EUROPA-
KOMMISSIONEN

Bruxelles, den 29.5.2019
COM(2019) 250 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Vejledning vedrørende forordningen om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union

Indhold

1 Indledning 2

Formålet med retningslinjerne 3

2 Samspillet mellem forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse — blandede datasæt 4

2.1 Begrebet "andre data end personoplysninger" i henhold til forordningen om fri udveksling af andre data end personoplysninger 4

Personoplysninger 5

Andre data end personoplysninger 6

2.2 Blandede datasæt 8

3 Fri udveksling af oplysninger og fjernelse af dataplaceringskrav 11

3.1 Fri udveksling af andre data end personoplysninger 12

3.2 Fri udveksling af personoplysninger 14

3.3 Anvendelsesområde for forordningen om fri udveksling af andre data end personoplysninger 15

3.4 Aktiviteter vedrørende medlemsstaternes interne organisation 16

4 Selvreguleringstilgange til støtte for den frie udveksling af oplysninger 18

4.1 Dataportering og skift mellem cloudtjenesteleverandører 18

Portabilitetsbegrebet og samspillet med den generelle forordning om databeskyttelse 19

4.2 Adfærdskodekser og certificeringsordninger for beskyttelse af personoplysninger 21

4.3 Styrket tillid til grænseoverskridende databehandling — sikkerhedscertificering 22

Afsluttende bemærkninger 23

Dette dokument stilles til rådighed af Kommissionen udelukkende til orientering. Det indeholder ikke en autoritativ fortolkning af 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 og udgør ikke en afgørelse eller udtalelse vedtaget af Kommissionen. Det berører hverken eventuelle afgørelser eller udtalelser vedtaget af Kommissionen eller Domstolens kompetence til at fortolke forordningen i overensstemmelse med EU-traktaterne.

1 Indledning

Vi befinder os i en tid, hvor økonomien i stadig højere grad styres af data, hvorfor fokus for virksomhedsprocesserne i virksomheder af enhver størrelse og inden for alle sektorer ligger på overførslen af oplysninger. Nye digitale teknologier skaber nye muligheder for den brede offentlighed, virksomheder og offentlige myndigheder i EU.

Europa-Parlamentet og Rådet vedtog i november 2018 forordning (EU) 2018/1807 om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union[1] ("forordning om fri udveksling af andre data end personoplysninger") på grundlag af et forslag fra Kommissionen. Formålet var at øge den grænseoverskridende udveksling af oplysninger og styrke dataøkonomien. Forordningen anvendes fra den 28. maj 2019. Princippet om fri udveksling af personoplysninger er allerede fastlagt i forordning (EU) 2016/679 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)[2]. Der findes således i dag en omfattende ramme for et fælles europæisk dataområde og fri udveksling af alle oplysninger inden for EU[3].

Forordningen om fri udveksling af andre data end personoplysninger skaber retssikkerhed for virksomhederne med hensyn til behandling af deres oplysninger på et hvilket som helst sted i EU, højner tilliden til databehandlingstjenesterne og modvirker leverandørfastlåsning. Herved øges forbrugernes valgfrihed, effektiviteten højnes, og indførelsen af cloudteknologier fremmes. Dette fører betydelige besparelser med sig for virksomheder i EU. Ifølge en undersøgelse kan virksomhederne i EU nedbringe deres IT-udgifter med 20-50 % ved at migrere data til skyen[4].

De to forordninger har betydet, at oplysninger i dag kan overføres frit mellem medlemsstaterne, hvilket gør det muligt for brugere af databehandlingstjenester at udnytte de oplysninger, der er indsamlet på forskellige EU-markeder, med henblik på at forbedre deres produktivitet og konkurrenceevne. Derfor vil brugerne kunne drage fuld nytte af de stordriftsfordele, som det store EU-marked fører med sig, idet deres globale konkurrenceevne styrkes, og sammenkoblingen af den europæiske dataøkonomi forbedres.

Forordningen om fri udveksling af andre data end personoplysninger omfatter tre nøgleelementer:

---

[1] 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).

[2] 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).

[3] Den generelle forordning om databeskyttelse finder også anvendelse på Det Europæiske Økonomiske Samarbejdsområde (EØS), som omfatter Island, Liechtenstein og Norge. Forordningen om fri udveksling af andre data end personoplysninger er endvidere mærket som EØS-relevant.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Foreligger online: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Medlemsstaterne må som udgangspunkt ikke pålægge krav, hvad angår oplysningernes placering. Undtagelser fra denne regel gives i henhold til proportionalitetsprincippet udelukkende af hensyn til den offentlige sikkerhed.
- Der oprettes en samarbejdsmekanisme til sikring af, at de kompetente myndigheder fortsat kan gøre deres rettigheder gældende, hvad angår adgangen til de oplysninger, der behandles i en anden medlemsstat.
- Der skabes incitamenter for industrien — med støtte fra Kommissionen — til at udarbejde adfærdskodekser for selvregulering i forbindelse med tjenesteleverandørskift og dataportering.

Formålet med retningslinjerne

Retningslinjerne er i overensstemmelse med artikel 8, stk. 3, i forordningen om fri udveksling af andre data end personoplysninger, i henhold til hvilken Kommissionen skal offentliggøre retningslinjer om samspillet mellem denne forordning og den generelle forordning om databeskyttelse "med hensyn til datasæt bestående af både personoplysninger og andre data end personoplysninger".

Retningslinjerne skal gøre det lettere for brugerne — især små og mellemstore virksomheder — at forstå samspillet mellem forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse[5]. De har derfor navnlig fokus på: i) begreberne andre data end personoplysninger og personoplysninger ii) principperne for fri udveksling af oplysninger og forbuddet mod datalokaliseringskrav i henhold til begge forordninger og iii) begrebet dataportabilitet i henhold til forordningen om fri udveksling af andre data end personoplysninger. Retningslinjerne vedrører derudover selvreguleringskravene som fastsat i begge forordninger.

Forordningen om fri udveksling af andre data end personoplysninger vedrører udelukkende "andre data end personoplysninger" som defineret i den generelle forordning om databeskyttelse. Den generelle forordning om databeskyttelse regulerer behandlingen af personoplysninger, som er en væsentlig del af EU's databeskyttelsesramme[6]. Forordningen

[5] Betragtning 37 i 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.

[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).
- 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).
- Direktiv (EU) 2016/680 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).
- 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

trådte i kraft i medlemsstaterne den 25. maj 2018. Forordningen indeholder harmoniserede bestemmelser til beskyttelse af personer i EU/EØS, hvad angår behandlingen af deres personoplysninger og den frie udveksling af disse oplysninger. Den generelle forordning om databeskyttelse: i) definerer personoplysninger ii) fastlægger retsgrundlaget for deres behandling og iii) fastsætter de rettigheder og forpligtelser, der gælder ved behandlingen af disse oplysninger[7] — for blot at nævne nogle få af forordningens bestemmelser. Med hensyn til princippet om fri udveksling af personoplysninger gælder følgende i henhold til artikel 1, stk. 3, i den generelle forordning om databeskyttelse: "Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger."

I den virkelige verden består datasæt som oftest både af personoplysninger og andre data end personoplysninger. Dette benævnes typisk "blandede datasæt". I afsnit 2.2 nedenfor uddybes samspillet mellem forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse med hensyn til blandede datasæt.

Af præciseringshensyn finder der ingen kontradiktoriske forpligtelser anvendelse i henhold til den generelle forordning om databeskyttelse og forordningen om fri udveksling af andre data end personoplysninger.

