ARTIKEL 29-GRUPPEN VEDRØRENDE DATABESKYTTELSE

16/DA
WP 242 rev.01

Retningslinjer vedrørende retten til dataportabilitet

Vedtaget den 13. december 2016
Som senest revideret og vedtaget den 5. april 2017

Denne arbejdsgruppe blev nedsat i henhold til artikel 29 i direktiv 95/46/EF. Den fungerer som en uafhængig europæisk rådgivningsinstans vedrørende databeskyttelse og beskyttelse af privatlivets fred. Gruppens arbejdsopgaver er fastsat i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatsfunktionen varetages af direktorat C (Civilret, grundlæggende rettigheder og EU-borgerskab) i Kommissionen, Generaldirektoratet for Retlige Anliggender og Forbrugere, B-1049 Bruxelles, kontor MO59 05/35.

Websted: http://ec.europa.eu/justice/data-protection/index_en.htm

INDHOLDSFORTEGNELSE

Resumé

Artikel 20 i databeskyttelsesforordningen skaber en ny ret til dataportabilitet, som er nært beslægtet med retten til indsigt, men den afviger på mange måder herfra. Den gør det muligt for registrerede i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage de personoplysninger, som de har givet til en dataansvarlig, og at transmittere disse oplysninger til en anden dataansvarlig. Formålet med denne nye ret er at give den registrerede øget kontrol over de personoplysninger, der vedrører ham eller hende.

Eftersom den gør det muligt at transmittere personoplysninger direkte fra én dataansvarlig til en anden, er retten til dataportabilitet også et vigtigt redskab, der vil understøtte den frie udveksling af personoplysninger i EU og fremme konkurrencen mellem dataansvarlige. Den vil gøre det nemmere at skifte mellem forskellige tjenesteydere og vil derfor fremme udviklingen af nye tjenester som led i strategien for det digitale indre marked.

Denne udtalelse indeholder en vejledning i, hvordan retten til dataportabilitet som indført ved databeskyttelsesforordningen skal fortolkes og gennemføres. Den har til formål at drøfte retten til dataportabilitet og dens anvendelsesområde. Den præciserer de betingelser, som gælder for denne nye ret under hensyntagen til retsgrundlaget for databehandlingen (enten den registreredes samtykke eller nødvendigheden af at opfylde en kontrakt) og det faktum, at denne ret er begrænset til personoplysninger givet af den registrerede. Udtalelsen indeholder også konkrete eksempler og kriterier, som skal forklare, under hvilke omstændigheder denne ret finder anvendelse. I denne henseende mener WP29, at retten til dataportabilitet gælder for de oplysninger, som den registrerede bevidst og aktivt har givet, samt de personoplysninger, der genereres af dennes aktivitet. Denne nye ret kan ikke undermineres og begrænses til de personoplysninger, som meddeles direkte af den registrerede, f.eks. via en online-formular.

Som en god praksis bør de dataansvarlige begynde at udvikle midler, der kan bidrage til besvarelse af anmodninger om dataportabilitet såsom værktøjer til download samt programmeringsgrænseflader for applikationer. De bør garantere, at personoplysninger transmitteres i et struktureret, almindeligt anvendt og maskinlæsbart format, og de bør tilskyndes til at sikre dataformatets interoperabilitet ved udførelsen af en anmodning om dataportabilitet.

Denne udtalelse hjælper også dataansvarlige med klart at forstå deres respektive forpligtelser og anbefaler bedste praksis samt værktøjer, der sikrer overholdelse af retten til dataportabilitet. Endelig anbefales det i udtalelsen, at aktører fra industrien og brancheforeninger samarbejder om et fælles sæt af interoperable standarder og formater for at kunne leve op til kravene om retten til dataportabilitet.

I. Indledning

Artikel 20 i databeskyttelsesforordningen (GDPR) indfører en ny ret til dataportabilitet. Denne ret gør det muligt for registrerede i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage de personoplysninger, de har givet til en dataansvarlig, og uden hindring at transmittere de pågældende oplysninger til en anden dataansvarlig. Denne ret, som finder anvendelse under iagttagelse af visse betingelser, understøtter brugervalg, brugerkontrol og brugerbestemmelse.

