler myndighet og ansvar for databehandling blant offentlige myndigheter og offentligrettslige organer som definert i artikkel 2 nr. 1 punkt 4 i direktiv 2014/24/EU, uten kontraktsregulert godtgjøring til private parter, samt lover og forskrifter i medlemsstatene som omfatter gjennomføringen av slik myndighet og slikt ansvar.

Artikkel 3

Definisjoner

I denne forordning menes med

1) «data» andre opplysninger enn personopplysninger som definert i artikkel 4 nr. 1 i forordning (EU) 2016/679,

2) «behandling» enhver operasjon eller serie av operasjoner som gjøres med data eller datasett i elektronisk format, enten automatisert eller ikke, for eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,

3) «utkast til lovgivning» en tekst som utarbeides med sikte på at den skal vedtas som en lov eller forskrift av allmenn art, og denne teksten befinnes seg på det forberedende stadiet der det fortsatt er mulig å foreta vesentlige endringer,

4) «tjenesteyter» enhver fysisk eller juridisk person som leverer databehandlingstjenester,

5) «datalokaliseringskrav» alle forpliktelser, forbud, vilkår, begrensinger eller andre krav som er fastsatt i en medlemsstats lover eller forskrifter, eller som følger av allmenn og konsekvent forvaltningspraksis i en medlemsstat og i offentligrettslige organer, herunder på området offentlige innkjøp, uten at det berører direktiv 2014/24/EU, og som innebærer at databehandling skal finne sted på en bestemt medlemsstats territorium, eller hindrer at data behandles i en annen medlemsstat,

6) «vedkommende myndighet» en myndighet i en medlemsstat eller enhver annen enhet som i henhold til nasjonal rett har myndighet til å utføre et offentlig verv eller utøve offentlig myndighet, som i forbindelse med utøvelsen av sitt offentlige verv har rett til å få tilgang til data som behandles av en fysisk eller juridisk person som fastsatt i unionsretten eller nasjonal rett,

7) «bruker» en fysisk eller juridisk person, herunder en offentlig myndighet eller et offentligrettslig organ, som benytter eller anmoder om en databehandlingstjeneste,

8) «yrkesbruker» en fysisk eller juridisk person, herunder en offentlig myndighet eller et offentligrettslig organ, som benytter eller anmoder om en databehandlingstjeneste i forbindelse med sin forretnings-, industri-, håndverks- eller yrkesvirksomhet eller sine oppgaver.

Artikkel 4

Fri utveksling av opplysninger i Unionen

1. Datalokaliseringskrav skal være forbudt, så fremt de ikke er begrunnet ut fra hensynet til offentlig sikkerhet i samsvar med forholdsmessighetsprinsippet.

Første ledd i dette nummer berører ikke nr. 3 og datalokaliseringskravene som er fastsatt på grunnlag av gjeldende unionsrett.

2. Medlemsstatene skal umiddelbart oversende Kommisjonen ethvert utkast til lovgivning som innfører et nytt datalokaliseringskrav eller foretar endringer i et eksisterende datalokaliseringskrav etter framgangsmåtene fastsatt i artikkel 5, 6 og 7 i direktiv (EU) 2015/1535.

3. Innen 30. mai 2021 skal medlemsstatene sikre at alle eksisterende datalokaliseringskrav som er fastsatt i en lov eller forskrift av allmenn art og som ikke er i samsvar med nr. 1 i denne artikkel, oppheves.

Innen 30. mai 2021 skal en medlemsstat som anser at et eksisterende tiltak som inneholder et datalokaliseringskrav, er i samsvar med nr. 1 i denne artikkel og derfor kan fortsette å gjelde, underrette Kommisjonen om dette tiltaket, sammen med en begrunnelse for at det skal fortsette å gjelde. Uten at det berører artikkel 258 i TEUV skal Kommisjonen, innen en frist på seks måneder fra datoen for mottak av underretningen, undersøke om dette tiltaket er i samsvar med nr. 1 i denne artikkel, og skal dersom det er relevant, framlegge merknader til den berørte medlemsstaten, herunder om nødvendig en anbefaling om endring eller oppheving av tiltaket.