2 Samspillet mellem forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse — blandede datasæt

2.1 Begrebet "andre data end personoplysninger" i henhold til forordningen om fri udveksling af andre data end personoplysninger

Forordningen om fri udveksling af andre data end personoplysninger[8] har til formål at sikre den frie udveksling af andre data end personoplysninger. I forordningen henvises der gennem hele teksten til begrebet "data", som i henhold til artikel 4, stk. 1, i forordning (EU) 2016/679

om databeskyttelse inden for elektronisk kommunikation), (EFT L 201 af 31.7.2002, s. 37) (under revision).

[7] Se Det Europæiske Databeskyttelsesråds websted for yderligere retningslinjer vedrørende forskellige aspekter af 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) og den europæiske databeskyttelseslov, idet Rådet har udsendt en række retningslinjer i henhold til artikel 70 i den generelle forordning om databeskyttelse: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_da. Webstedet omfatter endvidere henvisninger til retningslinjer, anbefalinger og andre dokumenter som udsendt af forgængeren til Det Europæiske Databeskyttelsesråd (Artikel 29-Gruppen). Derudover har Kommissionen udsendt en meddelelse om databeskyttelse for at øge borgernes og virksomhedernes opmærksomhed på 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): vejledning om den direkte anvendelse af den generelle forordning om databeskyttelse (COM/2018/043 final): https://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

[8] Artikel 1 i 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.

(den generelle forordning om databeskyttelse) skal forstås som andre data end personoplysninger[9]. Disse data, som også i dette dokument angives som "**andre data end personoplysninger**", er det modsatte af personoplysninger i henhold til den generelle forordning om databeskyttelse.

Personoplysninger

I henhold til den generelle forordning om databeskyttelse er "personoplysninger" "enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede"); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet."

Den brede definition af personoplysninger er tilsigtet og er i det væsentlige forblevet uændret i den generelle forordning om databeskyttelse i forhold til den tidligere lovgivning[10]. Forskellige aspekter af definitionen af personoplysninger, såsom "enhver form for information", "om" eller "identificeret eller identificerbar", er allerede blevet behandlet af Artikel 29-Gruppen[11] i dens udtalelse 4/2007 om begrebet personoplysninger af 20. juni 2007, WP 136.

Inden for områder såsom forskning er det almindelig praksis at pseudonymisere personoplysninger for at skjule en persons identitet. Ved **pseudonymisering** behandles personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt person uden brug af supplerende oplysninger. Disse supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger (f.eks. kryptering)[12,13]. Ikke desto mindre anses pseudonymiserede oplysninger stadig som

---

[9] Se artikel 3, stk. 1, i 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.

[10] Se artikel 2, litra a), i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (udløber den 24 . maj 2018, ophævet ved den generelle forordning om databeskyttelse). Se endvidere Domstolens retspraksis vedrørende definitionen af personoplysninger, i henhold til hvilken der anerkendes en bred fortolkning af begrebet, eksempelvis Domstolens dom af 29. januar 2009, *Productores de Música de España (Promusicae)* mod *Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; Domstolens dom af 24. november 2011, *Scarlet Extended SA* mod *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; Domstolens dom af 19. oktober 2016, *Patrick Breyer* mod *Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[11] Artikel 29-Gruppen var et rådgivningsorgan, der rådgav Kommissionen om databeskyttelse og bidrog til udarbejdelsen af harmoniserede databeskyttelsespolitikker i EU. Efter ikrafttrædelsen af den generelle forordning om databeskyttelse den 25. maj 2018 blev Artikel 29-Gruppen erstattet af Det Europæiske Databeskyttelsesråd.

[12] Jf. artikel 4, stk. 5, i 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), som indeholder en definition af "pseudonymisering".

[13] Eksempelvis betragtes en undersøgelse af virkningerne af et nyt lægemiddel som en pseudonymisering, når personoplysningerne vedrørende deltagerne udskiftes med unikke attributter (f.eks. et tal eller en kode) i

oplysninger om en identificerbar person, hvis de kan henføres til denne person ved brug af supplerende oplysninger[14]. Disse data er i henhold til den generelle forordning om databeskyttelse **personoplysninger**.

Andre data end personoplysninger

Hvis dataene ikke er "personoplysninger" i henhold til den generelle forordning om databeskyttelse, er der tale om **andre data end personoplysninger**. Andre data end personoplysninger kan kategoriseres efter deres oprindelse:

- for det første som oplysninger, der oprindeligt ikke vedrørte en identificeret eller identificerbar fysisk person, herunder oplysninger om vejrforhold genereret af følere, der er installeret på vindmøller, eller oplysninger vedrørende industrielle maskiners vedligeholdelsesbehov

- for det andet som oplysninger, der oprindeligt var personoplysninger, men som senere blev **anonymiserede**[15]. "Anonymiseringen" af personoplysninger adskiller sig fra pseudonymiseringen (se ovenfor), da oplysninger, der er anonymiseret korrekt, ikke kan henføres til en bestemt person — selv med brug af supplerende oplysninger[16] — og er dermed andre data end personoplysninger.

Vurderingen af, hvorvidt oplysningerne er anonymiseret korrekt, afhænger af de specifikke og unikke forhold, der gør sig gældende for det enkelte tilfælde[17]. Der er fundet flere eksempler, hvor datasæt, der angiveligt blev anonymiseret, alligevel blev identificeret, hvorfor en sådan evaluering kan være udfordrende[18]. For at finde ud af, om en person er identificerbar, skal der

---

undersøgelsesdokumentationen, og deres personoplysninger opbevares separat sammen med de tildelte unikke attributter i et sikret dokument (f.eks. i en database, der er beskyttet med adgangskode).

[14] Se betragtning 26 i 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).

[15] Se betragtning 26 i 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), i henhold til hvilken: "Databeskyttelsesprincipperne bør derfor ikke gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres."

[16] Se Domstolens dom af 19. oktober 2016, sag *Patrick Breyer* mod *Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Ifølge Domstolens dom kan en dynamisk IP-adresse udgøre personoplysninger, selv når en tredjepart (f.eks. en internettjenesteleverandør) er i besiddelse af supplerende oplysninger, der ville gøre det muligt at identificere den pågældende person. Muligheden for at identificere personen skal gives i form af midler, der med rimelighed kan tænkes bragt i anvendelse til at identificere den pågældende — enten direkte eller indirekte.

[17] Dataanonymiseringen bør altid ske ved brug af de nyeste avancerede anonymiseringsteknikker.

[18] Der findes eksempler på, at angiveligt anonymiserede oplysninger alligevel blev identificeret, i undersøgelsen vedrørende fremtidige overførsler af oplysninger som udarbejdet for Europa-Parlamentets Udvalg om Industri, Forskning og Energi af Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee*, 2017, s. 22, tekstboks 2. Foreligger online: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

ses på alle de midler, en dataansvarlig eller anden person med rimelighed må antages at benytte sig af for at identificere en person direkte eller indirekte[19].

Eksempler på andre data end personoplysninger:

- Oplysninger, der aggregeres, således at det ikke længere er muligt at identificere individuelle hændelser (herunder en persons individuelle rejser til udlandet eller rejsemønstre, der ville kunne udgøre personoplysninger), kan betegnes som anonymiserede data[20]. De anonyme oplysninger bruges eksempelvis til statistiske formål eller i salgsrapporter (blandt andet for at vurdere et produkts popularitet og dets egenskaber).
- Oplysninger om højfrekvenshandel inden for finanssektoren eller oplysninger om præcisionsdyrkning, der bruges som hjælp ved overvågning og optimering af brugen af pesticider, næringsstoffer og vand.