Fysiske personer, der gjorde brug af denne ret til indsigt i henhold til databeskyttelsesdirektivet 95/46/EF, var begrænsede af den dataansvarliges valg af format ved levering af de ønskede oplysninger. **Hensigten med den nye ret til dataportabilitet er at give registrerede øget kontrol over deres egne personoplysninger, da den gør det nemmere for dem at flytte, kopiere eller transmittere personoplysninger fra ét IT-miljø til et andet** (hvad enten det er til deres eget system, betroede tredjeparters eller nye dataansvarliges systemer).

Ved at bekræfte fysiske personers personlige rettigheder og kontrol over de personoplysninger, der vedrører dem, er dataportabilitet også en mulighed for at "rebalancere" forholdet mellem registrerede og dataansvarlige[1].

Retten til personlig dataportabilitet kan også øge konkurrencen mellem tjenester (ved at gøre det nemmere at skifte tjenesteudbyder), men databeskyttelsesforordningen regulerer personoplysninger og ikke konkurrence. Artikel 20 begrænser i særdeleshed ikke retten til dataportabilitet til data, der er nødvendige eller nyttige ved tjenesteskift[2].

Selv om dataportabilitet er en ny ret, findes der allerede andre typer af portabilitet eller andre typer, der drøftes på andre områder af lovgivningen (f.eks. i sammenhæng med opsigelse af en kontrakt, roamingtjenester og adgang til tjenester på tværs af grænser[3]). Der kan opstå synergier og endog fordele for fysiske personer mellem de forskellige typer af portabilitet, hvis de skabes ved en kombineret fremgangsmåde, selv om analogier bør behandles varsomt.

Denne udtalelse er en vejledning til dataansvarlige, således at de kan opdatere deres praksis, processer og politikker. Udtalelsen præciserer betydningen af dataportabilitet for at sætte registrerede i stand til effektivt at udnytte deres nye ret.

II. Hvad er hovedelementerne i dataportabilitet?

Databeskyttelsesforordningen definerer retten til dataportabilitet i artikel 20, stk. 1, således:

> *Den registrerede har 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 dataansvarlige, som personoplysningerne er blevet givet til [...]*

- En ret til at modtage personoplysninger

For det første er dataportabilitet en **ret, den registrerede har til at modtage en delmængde af de personoplysninger**, der er behandlet af en dataansvarlig om ham eller hende, og til at

[1] Hovedformålet med dataportabilitet er at øge fysiske personers kontrol over deres personoplysninger og at sørge for, at de spiller en aktiv rolle i dataøkosystemet.
[2] Denne ret gør det eksempelvis muligt for banker at yde ekstra tjenester under brugerens kontrol ved at anvende personoplysninger, der i første omgang er indsamlet som en del af en energiforsyningstjeneste.
[3] Se Kommissionens dagsorden for et digitalt indre marked: https://ec.europa.eu/digital-agenda/en/digital-single-market, navnlig den første politiske søjle "Bedre onlineadgang til digitale varer og tjenester".

opbevare de pågældende oplysninger til yderligere personlig brug. En sådan opbevaring kan være på en privat enhed eller en privat cloud, uden at oplysningerne nødvendigvis transmitteres til en anden dataansvarlig.

I denne henseende supplerer dataportabilitet retten til indsigt. Et særligt træk ved dataportabilitet er, at den gør det nemt for registrerede selv at administrere og videreanvende personoplysninger. Disse oplysninger bør modtages "*i et struktureret, almindeligt anvendt og maskinlæsbart format*". En registreret kunne eksempelvis være interesseret i at hente sin aktuelle playliste (eller en historik over aflyttede numre) fra en musikstreamingtjeneste for at finde ud af, hvor mange gange han har lyttet til specifikke numre, eller for at finde ud af, hvilken musik han ønsker at købe eller lytte til på en anden platform. Ligeledes ønsker han måske at hente sin kontaktliste fra webmailprogrammet for f.eks. at oprette en bryllupsliste eller få oplysninger om køb foretaget ved brug af forskellige bonuskort eller at vurdere sine CO2-fodspor[4].

- **En ret til at transmittere personoplysninger fra én dataansvarlig til en anden dataansvarlig**

For det andet giver artikel 20, stk. 1, registrerede **ret til at transmittere personoplysninger fra én dataansvarlig til en anden dataansvarlig** "uden hindring". Oplysninger kan også transmitteres direkte fra én dataansvarlig til en anden efter anmodning fra den registrerede, og hvor det er teknisk muligt (artikel 20, stk. 2). I denne henseende tilskynder punkt 68 dataansvarlige til at udvikle indbyrdes kompatible formater, der muliggør dataportabilitet[5], men uden at skabe en forpligtelse for den dataansvarlige til at indføre eller opretholde behandlingssystemer, som er teknisk kompatible[6]. Databeskyttelsesforordningen forbyder dog dataansvarlige at skabe barrierer for transmissionen.