4. Medlemsstatene skal gjøre nærmere opplysninger om eventuelle datalokaliseringskrav som er fastsatt i en lov eller forskrift av allmenn art og som gjelder på deres territorium, offentlig tilgjengelige gjennom et nasjonalt nettbasert felles informasjonssted som de skal holde oppdatert, eller legge fram oppdaterte opplysninger om slike lokaliseringskrav på et sentralt informasjonssted som er opprettet i henhold til en annen unionsrettsakt.

5. Medlemsstatene skal underrette Kommisjonen om adressen til deres felles informasjonssted som nevnt i nr. 4. Kommisjonen skal offentliggjøre lenkene til disse stedene på sitt nettsted, sammen med en regelmessig oppdatert konsolidert liste over alle datalokaliseringskrav nevnt i nr. 4, herunder sammenfattende opplysninger om disse kravene.

Artikkel 5

Vedkommende myndigheters tilgang til data

1. Denne forordning skal ikke påvirke vedkommende myndigheters rett til å anmode om eller få tilgang til data i forbindelse med utøvelsen av deres offentlige verv i samsvar med unionsretten eller nasjonal rett. Vedkommende myndigheter kan ikke nektes tilgang til data med den begrunnelse at dataene behandles i en annen medlemsstat.

2. Dersom vedkommende myndighet etter å ha anmodet om tilgang til en brukers data, ikke får tilgang, og dersom det ikke finnes noen spesifikke samarbeidsordninger i henhold til unionsretten eller internasjonale avtaler om utveksling av opplysninger mellom vedkommende myndigheter i forskjellige medlemsstater, skal vedkommende myndighet be om bistand fra en vedkommende myndighet i en annen medlemsstat etter framgangsmåten fastsatt i artikkel 7.

3. Dersom en anmodning om bistand innebærer at den anmodede myndigheten skal skaffe seg tilgang til en fysisk eller juridisk persons lokaler, herunder databehandlingsutstyr og -midler, skal slik tilgang være i samsvar med unionsretten eller nasjonal prosessrett.

4. Medlemsstatene kan innføre sanksjoner som er virkningsfulle, står i forhold til overtredelsen og virker avskrekkende, for manglende oppfyllelse av en forpliktelse til å framlegge opplysninger, i samsvar med unionsretten og nasjonal rett.

Dersom en bruker misbruker sine rettigheter, kan en medlemsstat dersom det er berettiget fordi det haster med tilgang til data og idet det tas hensyn til de berørte partenes interesser, vedta strengt forholdsmessige midlertidige tiltak mot denne brukeren. Dersom et midlertidig tiltak krever relokalisering av data i et tidsrom på over 180 dager etter relokaliseringen, skal Kommisjonen underrettes om dette innen den nevnte 180-dagersperioden. Kommisjonen skal så raskt som mulig undersøke tiltaket og dets forenlighet med unionsretten, og dersom det er relevant, treffe nødvendige tiltak. Kommisjonen skal utveksle opplysninger om erfaringene som er gjort i forbindelse med dette, med medlemsstatenes felles kontaktpunkter som nevnt i artikkel 7.

Artikkel 6

Overføring av data

1. Kommisjonen skal oppmuntre til og legge til rette for utarbeidingen av atferdsregler for egenregulering på unionsplan («atferdsregler») for å bidra til en konkurransedyktig dataøkonomi, basert på prinsippene om åpenhet og interoperabilitet, og idet det tas behørig hensyn til åpne standarder, som blant annet omfatter følgende aspekter:

a) Beste praksis for å forenkle bytting av tjenesteytere og overføring av data i et strukturert, allment benyttet og maskinleselig format, herunder åpne standardformater dersom den tjenesteyteren som mottar dataene, krever eller anmoder om det.

b) Minstekrav til informasjon for å sikre at yrkesbrukere, før det inngås en avtale om databehandling, får tilstrekkelig detaljert, klar og åpen informasjon om prosesser, tekniske krav, tidsfrister og kostnader som gjelder dersom en yrkesbruker ønsker å bytte til en annen tjenesteyter eller overføre data tilbake til sine egne IT-systemer.

c) Strategier med hensyn til sertifiseringsordninger som gjør det lettere å sammenligne databehandlingsprodukter og -tjenester for yrkesbrukere, samtidig som det tas hensyn til etablerte nasjonale eller internasjonale standarder, for å gjøre det lettere å sammenligne disse produktene og tjenestene. Slike strategier kan blant annet omfatte kvalitetsstyring, miljøstyring og håndtering av informasjonssikkerhet og driftskontinuitet.

d) Kommunikasjonskjøreplaner med en tverrfaglig tilnærming for å øke bevisstheten om atferdsregler blant de berørte partene.