Hvis de andre data, der ikke er personoplysninger, på nogen som helst måde alligevel kan sættes i forbindelse med en person, således at denne enten direkte eller indirekte bliver identificerbar, skal oplysningerne betragtes som personoplysninger.

Hvis en kvalitetskontrolrapport for en produktionslinje eksempelvis gør det muligt at sætte oplysningerne i forbindelse med de specifikke fabriksarbejdere (f.eks. de medarbejdere, der står for indstillingen af produktionsparametre), betragtes oplysningerne som personoplysninger. I dette tilfælde finder den generelle forordning om databeskyttelse anvendelse. Det samme gælder, hvis det grundet teknologiske og dataanalytiske udviklinger bliver muligt at konvertere anonymiserede oplysninger til personoplysninger. [21]

I definitionen af personoplysninger henvises der til "fysiske personer", og derfor udgør datasæt bestående af navne og kontaktoplysninger på juridiske personer i princippet andre data end personoplysninger.[22] I visse situationer kan der dog være tale om

[19] Se betragtning 26 i forordning (EU) 2016/679 (generel forordning om databeskyttelse): "For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning såsom de relaterede omkostninger og den tid, der skal afsættes til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling."

[20] Se Artikel 29-Gruppen: *Udtalelse nr. 05/2014 om anonymiseringsteknikker*, vedtaget den 10. april 2014, WP216, s. 9: "Det er kun, hvis den registeransvarlige, aggregerer dataene til et niveau, hvor de enkelte hændelser ikke længere kan identificeres, at det resulterende datasæt kan betegnes som anonymt. Eksempel: Hvis en organisation indsamler data om individuelle rejser, vil de individuelle rejsemønstre på hændelsesniveau stadig blive betegnet som personoplysninger for alle parter, så længe den dataansvarlige (eller enhver anden part) stadig har adgang til de originale oplysninger, selv om de direkte identifikatorer er blevet fjernet fra det datasæt, der er videregivet til tredjemand. Hvis den dataansvarlige derimod sletter de originale oplysninger og kun udleverer aggregeret statistik på et højt niveau til tredjemand, som f.eks. "om mandagen på rute X er der 160 % flere passagerer end om tirsdagen", vil dette blive betegnet som anonyme oplysninger."

[21] Bliver personoplysningerne behandlet på en ulovlig måde, eller denne behandling på anden vis udgør en overtrædelse af den generelle forordning om databeskyttelse, har de registrerede (fysiske personer) i henhold til den generelle forordning om databeskyttelse ret til at indgive en klage til en national tilsynsmyndighed (databeskyttelsesmyndighed) i EU eller adgang til effektive retsmidler for en national domstol. Kapitel VI, afsnit 2, i den generelle forordning om databeskyttelse regulerer de nationale tilsynsmyndigheders opgaver, kompetencer og beføjelser.

[22] Betragtning 14 i 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

personoplysninger[23]. Det er eksempelvis tilfældet, når navnet på den juridiske person svarer til den fysiske persons navn, når denne person er ejeren, eller oplysningerne vedrører en identificeret eller identificerbar fysisk person[24].

2.2 Blandede datasæt

Forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse har forskellige tilgange til den frie udveksling af oplysninger i EU.

I henhold til forordningen om fri udveksling af andre data end personoplysninger gælder der et generelt forbud mod dataplaceringskrav for andre data end personoplysninger. I henhold til artikel 4, stk. 1, i forordningen er dataplaceringskrav forbudt, medmindre de er begrundet i hensynet til den offentlige sikkerhed og i overensstemmelse med proportionalitetsprincippet.

Den generelle forordning om databeskyttelse sikrer — foruden en høj beskyttelsesgrad af personoplysninger — også den frie udveksling af personoplysninger. I henhold til forordningens artikel 1, stk. 3, må den frie udveksling af personoplysninger i EU "hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger". De to forordninger sikrer således den frie udveksling af "alle" oplysninger i EU. I afsnit 3.1 og 3.2 gennemgås de specifikke bestemmelser yderligere.

Et blandet datasæt består af både personoplysninger og andre data end personoplysninger. De blandede datasæt udgør størstedelen af de datasæt, der anvendes inden for dataøkonomien, og er ret almindelige, da de tekniske udviklinger såsom tingenes internet (dvs. genstande til digital forbindelse), kunstig intelligens og teknologier, der muliggør big data-analyser.

Eksempler på blandede datasæt:

- en virksomheds skatteopgørelse, hvoraf virksomhedsdirektørens navn og telefonnummer fremgår
- datasæt i en bank, navnlig indeholdende kundeoplysninger og transaktionsoplysninger, herunder betalingstjenester (kredit- og debetkort), applikationer til forvaltning af partnerrelationer samt låneaftaler, dokumenter med blandede oplysninger om fysiske og juridiske personer

---

sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse): "Denne forordning finder ikke anvendelse på behandling af personoplysninger, der vedrører juridiske personer, navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger." I den forbindelse skal definitionen af personoplysninger i artikel 4, stk. 1, i den generelle forordning om databeskyttelse tages i betragtning.

[23] Se Domstolens dom af 9. november 2010 i de forenede sager *Volker und Markus Schecke GbR*, C-92/09 og *Hartmut Eifert*, C-93/09 mod *Land Hessen*, ECLI:EU:C:2010:662, præmis 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_da

- et forskningsinstituts anonymiserede statistiske data og de originale data, der oprindeligt blev indsamlet, herunder besvarelser fra individuelle respondenter på spørgsmål i statistiske rundspørger
- en virksomheds videndatabase over IT-problemer og løsninger heraf baseret på individuelle IT-hændelsesrapporter
- data forbundet med tingenes internet, når der ud fra nogle af disse data kan gøres antagelser vedrørende identificerbare personer (f.eks. tilstedeværelse på en specifik adresse og brugsmønstre) samt
- analyser af driftslogdata vedrørende produktionsudstyr inden for produktionsindustrien.

Eksempel: tjenester til forvaltning af kunderelationer

Nogle banker benytter sig af tjenester til forvaltning af kunderelationer (customer relationship management, CRM), der udbydes af tredjeparter. Kundeoplysningerne skal i den forbindelse offentliggøres i CRM-miljøet. De oplysninger, der registreres i CRM-tjenesten, omfatter alle de oplysninger, der kræves for effektivt at kunne forvalte interaktionen med kunden, herunder deres post- og e-mailadresse, deres telefonnummer, de varer og tjenesteydelser, de køber, samt salgsrapporter, herunder aggregerede data. Disse data kan derfor både omfatte personoplysninger og andre data end personoplysninger.

I forordningen om fri udveksling af andre data end personoplysninger[25] lyder det i forbindelse med blandede datasæt:

"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."

I tilfælde af et datasæt bestående af både personoplysninger og andre data end personoplysninger betyder det, at:

- forordningen om fri udveksling af andre data end personoplysninger finder anvendelse på den del af sættet, der omfatter andre data end personoplysninger
- bestemmelsen om fri udveksling i den generelle forordning om databeskyttelse[26] finder anvendelse på den del af sættet, der omfatter personoplysninger, samt
- hvis den del, der omfatter andre data end personoplysninger, og de dele, der omfatter personoplysninger, "er knyttet uløseligt sammen", finder databeskyttelsesrettighederne og

[25] Artikel 2, stk. 2.