I virkeligheden giver dette element af dataportabilitet ikke kun registrerede mulighed for at få og videreanvende, men også at transmittere oplysninger, de har giver til en anden tjenesteudbyder (enten inden for samme branche eller i en anden). Ud over at give forbrugerne indflydelse ved at forhindre "fastlåsning" forventes det også at retten til dataportabilitet giver mulighed for innovation og datadeling mellem de dataansvarlige på en sikker og beskyttet måde under den registreredes kontrol[7]. Dataportabilitet kan fremme brugeres kontrollerede og begrænsede deling af personoplysninger mellem organisationer og således berige tjenester og kundeoplevelser[8]. Dataportabilitet kan smidiggøre transmission og videreanvendelse af personoplysninger vedrørende brugere blandt de forskellige tjenester, de er interesseret i.

---

[4] I disse tilfælde vedrører behandlingen af oplysninger foretaget af den registrerede enten personlige eller familiemæssige aktiviteter, når hele behandlingen udføres under kontrol af den registrerede alene, eller den kan foretages af en anden part på den registreredes vegne. I sidstnævnte tilfælde bør den anden part betragtes som dataansvarlig, hvorfor de principper og forpligtelser, der er fastsat i databeskyttelsesloven, skal overholdes, selv om det blot drejer sig om opbevaring af personoplysninger.

[5] Se også afsnit V.

[6] Som følge heraf bør der lægges særlig vægt på formatet af de transmitterede oplysninger for at garantere, at oplysningerne nemt kan videreanvendes af den registrerede eller en anden dataansvarlig. Se også afsnit V.

[7] Se flere forsøgsmæssige anvendelser i Europa, f.eks. MiData i Det Forenede Kongerige MesInfos/SelfData af FING i Frankrig.

[8] De såkaldte quantified self- og IoT-brancher har vist fordelen (og risiciene) ved at sammenkæde personoplysninger fra forskellige aspekter af en fysisk persons liv såsom fitness, beskæftigelse og kalorieindtag for at få et mere komplet billede af en fysisk persons liv i en enkelt fil.

- **Den dataansvarliges rolle**

Dataportabilitet garanterer retten til at modtage personoplysninger og til at behandle dem i overensstemmelse med den registreredes ønsker[9].

Dataansvarlige, der besvarer anmodninger om dataportabilitet, jf. betingelserne i artikel 20, er ikke ansvarlige for behandlingen foretaget af den registrerede eller nogen anden virksomhed, der modtager personoplysninger. De handler på vegne af den registrerede, herunder når personoplysningerne transmitteres direkte til en anden dataansvarlig. I denne henseende er den dataansvarlige ikke ansvarlig for, om den dataansvarlige, der modtager oplysningerne, overholder databeskyttelsesloven, i betragtning af at det ikke er den dataansvarlige, som sender oplysningerne, der vælger modtageren. Samtidig bør den dataansvarlige træffe beskyttelsesforanstaltninger for at sikre, at de virkelig handler på den registreredes vegne. De kan f.eks. indføre procedurer, der sikrer, at typen af transmitterede personoplysninger virkelig er de oplysninger, som den registrerede ønsker at transmittere. Dette kunne gennemføres ved at indhente en bekræftelse fra den registrerede enten før transmissionen eller på et tidligere tidspunkt, hvor det oprindelige samtykke til behandling blev givet, eller aftalen blev indgået.

Dataansvarlige, der besvarer en anmodning om dataportabilitet, har ingen speciel forpligtelse til at undersøge og verificere kvaliteten af oplysningerne, før de transmitteres. Disse oplysninger burde naturligvis allerede være korrekte og ajourførte i henhold til principperne anført i artikel 5, stk. 1, i databeskyttelsesforordningen. Desuden pålægger dataportabilitet ikke den dataansvarlige en forpligtelse til at opbevare personoplysninger længere end nødvendigt eller ud over en eventuel nærmere angivet opbevaringsperiode[10]. Vigtigst af alt er, at der ikke er nogen yderligere krav om opbevaring af oplysninger ud over den ellers gældende opbevaringsperiode for blot at behandle en eventuel fremtidig anmodning om dataportabilitet.