2. Kommisjonen skal sikre at atferdsreglene utarbeides i nært samarbeid med alle berørte parter, herunder sammenslutninger av SMB-er og nystartede foretak, brukere og skytjenesteleverandører.

3. Kommisjonen skal oppmuntre tjenesteytere til å sluttføre utarbeidingen av atferdsregler innen 29. november 2019 og gjennomføre dem i praksis innen 29. mai 2020.

Artikkel 7

Framgangsmåte for samarbeid mellom myndigheter

1. Hver medlemsstat skal utpeke et felles kontaktpunkt som skal holde kontakt med de felles kontaktpunktene i andre medlemsstater og Kommisjonen med hensyn til anvendelsen av denne forordning. Medlemsstatene skal underrette Kommisjonen om de utpekte kontaktpunktene og om eventuelle endringer av dem.

2. Dersom en vedkommende myndighet i en medlemsstat ber om bistand fra en annen medlemsstat i henhold til artikkel 5 nr. 2, for å få tilgang til data, skal den avgi en behørig begrunnet anmodning til sistnevnte medlemsstats utpekte kontaktpunkt. Anmodningen skal inneholde en skriftlig forklaring av grunnene og det rettslige grunnlaget for å søke tilgang til dataene.

3. Det felles kontaktpunktet skal identifisere den berørte vedkommende myndigheten i sin medlemsstat og oversende den mottatte anmodningen i henhold til nr. 2 til denne vedkommende myndigheten.

4. Den berørte vedkommende myndigheten skal uten unødig opphold og innen en frist som står i forhold til hvor mye anmodningen haster, gi et svar med de opplysningene som ønskes, eller underrette anmodende vedkommende myndighet om at den ikke anser at vilkårene for å be om bistand i henhold til denne forordning, er oppfylt.

5. Alle opplysninger som utveksles i forbindelse med bistand som det anmodes om og som gis i henhold til artikkel 5 nr. 2, skal bare benyttes i forbindelse med den saken som ligger til grunn for anmodningen.

6. De felles kontaktpunktene skal gi brukerne generell informasjon om denne forordning, herunder atferdsreglene.

Artikkel 8

Vurdering og retningslinjer

1. Senest 29. november 2022 skal Kommisjonen framlegge for Europaparlamentet, Rådet og Den europeiske økonomiske og sosiale komité en rapport som vurderer gjennomføringen av denne forordning, særlig med hensyn til

a) anvendelsen av denne forordning, særlig av datasettene som består av både personopplysninger og andre opplysninger enn personopplysninger, på bakgrunn av markedsutviklingen og den teknologiske utviklingen som kan øke mulighetene for å avanonymisere data,

b) medlemsstatenes gjennomføring av artikkel 4 nr. 1, og særlig unntaket som gjelder offentlig sikkerhet, og

c) utarbeidingen og den effektive gjennomføringen av atferdsregler samt tjenesteyternes formidling av opplysninger.

2. Medlemsstatene skal framlegge for Kommisjonen de opplysningene som er nødvendige for utarbeiding av rapporten nevnt i nr. 1.

3. Senest 29. mai 2019 skal Kommisjonen offentliggjøre retningslinjer om samspillet mellom denne forordning og forordning (EU) 2016/679, særlig når det gjelder datasett som består av både personopplysninger og andre opplysninger enn personopplysninger.

Artikkel 9

Sluttbestemmelser

Denne forordning trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Denne forordning får anvendelse seks måneder etter at den er kunngjort.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Strasbourg 14. november 2018.

For Europaparlamentet	*For Rådet*
A. TAJANI	K. EDTSTADLER
President	*Formann*