[26] Artikel 1, stk. 3, i 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). Se også afsnit 3.2 heri.

-forpligtelserne i henhold til den generelle forordning om databeskyttelse fuld anvendelse på det samlede blandede datasæt — dette gælder også, selv om personoplysningerne kun udgør en lille del af datasættet[27].

Fortolkningen er i overensstemmelse med retten til beskyttelse af personoplysninger i henhold til Den Europæiske Unions charter om grundlæggende rettigheder[28] og betragtning 8 i forordningen om fri udveksling af andre data end personoplysninger[29]. I henhold til betragtning 8 heri gælder følgende: "De retlige rammer for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger ..., navnlig [den generelle forordning om databeskyttelse] samt Europa-Parlamentets og Rådets direktiv (EU) 2016/680 og 2002/58/EF berøres ikke af nærværende forordning."

Et praktisk eksempel:

En virksomhed med aktiviteter i EU tilbyder sine tjenester via en platform. Virksomheder (kunder) uploader deres dokumenter indeholdende blandede datasæt til platformen. Som dataansvarlig skal den virksomhed, der uploader dokumenterne, sikre, at behandlingen er i overensstemmelse med den generelle forordning om databeskyttelse. Ved at behandle datasættet på vegne af den dataansvarlige skal den virksomhed, der tilbyder tjenesterne (databehandleren), gemme eller behandle oplysningerne i overensstemmelse med den generelle forordning om databeskyttelse, eksempelvis for at sikre et passende sikkerhedsniveau for oplysningerne, herunder gennem kryptering.

Ordlyden "knyttet uløseligt sammen" defineres ikke i nogen af de to forordninger[30]. Af praktiske hensyn kan dette henvise til en situation, hvor et datasæt omfatter personoplysninger og andre data end personoplysninger, men en adskillelse heraf ville være umulig eller af den dataansvarlige anses som økonomisk ineffektiv eller teknisk umulig. Når virksomheden eksempelvis køber CRM- og salgsrapportsystemer, vil den skulle fordoble sine udgifter til software, idet den skal købe separat software til CRM- (personoplysninger) og salgsrapportsystemerne (aggregerede data/andre data end personoplysninger) baseret på CRM-dataene.

En adskillelse af datasættet ville også muligvis medføre en betydelig nedgang i datasættets værdi. Derudover betyder dataenes ændrede form (se afsnit 2.1), at det bliver mere besværligt at skelne klart mellem og således adskille de forskellige datakategorier.

---

27 Som påpeget i arbejdsdokument fra *Kommissionens tjenestegrene, konsekvensanalysen, som ledsager dokumentet Forslag til Europa-Parlamentets og Rådets forordning om en ramme for fri udveksling af andre data end personoplysninger i Den Europæiske Union* (SWD(2017) 304 final), del 1/2, s. 3, skal GDPR (den generelle forordning om databeskyttelse) overholdes fuldt ud, hvad angår den del af datasættet, der omfatter personoplysninger — uanset hvor mange personoplysninger, der er indeholdt i de blandede datasæt.

28 Den Europæiske Unions charter om grundlæggende rettigheder (EUT C 362 af 26.10.2012, s. 391).

29 Betragtning 8 heri.

30 Forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse.

Der er væsentligt, at ingen af de to forordninger forpligter virksomheder til at adskille de datasæt, de er ansvarlige for eller behandler.

Et blandet datasæt er således generelt underlagt forpligtelser fra de dataansvarliges og databehandlernes side og skal respektere de registreredes rettigheder i henhold til den generelle forordning om databeskyttelse.

Behandling af helbredsoplysninger

Der kan indgå helbredsoplysninger i et blandet datasæt. Eksempler herpå er elektroniske helbredsjournaler, kliniske forsøg eller sæt bestående af data som indsamlet af diverse mobilapplikationer på sundheds- og velværeområdet (herunder applikationer til måling af vores sundhedstilstand for at minde os om at tage vores medicin eller registrere vores fysiske fremskridt)[31]. I takt med de teknologiske udviklinger bliver det stadig vanskeligere at adskille personoplysninger fra andre data end personoplysninger i disse datasæt. Behandlingen heraf skal således være i overensstemmelse med den generelle forordning om databeskyttelse, navnlig (set i lyset af at helbredsoplysninger i henhold til forordningen udgør en særlig kategori af data) artikel 9, i henhold til hvilken der gælder et generelt forbud mod at behandle særlige kategorier af data og undtagelser fra dette forbud.

Oplysningerne i de blandede datasæt, der omfatter helbredsoplysninger, kan være en værdifuld informationskilde, f.eks. i forbindelse med yderligere medicinsk forskning, til måling af bivirkningerne af receptpligtig medicin, til sygdomsrelaterede statistiske formål eller til udvikling af nye sundhedsplejetjenester eller behandlinger. Den generelle forordning om databeskyttelse skal dog overholdes ved udførelsen af oprindelig og yderligere databehandling. Derfor skal denne behandling af helbredsoplysninger være baseret på et gyldigt retsgrundlag[32] og en passende dokumentation, være sikker og tilvejebringe tilstrækkelige garantier.

Endelig skal databehandlingen være forbundet med retssikkerhed og tillid for personer og virksomheder. Dette er også helt afgørende for dataøkonomien. Dette sikres med de to forordninger, som begge har til formål ikke at ændre ved den frie udveksling af oplysninger.

3 Fri udveksling af oplysninger og fjernelse af dataplaceringskrav

I dette afsnit forklares begrebet dataplaceringskrav i henhold til forordningen om fri udveksling af andre data end personoplysninger og princippet om fri udveksling i den generelle forordning om databeskyttelse mere specifikt. På trods af at disse bestemmelser er

[31] Ved udvikling og drift af mobilapplikationer på sundhedsområdet skal bestemmelserne i den generelle forordning om databeskyttelse strengt overholdes. Disse krav specificeres yderligere i den adfærdskodeks for databeskyttelse i forbindelse med mobilapplikationer på sundhedsområdet, der er under udarbejdelse. Der findes yderligere oplysninger om status for udarbejdelsen heraf på: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Se artikel 6, stk. 1, i 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).

målrettet medlemsstaterne, kan de give virksomhederne en bedre forståelse af, hvordan de to forordninger bidrager til den frie udveksling af alle oplysninger i EU.

3.1 Fri udveksling af andre data end personoplysninger

I henhold til forordningen om fri udveksling af andre data end personoplysninger[33] er dataplaceringskrav "forbudt, medmindre de er begrundet i hensynet til den offentlige sikkerhed og i overensstemmelse med proportionalitetsprincippet."

Dataplaceringskrav defineres[34] som "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[35]."

Definitionen illustrerer, at der findes forskellige former for foranstaltninger, der begrænser den frie udveksling af oplysninger i EU. Disse kan være fastlagt i lovgivning, administrative regulativer og bestemmelser eller bygge på almen og fast administrativ praksis. Forbuddet mod dataplaceringskrav gælder desuden både for direkte og indirekte foranstaltninger, der begrænser den frie udveksling af andre data end personoplysninger.

Direkte dataplaceringskrav kan eksempelvis omfatte en forpligtelse til at gemme oplysninger et bestemt geografisk sted (f.eks. skal servere befinde sig i en specifik medlemsstat) eller en forpligtelse til at opfylde unikke nationale tekniske krav (f.eks. skal oplysningerne have specifikke nationale formater).