Når de personoplysninger, der anmodes om, behandles af en dataansvarlig, skal den aftale, der indgås, i henhold til artikel 28 i databeskyttelsesforordningen indeholde en forpligtelse til at bistå "den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger (...) til at besvare anmodninger om udøvelse af den registreredes rettigheder". Den dataansvarlige bør derfor i samarbejde med sine databehandlere indføre særlige procedurer til besvarelse af anmodninger om dataportabilitet. I tilfælde af et fælles controllership bør en kontrakt klart fordele ansvaret mellem de enkelte dataansvarlige vedrørende behandlingen af anmodninger om dataportabilitet.

Derudover er en dataansvarlig, der modtager oplysninger,[11] ansvarlig for at sikre, at de modtagne flytbare data er relevante og ikke overdrevne med hensyn til den nye databehandling. I tilfælde af en anmodning om dataportabilitet til en webmailtjeneste, hvor anmodningen bruges af den registrerede til at hente e-mails og sende dem til en sikret arkivplatform, behøver den nye dataansvarlige f.eks. ikke at behandle kontaktoplysningerne på den registreredes forretningsforbindelser. Hvis disse oplysninger ikke er relevante med hensyn til formålet med den nye behandling, bør de ikke beholdes og behandles.

[9] Retten til dataportabilitet er ikke begrænset til personoplysninger, som er nyttige og relevante for lignende tjenester, som udbydes af den dataansvarliges konkurrenter.

[10] Hvis den dataansvarlige i ovennævnte eksempel ikke opbevarer en fortegnelse over sange, som en bruger har spillet, kan disse personoplysninger ikke være omfattet af en anmodning om dataportabilitet.

[11] dvs. som modtager personoplysninger efter en anmodning om dataportabilitet fremsat af den registrerede til en anden dataansvarlig.

Dataansvarlige, der modtager oplysninger, er i alle tilfælde ikke forpligtede til at acceptere og behandle personoplysninger, der er transmitteret efter en anmodning om dataportabilitet. Hvis en registreret anmoder om transmission af oplysninger om sine banktransaktioner til en tjeneste, der bistår ham eller hende med budgetlægning, behøver den dataansvarlige, der modtager oplysningerne, heller ikke at acceptere alle oplysninger eller at opbevare alle oplysninger om transaktionerne, når de er blevet rubriceret, for så vidt angår den nye tjeneste. Med andre ord bør de accepterede og opbevarede oplysninger kun være de mest nødvendige og relevante for den tjeneste, der ydes af den dataansvarlige, der modtager oplysningerne.

En organisation, som "modtager" oplysninger, bliver en ny dataansvarlig med hensyn til disse personoplysninger og skal respektere principperne i artikel 5 i databeskyttelsesforordningen. Derfor skal den "nye" dataansvarlige, som modtager oplysninger, klart og direkte anføre formålet med den nye behandling før en eventuel anmodning om transmission af de flytbare data i overensstemmelse med kravene om gennemsigtighed som fastsat i artikel 14[12]. Med hensyn til eventuel anden databehandling, som den dataansvarlige udfører i henhold til sit ansvar, bør han anvende de principper, der er fastsat i artikel 5 såsom lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, integritet og fortrolighed, opbevaringsbegrænsning og ansvarlighed[13].

Dataansvarlige, der opbevarer personoplysninger, bør være parate til at fremme deres registreredes ret til dataportabilitet. Dataansvarlige kan også vælge at acceptere oplysninger fra en registreret, men de er ikke forpligtede til det.

- **Dataportabilitet vs. registreredes øvrige rettigheder**

Når en fysisk person udøver sin ret til dataportabilitet, gør han eller hun det, uden at det berører andre rettigheder (som det er tilfældet med alle andre rettigheder i databeskyttelsesforordningen). En registreret kan fortsætte med at bruge og nyde godt af den dataansvarliges tjeneste, selv efter en dataportabilitetsaktivitet. Dataportabilitet udløser ikke automatisk sletning af data[14] fra den dataansvarliges system og påvirker ikke den oprindelige opbevaringsperiode, som gælder for de oplysninger, der er transmitteret. Den registrerede kan udøve sine rettigheder, så længe den dataansvarlige stadig behandler oplysningerne.

Hvis den registrerede ønsker at udøve sin ret til sletning ("ret til at blive glemt" i henhold til artikel 17), kan dataportabilitet heller ikke anvendes af en datasansvarlig som en måde til at forsinke eller afslå en sådan sletning.