Indirekte dataplaceringskrav, der forhindrer behandlingen af andre data end personoplysninger i en anden medlemsstat, kan have forskellige former. Disse omfatter eventuelt krav om brug af teknologiske faciliteter, der er certificeret eller godkendt i en bestemt medlemsstat, eller andre krav, der har den virkning, at det bliver sværere at behandle oplysninger uden for et specifikt geografisk område eller territorium i EU[36,37].

---

33 Artikel 4, stk. 1.

34 Artikel 3, stk. 5, i 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.

35 Bemærk, at manglende retssikkerhed med hensyn til omfanget af berettigede og uberettigede dataplaceringskrav begrænser markedsdeltagernes og den offentlige sektors valgmuligheder med hensyn til, hvor data behandles, yderligere (se betragtning 4 i 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).

36 Betragtning 4 i 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.

37 Se to undersøgelser om dataplaceringskrav, der blev gennemført inden vedtagelsen af forordningen om fri udveksling af andre data end personoplysninger: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, SMART-nummer 2015/2016. Foreligger online: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 og 2) Time.lex, Spark Legal Network og Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*. SMART-nummer 2015/0054. Foreligger online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

Ved vurderingen af, hvorvidt en bestemt foranstaltning udgør et indirekte dataplaceringskrav, skal der tages højde for det særlige forhold, der gør sig gældende for det specifikke tilfælde.

I forordningen om fri udveksling af andre data end personoplysninger[38] henvises der til begrebet **offentlig sikkerhed** som anført i Domstolens retspraksis. Offentlig sikkerhed "omfatter både den interne og eksterne sikkerhed i en medlemsstat[39] 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[40] 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."

Derudover skal alle dataplaceringskrav, der begrundes i den offentlige sikkerhed, være i overensstemmelse med proportionalitetsprincippet, i henhold til hvilket de vedtagne foranstaltninger i overensstemmelse med Domstolens retspraksis kan sikre, at det forfulgte mål bliver opfyldt og ikke går videre, end hvad der kræves i forhold til formålet[41].

Af præciseringshensyn berører forbuddet mod dataplaceringskrav ikke de eksisterende begrænsninger som fastsat i EU-lovgivningen[42].

Forordningen om fri udveksling af andre data end personoplysninger pålægger endvidere ikke virksomhederne forpligtelser, og den begrænser heller ikke deres kontraktfrihed vedrørende beslutningen om, hvor deres oplysninger skal behandles.

Medlemsstaterne skal gøre de nærmere oplysninger om eventuelle dataplaceringskrav, som er gældende på deres område, offentligt tilgængelige via et **nationalt centralt onlineinformationssted** (nationale websteder). De skal ajourføre dette eller indgive ajourførte oplysninger om sådanne dataplaceringskrav til et centralt informationssted, som er

---

38 Betragtning 19 heri.

39 Se eksempelvis Domstolens dom af 23. november 2010, *Land Baden-Württemberg* mod *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, præmis 43, og dommen af 4. april 2017, *Sahar Fahimian* mod *Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, præmis 39.

40 Se eksempelvis Domstolens dom af 22. december 2008, *Kommissionen for De Europæiske Fællesskaber* mod *Republikken Østrig*, C-161/07, ECLI:EU:C:2008:759, præmis 35, og den retspraksis, der er anført heri, og dommen af 26. marts 2009, *Kommissionen for De Europæiske Fællesskaber* mod *Den Italienske Republik*, C-326/07, ECLI:EC:C:2009:193, præmis 70, og den retspraksis, der er anført heri.

41 Se eksempelvis Domstolens dom af 8. juli 2010, *Afton Chemical Limited* mod *Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, præmis 45, og den retspraksis, der er anført heri.

42 Se eksempelvis artikel 245, stk. 2, i direktiv 2006/112/EF af 28. november 2006 om det fælles merværdiafgiftssystem, i henhold til hvilket "medlemsstaterne kan bestemme, at afgiftspligtige personer, der er etableret på deres område, skal meddele dem opbevaringsstedet, når det ligger uden for deres område". Dette krav skal dog forstås i henhold til artikel 249, som fastslår at: "Når en afgiftspligtig person opbevarer udstedte eller modtagne fakturaer elektronisk, således at der sikres onlineadgang til dataene, og opbevaringsstedet er beliggende i en anden medlemsstat end den, hvor vedkommende er etableret, har de kompetente myndigheder i den afgiftspligtige persons etableringsmedlemsstat ved anvendelsen af dette direktiv ret til elektronisk adgang til, downloading og anvendelse af disse fakturaer inden for de grænser, der er fastsat i etableringsmedlemsstatens forskrifter, og i det omfang de kompetente myndigheder finder det nødvendigt af kontrolhensyn."

oprettet i henhold til en anden EU-retsakt.[43] Som hjælp for virksomhederne og for at sikre nem adgang til relevante oplysninger i hele EU offentliggør Kommissionen links til disse informationssteder på Dit Europa-portalen[44].

3.2 Fri udveksling af personoplysninger

I den generelle forordning om databeskyttelse[45] er følgende fastsat: "Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger."

Hvis en medlemsstat pålægger placeringskrav i forbindelse med personoplysninger, medmindre det begrundes i beskyttelse af personoplysninger, skal disse vurderes i overensstemmelse med bestemmelserne om grundlæggende frihedsrettigheder og de tilladte fravigelser fra disse friheder i henhold til traktaten om Den Europæiske Unions funktionsmåde[46,47] og relevant EU-lovgivning, herunder tjenesteydelsesdirektivet[48] og direktivet om elektronisk handel[49].

Eksempel:

I henhold til en national lov skal lønkonti af reguleringshensyn — f.eks. for den nationale skattemyndighed — være placeret i en bestemt medlemsstat. En sådan national bestemmelse falder uden for artikel 1, stk. 3, i den generelle forordning om databeskyttelse, da dette begrundes i andet end beskyttelsen af personoplysninger. Dette krav skal i stedet vurderes i overensstemmelse med bestemmelserne om grundlæggende frihedsrettigheder og de tilladte fravigelser fra disse friheder i henhold til traktaten om Den Europæiske Unions funktionsmåde.

---

43 Artikel 4, stk. 4, i 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.

44 https://europa.eu/youreurope/index.htm

45 Artikel 1, stk. 3, i 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).

46 Den konsoliderede udgave af traktaten om Den Europæiske Unions funktionsmåde (EUT C 326 af 26.10.2012, s. 47).

47 Se også Domstolens dom af 19. juni 2008, *Kommissionen for De Europæiske Fællesskaber* mod *Storhertugdømmet Luxembourg*, C-319/06, ECLI:EU:C:2008:350, præmis 90-91: Domstolen fandt, at en forpligtelse til at holde bestemte dokumenter til rådighed og opbevare dem i en bestemt medlemsstat udgør en hindring for den frie udveksling af tjenesteydelser. Det er ikke tilstrækkeligt at begrunde dette med, at det "generelt kan gøre det lettere for denne stats myndigheder at opfylde deres kontrolopgave".

48 Europa-Parlamentets og Rådets direktiv 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked (EUT L 376 af 27.12.2006, s. 36).

49 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.

Den generelle forordning om databeskyttelse[50] anerkender, at medlemsstaterne kan indføre betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger. Disse nationale begrænsninger bør dog som anført i betragtning 53 ikke hæmme den frie udveksling af personoplysninger i EU, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger. Dette er i overensstemmelse med artikel 16 i traktaten om Den Europæiske Unions funktionsmåde, som indeholder retsgrundlaget for vedtagelsen af bestemmelser om retten til beskyttelse af personoplysninger og bestemmelser vedrørende den frie udveksling sådanne oplysninger.

3.3 Anvendelsesområde for forordningen om fri udveksling af andre data end personoplysninger

Som anført tidligere har forordningen om fri udveksling af andre data end personoplysninger til formål at sikre den frie udveksling af andre data end personoplysninger "inden for Unionen"[51]. Den finder således ikke anvendelse på databehandlingstjenester, der finder sted uden for EU, og på dataplaceringskrav vedrørende denne behandling[52,53].

Forordningens anvendelsesområde er i henhold til artikel 2, stk. 1, således begrænset til behandling af elektroniske andre data end personoplysninger i EU, når denne behandling:

(a) leveres som en tjeneste til brugere, der er bosiddende eller etableret i EU, uanset om tjenesteleverandøren er etableret i EU eller ej, eller
(b) foretages af en fysisk eller juridisk person, der er bosiddende eller etableret i EU, til eget behov.

Eksempler:

Artikel 2, stk. 1, litra a), i forordningen om fri udveksling af andre data end personoplysninger:

- En cloudtjenesteleverandør, der er etableret i USA, leverer behandlingstjenester til kunder, der er bosiddende eller etableret i EU. Cloudtjenesteleverandøren forvalter sine aktiviteter via servere på EU's område. Her gemmes og behandles de europæiske kunders oplysninger. Cloudtjenesteleverandøren er ikke forpligtet til selv at eje EU-baseret infrastruktur, men har eksempelvis mulighed for at leje serverplads i EU.

[50] Artikel 9, stk. 4, i 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).

[51] Se artikel 1 i 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.

[52] Se betragtning 15 i 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.

[53] Begrebet "behandling" (artikel 3, stk. 2, i 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) er genstand for en bred definition, og forordningen — som fremhævet i betragtning 17 — bør gælde for databehandling i bredeste forstand og omfatte brugen af alle typer IT-systemer.

Forordningen om fri udveksling af andre data end personoplysninger finder anvendelse på denne type databehandling.

- En cloudtjenesteleverandør, der er etableret i Japan, tilbyder sine tjenester til europæiske kunder. Leverandørens behandlingskapacitet er placeret i Japan, hvor også alle behandlingsaktiviteter finder sted. Forordningen om fri udveksling af andre data end personoplysninger finder ikke anvendelse i dette tilfælde, såfremt alle behandlingsaktiviteter udføres uden for EU[54].

Artikel 2, stk. 1, litra b), i forordningen om fri udveksling af andre data end personoplysninger:

- En lille europæisk nystartet virksomhed fra medlemsstat A beslutter sig for at udvide sine forretninger ved at åbne en afdeling i medlemsstat B. Den nystartede virksomhed vælger for at begrænse udgifterne at centralisere den nye afdelings datalagring og -behandling i virksomhedens server i medlemsstat A. Medlemsstaterne må ikke forbyde sådanne bestræbelser på at centralisere IT-løsninger, medmindre dette i henhold til proportionalitetsprincippet begrundes i den offentlige sikkerhed.

På trods af at forordningen om fri udveksling af andre data end personoplysninger ikke finder anvendelse på de tilfælde, hvor alle behandlingsaktiviteter for andre data end personoplysninger udføres uden for EU, skal den generelle forordning om databeskyttelse overholdes, når datasættet omfatter personoplysninger. Under alle omstændigheder skal navnlig bestemmelserne om overførsel af personoplysninger til tredjelande eller internationale organisationer i henhold til den generelle forordning om databeskyttelse overholdes[55].

3.4 Aktiviteter vedrørende medlemsstaternes interne organisation

I henhold til forordningen om fri udveksling af andre data end personoplysninger er medlemsstaterne ikke forpligtede til at outsource levering af tjenesteydelser forbundet med

[54] Bemærk, at 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 ikke vedrører dataplaceringskrav som pålagt af medlemsstater for lagring af andre data end personoplysninger i tredjelande. Disse kan være medtaget i nationale retsordener. Af præciseringshensyn finder den generelle forordning om databeskyttelse anvendelse på behandling af personoplysninger om registrerede, der er i EU, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU, hvis behandlingsaktiviteterne vedrører: a) udbud af varer eller tjenester til sådanne registrerede personer i Unionen, uanset om betaling fra den registrerede person er påkrævet, eller b) overvågning af sådanne registrerede personers adfærd, for så vidt deres adfærd finder sted i Unionen. (se artikel 3, stk. 2, i den generelle forordning om databeskyttelse).

[55] Se Kommissionens websted, hvad angår overførsel af personoplysninger til tredjelande: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_da og meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM/2017/07 final, på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Hvad angår Japan har Kommissionen vedtaget sin afgørelse af 23. januar 2019, hvilket vil muliggøre fri dataudveksling mellem de to økonomier på grundlag af en garanteret høj beskyttelse.

andre data end personoplysninger, som de ønsker selv at levere eller at organisere på anden vis end gennem offentlige kontrakter.[56].

Artikel 2, stk. 3, andet afsnit, i forordningen om fri udveksling af andre data end personoplysninger lyder som følger:

"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[57], **uden kontraktmæssig betaling til private parter**, og berører heller ikke medlemsstaternes love og administrative bestemmelser vedrørende gennemførelsen af disse beføjelser og ansvar."[58]

Valget af denne "selvforsyning" af databehandlingstjenester, herunder "insourcing" eller gensidige aftaler mellem offentlige myndigheder, kan begrundes i legitime interesser. De typiske eksempler omfatter brugen af en "regeringssky" eller en regering, der bestiller et centralt IT-bureau til at levere databehandlingstjenester til offentlige institutioner og organer.

I forordningen om fri udveksling af andre data end personoplysninger opfordres medlemsstaterne dog til at tage lønsomheden og andre fordele ved brugen af eksterne tjenesteleverandører i betragtning[5960]. Så snart de nationale myndigheder begynder at "outsource" databehandling med kontraktmæssig betaling til private parter, og behandlingen foregår i EU, er denne behandling omfattet af forordningen om fri udveksling af andre data end personoplysninger. Det betyder, at princippet om fri udveksling af andre data end personoplysninger gælder for de nationale myndigheders almene og administrative praksis. De skal navnlig afholde sig fra at lægge begrænsninger på dataplacering, f.eks. i udbud om offentlige indkøb.[61]

---

[56] Betragtning 14 i 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.

[57] I henhold til artikel 2, stk. 1, nr. 4), i 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) forstås ved "offentligretlige organer" organer med følgende karakteristika: a) De er oprettet specielt med henblik på at imødekomme almenhedens behov, dog ikke behov af industriel eller kommerciel karakter, b) de er en juridisk person, og c) de finansieres for størstedelens vedkommende af staten, regionale eller lokale myndigheder eller af andre offentligretlige organer eller er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller de har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale eller lokale myndigheder eller andre offentligretlige organer.

[58] Det fremhæves i betragtning 13 i 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, at forordningen ikke berører direktiv 2014/24/EU.

[59] Betragtning 14 i 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.

[60] En ekstern tjenesteleverandør er enhver enhed, der ikke er et "offentligretligt organ" i henhold til artikel 2, stk. 1, nr. 4), i 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).

[61] Betragtning 13 i 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.