Hvis en registreret opdager, at personoplysninger, der er anmodet om i henhold til retten til dataportabilitet, ikke fuldt ud svarer til hans eller hendes anmodning, bør en eventuel

[12] Derudover bør den nye dataansvarlige ikke behandle personoplysninger, som ikke er relevante, og behandlingen skal begrænses til det, der er nødvendigt for de nye formål, selv om personoplysningerne er den del af et mere globalt datasæt, som transmitteres gennem en portabilitetsproces. Personoplysninger, som ikke er nødvendige for at opfylde formålet med den nye behandling, bør hurtigst muligt slettes.

[13] Så snart den dataansvarlige har modtaget de personoplysninger, der er sendt som en del af retten til dataportabilitet, kan de betragtes som "tilvejebragt af" den registrerede og kan retransmitteres i henhold til retten til dataportabilitet i det omfang, at de andre betingelser, der finder anvendelse på denne ret (dvs. retsgrundlaget for behandlingen ...), opfyldes.

[14] Som anført i artikel 17 i databeskyttelsesforordningen

yderligere anmodning om personoplysninger i henhold til en ret til indsigt overholdes fuldt ud i overensstemmelse med artikel 15 i databeskyttelsesforordningen.

Når en specifik lovgivning i EU eller en medlemsstat på et andet område også indeholder bestemmelser om en eller anden form for portabilitet af de pågældende data, skal der også tages hensyn til de betingelser, der er fastsat i denne specifikke lovgivning, ved imødekommelse af en anmodning om dataportabilitet i henhold til databeskyttelsesforordningen. For det første hvis det fremgår tydeligt af anmodningen fra den registrerede, at hans eller hendes intention ikke er at udøve sine rettigheder i henhold til databeskyttelsesforordningen, men kun at udøve sine rettigheder i henhold til den sektorspecifikke lovgivning, gælder databeskyttelsesforordningens bestemmelser om dataportabilitet ikke for denne anmodning[15]. Hvis anmodningen derimod er rettet mod portabilitet i henhold til databeskyttelsesforordningen, tilsidesætter eksistensen af en sådan specifik lovgivning ikke den generelle anvendelse af princippet om dataportabilitet for nogen dataansvarlig som fastsat af databeskyttelsesforordningen. I stedet skal det i hvert enkelt tilfælde vurderes, hvorledes en sådan specifik lovgivning kan påvirke retten til portabilitet, hvis det overhovedet er muligt.

III. Hvornår finder dataportabilitet anvendelse?

- **Hvilke behandlingsaktiviteter omhandles af retten til dataportabilitet?**

For at overholde databeskyttelsesforordningen skal dataansvarlige have et klart retsgrundlag for behandling af personoplysninger.

For at falde ind under anvendelsesområdet for dataportabilitet skal behandlingsaktiviteter i henhold til artikel 20, stk. 1, litra a) baseres:

- enten på den registreredes samtykke (i henhold til artikel 6, stk. 1, litra a), eller i henhold til artikel 9, stk. 2, litra a), når det gælder særlige kategorier af personoplysninger)

- eller på en kontrakt, som den registrerede er part i i henhold til artikel 6, stk. 1, litra b).

Titler på bøger, der er købt af en fysisk person i en onlineboghandel, eller sange, der lyttes til via en musikstreamingtjeneste, er eksempler på personoplysninger, som almindeligvis falder ind under anvendelsesområdet for dataportabilitet, fordi de behandles på grundlag af indgåelse af en kontrakt, som den registrerede er part i.

Databeskyttelsesforordningen giver ikke en generel ret til dataportabilitet i tilfælde, hvor behandlingen af personoplysninger ikke er baseret på et samtykke eller en kontrakt[16].

[15] Hvis den registreredes anmodning eksempelvis er specielt rettet mod at give en tjenesteudbyder af kontooplysninger adgang til sin bankkontohistorik med det formål, som er nævnt i betalingstjenestedirektiv 2 (PSD2), bør en sådan adgang gives i henhold til bestemmelserne i dette direktiv.