4 Selvreguleringstilgange til støtte for den frie udveksling af oplysninger

Selvregulering bidrager til innovation og tillid blandt markedsdeltagerne og sikrer potentielt en bedre tilpasning til markedsændringer. Dette afsnit giver et overblik over selvreguleringsinitiativerne for behandling af både personoplysninger og andre data end personoplysninger.

4.1 Dataportering og skift mellem cloudtjenesteleverandører

Forordningen om fri udveksling af andre data end personoplysninger har blandt andet til formål at forhindre leverandørfastlåsning, som opstår, når brugerne ikke har mulighed for at skifte mellem tjenesteleverandører, idet deres oplysninger er "låst fast" i leverandørens system, f.eks. grundet et specifikt dataformat eller kontraktbestemmelser, og ikke kan trækkes ud af leverandørens IT-system. En uhindret dataportering er afgørende med hensyn til brugernes frie valg af leverandør af databehandlingstjenester og dermed den reelle konkurrence på markedet.

Det er blevet stadig vigtigere med dataportabilitet mellem virksomheder på tværs af en række digitale industrier, herunder cloudtjenester.

I henhold til artikel 6 i forordningen om fri udveksling af andre data end personoplysninger skal Kommissionen tilskynde til og fremme udvikling af adfærdskodekser for selvregulering på EU-plan ("adfærdskodekser") med henblik på at bidrage til en konkurrencedygtig dataøkonomi. Dette skaber en ramme for industriens udarbejdelse af adfærdskodekser for selvregulering i forbindelse med tjenesteleverandørskift og dataportering mellem forskellige IT-systemer.

Der bør i forbindelse med udarbejdelsen af disse adfærdskodekser for dataportering tages højde for en række aspekter, navnlig:

- **bedste praksis** for fremme af tjenesteleverandørskift og dataportering i et struktureret, alment anvendt og maskinlæsbart format
- **minimumsoplysningskrav** for at sikre, at professionelle brugere, inden der indgås en kontrakt, får tilstrækkeligt detaljerede og klare 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
- **strategier med hensyn til certificeringsordninger**, som gør det lettere at sammenligne cloudtjenester samt
- **kommunikationskøreplaner** for at skabe større bevidsthed om adfærdskodekserne.

På cloudtjenestemarkedet er Kommissionen begyndt at lette arbejdet for arbejdsgrupperne vedrørende cloudinteressenter på det digitale indre marked. I disse grupper samles cloudeksperter og professionelle brugere, herunder små og mellemstore virksomheder. På nuværende tidspunkt er en undergruppe i gang med at udarbejde adfærdskodekser for selvregulering i forbindelse med dataportering og skift mellem cloudtjenesteleverandører

(arbejdsgruppen SWIPO)[62], mens en anden undergruppe arbejder på at udvikle en certificeringsordning for cloudsikkerhed (arbejdsgruppen CSPCERT)[63].

SWIPO-arbejdsgruppen er i gang med at udarbejde adfærdskodekser, der skal dække alle typer af cloudtjenester. Infrastruktur som en tjeneste (IaaS), platforme som en tjeneste (PaaS) og software som en tjeneste (SaaS).

Kommissionen forventer, at de forskellige adfærdskodekser suppleres med **standardiserede kontraktbestemmelser**[64]. Dette ville sikre en tilstrækkelig teknisk og retlig nøjagtighed ved den praktiske gennemførelse og anvendelse af adfærdskodekserne, hvilket er særligt vigtigt for små og mellemstore virksomheder. Det er meningen, at de standardiserede kontraktbestemmelser skal udarbejdes efter adfærdskodekserne (som bør være afsluttet inden den 29. november 2019).

I henhold til artikel 8 i forordningen om fri udveksling af andre data end personoplysninger evaluerer Kommissionen senest den 29. november 2022 gennemførelsen af forordningen. Således bliver det muligt at vurdere: i) konsekvenserne af den frie udveksling af oplysninger i Europa ii) forordningens anvendelse, navnlig på blandede datasæt iii) hvorvidt medlemsstaterne reelt har ophævet de eksisterende uberettigede dataplaceringskrav og iv) adfærdskodeksernes markedseffektivitet inden for dataportering og skift mellem cloudtjenesteleverandører.

Portabilitetsbegrebet og samspillet med den generelle forordning om databeskyttelse

I begge forordninger[65] henvises der til dataportabilitet og målet om at lette dataportering fra ét IT-miljø til et andet, dvs. enten til en anden leverandørs systemer eller til lokale systemer. Dette forhindrer leverandørfastlåsning og styrker konkurrencen mellem tjenesteleverandørerne. Forordningerne har dog forskellige tilgange til portabilitet, hvad angår relationen mellem interessegrupperne og bestemmelsernes retlige karakter.

Retten til dataportabilitet i henhold til artikel 20 i den generelle forordning om databeskyttelse fokuserer på forholdet mellem den registrerede og den dataansvarlige. Artiklen omhandler den registreredes ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger om sig selv, som vedkommende har givet til en dataansvarlig, og har ret til at transmittere disse oplysninger til en anden dataansvarlig uden hindring fra den

[62] Arbejdsgruppen for cloudskifte og dataportering.

[63] Arbejdsgruppen for en certificeringsordning for europæiske cloudtjenesteleverandører. Se også afsnit 4.3.

[64] Se betragtning 30 i 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.

[65] Artikel 6 i 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 og artikel 20 i 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).

dataansvarlige, som personoplysningerne er blevet givet til[66]. Typisk er de registrerede i denne kontekst forbrugere af diverse onlinetjenester, der ønsker at skifte mellem disse tjenesteleverandører.

Artikel 6 i forordningen om fri udveksling af andre data end personoplysninger omtaler ikke professionelle brugeres ret til dataportering, men henviser til en selvreguleringstilgang med frivillige adfærdskodekser for industrien. På samme tid er artiklen målrettet situationer, hvor den professionelle bruger har valgt at outsource behandlingen af sine data til en tredjepart, der tilbyder databehandlingstjenester[67]. I henhold til artikel 3, stk. 8, i forordningen om fri udveksling af andre data end personoplysninger kan en "professionel bruger" både omfatte "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".

I praksis vedrører portabiliteten i henhold til artikel 6 i forordningen om fri udveksling af andre data end personoplysninger B2B-samspil mellem en professionel bruger (som i de situationer, der indebærer behandling af personoplysninger, betragtes som "dataansvarlig" i henhold til den generelle forordning om databeskyttelse) og en tjenesteleverandør (der på samme vis i nogle tilfælde betragtes som "databehandler").

Der kan på trods af afvigelserne opstå situationer, hvor dataporteringen både er dækket af forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse, hvad angår blandede datasæt.

Eksempel:

En virksomhed, der gør brug af en cloudtjeneste, vælger at skifte cloudtjenesteleverandør og overføre alle data til en ny leverandør. Tjenesteleverandørskiftet og dataporteringen er underlagt bestemmelserne i den kontrakt, der er indgået mellem kunden og cloudtjenesteleverandøren. Såfremt den tidligere cloudtjenesteleverandør følger adfærdskodekserne som udarbejdet i henhold til forordningen om fri udveksling af andre data end personoplysninger, skal dataporteringen ske i overensstemmelse med kravene heri.

Hvis de overførte datasæt omfatter personoplysninger, skal porteringen ske i overensstemmelse med alle de relevante bestemmelser i den generelle forordning om

[66] Se Artikel 29-Gruppen: *Retningslinjer vedrørende retten til dataportabilitet.* WP 242 rev.01, vedtaget den 13. december 2016 som senest revideret og vedtaget den 5. april 2017.

[67] Betragtning 29 i 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: "Mens fysiske personer og forbrugere nyder godt af eksisterende EU-ret [dvs. den generelle forordning om databeskyttelse], fremmer den ikke mulighederne for at skifte tjenesteleverandør for brugere, der handler i forbindelse med deres forretnings- eller erhvervsmæssige aktiviteter."

databeskyttelse, navnlig at den nye cloudtjenesteleverandør skal overholde de gældende krav, herunder sikkerhedskravet[68].

Eksempel:

Vælger en bank at skifte leverandør af tjenester til forvaltning af kunderelationer (CRM), skal der muligvis overføres oplysninger (både personoplysninger og andre data end personoplysninger) fra den tidligere leverandør til den nye. Disse oplysninger underlægges efterfølgende diverse reguleringskrav — nogle i henhold til den generelle forordning om databeskyttelse og andre i henhold til forordningen om fri udveksling af andre data end personoplysninger.

4.2 Adfærdskodekser og certificeringsordninger for beskyttelse af personoplysninger

Der kan gøres brug af adfærdskodekser og certificeringsordninger for at dokumentere opfyldelsen af de forpligtelser, der er indeholdt i den generelle forordning om databeskyttelse (se artikel 24, stk. 3, og artikel 28, stk. 5).

I henhold til artikel 40, stk. 1, og artikel 42, stk. 1, i den generelle forordning om databeskyttelse bør medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynde industrien til udarbejdelse af adfærdskodekser og fastlæggelse af certificeringsmekanismer for databeskyttelse.

Sammenslutninger eller andre organer, der repræsenterer en specifik kategori af dataansvarlige eller databehandlere, kan udarbejde en adfærdskodeks for den pågældende sektor. Der skal forelægges et udkast af kodeksen for den pågældende kompetente tilsynsmyndighed med henblik på godkendelse[69]. Hvis udkastet til adfærdskodeksen vedrører behandlingsaktiviteter i flere medlemsstater, skal tilsynsmyndigheden fremlægge dette for Databeskyttelsesrådet inden godkendelse. Rådet kommer efterfølgende med sin udtalelse om, hvorvidt udkastet til kodekset er i overensstemmelse med den generelle forordning om databeskyttelse.

Databeskyttelsesrådet offentliggjorde sine retningslinjer for adfærdskodekser og tilsynsmyndigheder, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies, i henhold til den generelle forordning om databeskyttelse[70]. Retningslinjerne omfatter

---

[68] Se Artikel 29-Gruppen: *Udtalelse 05/2012 om cloudcomputing* som vedtaget den 1. juli 2012, WP196. Her gives en nærmere beskrivelse af cloudbrugernes og cloudtjenesteleverandørernes position og forpligtelser i forbindelse med behandlingen af personoplysninger.

[69] Se artikel 40, stk. 5,og artikel 55 i 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).

[70] Det Europæiske Databeskyttelsesråd: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, vedtaget den 12. februar 2019, offentlig version, som findes på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_da

information om udarbejdelsen af adfærdskodekser, godkendelseskriterierne og anden nyttig information. Databeskyttelsesrådets retningslinjer nr. 1/2018 for certificering og identificering af certificeringskriterier i henhold til artikel 42 og 43 (Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43) i den generelle forordning om databeskyttelse informerer på samme måde om certificering i henhold til forordningen og udarbejdelse og godkendelse af certificeringskriterier[71].

Eksempler på adfærdskodekser udarbejdet af cloudindustrien:

EU's adfærdskodeks for cloudtjenester (EU Cloud Code of Conduct), som blev iværksat af Kommissionen og udarbejdet i samarbejde med Cloud Select Industry Group (C-SIG) på baggrund af databeskyttelsesdirektivet[72] og senere den generelle forordning om databeskyttelse. EU Cloud Code of Conduct dækker alle former for cloudtjenester — software som en tjeneste (SaaS), platforme som en tjeneste (PaaS) og infrastruktur som en tjeneste (IaaS)[73].

Adfærdskodeksen for leverandører af cloudinfrastrukturtjenester i Europa (The Code of Conduct of the Cloud Infrastructure Services Providers in Europe (CISPE))[74] fokuserer på IaaS-leverandører. CISPE-adfærdskodeksen omfatter krav til IaaS-leverandører, der handler som databehandlere i henhold til den generelle forordning om databeskyttelse. Derudover indeholder den bestemmelser om forvaltningsstrukturen for kodeksens gennemførelse og anvendelse.

Adfærdskodeksen for cloudsikkerhedsalliancer vedrørende overholdelse af GDPR (The Cloud Security Alliance's Code of Conduct for GDPR Compliance) er målrettet alle interesserede parter inden for cloudcomputing og den europæiske lovgivning om personoplysninger, herunder cloudtjenesteleverandører, cloudkunder og potentielle kunder, cloudauditører og cloudformidlere. Adfærdskodeksen dækker alle former for cloudtjenesteleverandører[75].

4.3 Styrket tillid til grænseoverskridende databehandling — sikkerhedscertificering

Hvis tilliden til sikkerheden i forbindelse med databehandling i andre medlemsstater i henhold til betragtning 33 i forordningen om fri udveksling af andre data end personoplysninger styrkes, burde det mindske tilbøjeligheden hos markedsdeltagerne og i den offentlige sektor til at bruge placeringen af data som substitut for datasikkerhed. CSPCERT-arbejdsgruppen er ud

[71] Det Europæiske Databeskyttelsesråd: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, vedtaget den 23. januar 2019, som findes på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_da

[72] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (udløber den 24. maj 2018).

[73] Der findes yderligere oplysninger om EU Cloud Code of Conduct på: https://eucoc.cloud/en/home.html

[74] Du finder yderligere oplysninger om CISPE-adfærdskodeksen på: https://cispe.cloud/code-of-conduct/

[75] Du finder yderligere oplysninger om CSA-adfærdskodeksen på: https://gdpr.cloudsecurityalliance.org/

over cybersikkerhedspakken som foreslået af Kommissionen i 2017[76] i gang med at udarbejde henstillinger med henblik på at udarbejde en europæisk cloudcertificeringsordning, som vil blive forelagt Kommissionen. Denne ordning kan potentielt fremme den frie udveksling af oplysninger, gøre det nemmere at sammenligne cloudtjenester og fremme udbredelsen af cloudcomputing. Kommissionen kan anmode Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om at udarbejde en kandidatordning i henhold til de relevante bestemmelser i retsakten om cybersikkerhed[77]. Denne ordning kan vedrøre både personoplysninger og andre data end personoplysninger. Ud over retsakten om cybersikkerhed — og som fremhævet i afsnit 4.2 — kan GDPR også anvendes til at påvise, at der foreligger fornødne garantier for datasikkerhed[78].

Afsluttende bemærkninger

Det er helt afgørende for EU's evne til at udnytte det fulde potentiale af data — idet der kan opstå værdikæder på tværs af sektorer og grænser — at retssikkerheden for og tilliden til databehandlingen er sikret. Dette sikres med de to forordninger, som begge har til formål at sikre den frie udveksling af oplysninger. Forordningen om fri udveksling af andre data end personoplysninger og den generelle forordning om databeskyttelse danner grundlaget for den frie udveksling af alle oplysninger inden for EU og en yderst konkurrencedygtig europæisk dataøkonomi.

[76] Se også: https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Europa-Parlamentets og Rådets forordning af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed)

[78] Se betragtning 74 i retsakten om cybersikkerhed.