[16] Se punkt 68 og artikel 20, stk. 3, i databeskyttelsesforordningen. Artikel 20, stk. 3, og punkt 68 fastsætter, at dataportabilitet ikke finder anvendelse, når databehandling er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, eller når en dataansvarlig udøver offentlige opgaver eller overholder en retlig forpligtelse. Dataansvarlige er derfor ikke forpligtede til at sørge for portabilitet i disse tilfælde. Det er imidlertid god praksis at udvikle processer til

Finansielle institutioner er eksempelvis ikke forpligtede til at besvare en anmodning om dataportabilitet vedrørende personoplysninger, der er behandlet som en del af deres forpligtelser til at forhindre og påvise hvidvask af penge og anden økonomisk kriminalitet dataportabilitet omfatter heller ikke professionelle kontaktoplysninger behandlet i et forretningsforhold mellem virksomheder, hvor behandlingen hverken er baseret på den registreredes samtykke eller på en kontrakt, som han eller hun er part i.

Hvad arbejdstageres oplysninger angår, finder retten til dataportabilitet kun anvendelse, hvis behandlingen er baseret på en kontrakt, som den registrerede er part i. I mange tilfælde vil det ikke blive betragtet, som om samtykke er givet frivilligt i denne sammenhæng på grund af skævheden i magtbalancen mellem arbejdsgiver og arbejdstager[17]. Nogle HR-behandlinger er i stedet baseret på retsgrundlaget for legitim interesse eller er nødvendige for overholdelse af specifikke retlige forpligtelser på beskæftigelsesområdet. I praksis vil retten til dataportabilitet i en HR-sammenhæng uden tvivl berøre nogle behandlingsaktiviteter (såsom løn- og godtgørelsestjenester, intern rekruttering), men i mange andre situationer vil der være behov for at tage stilling fra sag til sag for at kontrollere, om alle betingelser, der gælder for retten til dataportabilitet, overholdes.

Endelig finder retten til dataportabilitet kun anvendelse, hvis databehandlingen "foretages automatisk" og omfatter derfor ikke de fleste papirfiler.

- **Hvilke personoplysninger skal være omfattet?**

For at falde ind under anvendelsesområdet for retten til dataportabilitet skal oplysninger i henhold til artikel 20, stk. 1, være:

- personoplysninger vedrørende den pågældende person, og
- som han eller hun har *givet* til en dataansvarlig.

I artikel 20, stk. 4, anføres det også, at overholdelse af denne ret ikke må krænke andres rettigheder eller frihedsrettigheder.

Første betingelse: personoplysninger vedrørende den registrerede

Kun personoplysninger falder ind under en anmodning om dataportabilitet. Derfor falder alle oplysninger, som er anonyme[18] eller ikke vedrører den registrerede, ikke ind under anvendelsesområdet. Pseudonymiserede oplysninger, som klart kan forbindes med en registreret (f.eks. den person, der tilvejebringer den respektive identifikator, jf. artikel 11, stk. 2), falder imidlertid ind under anvendelsesområdet.

I mange tilfælde vil dataansvarlige behandle oplysninger, der indeholder personoplysninger fra flere registrerede. Hvis dette er tilfældet, bør dataansvarlige ikke fortolke sætningen "personoplysninger vedrørende den registrerede" alt for snævert. Som et eksempel kan

---

automatisk besvarelse af anmodninger om portabilitet ved at følge de principper, der gælder for retten til dataportabilitet. Et eksempel herpå ville være en offentlig tjeneste, der tilbyder nem download af tidligere selvangivelser. For dataportabilitet som en god praksis i tilfælde af behandling baseret på retsgrundlaget for nødvendigheden af en legitim interesse og for eksisterende frivillige ordninger, se side 47 og 48 i WP29 Udtalelse 6/2014 om den registeransvarliges legitime interesser (WP217).

[17] Som WP29 foreslog i sin udtalelse 8/2001 af 13. september 2001 (WP48).

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf

telefon-, meddelelsestjeneste- eller VoIP-registreringer omfatte (i abonnentens kontohistorik) oplysninger om tredjeparter, der er involveret i indgående og udgående opkald. Selv om registreringer derfor vil indeholde personoplysninger om flere personer, bør abonnenter være i stand til at få disse registreringer som svar på anmodninger om dataportabilitet, fordi registreringerne (også) vedrører den registrerede. Hvis disse registreringer derefter transmitteres til en ny dataansvarlig, bør denne nye dataansvarlige imidlertid ikke behandle dem til formål, der kunne krænke tredjeparters rettigheder eller frihedsrettigheder (se nedenfor: tredje betingelse).

Anden betingelse: oplysninger tilvejebragt af den registrerede

Den anden betingelse indskrænker anvendelsesområdet til oplysninger "tilvejebragt af" den registrerede.

Der er mange eksempler på personoplysninger, som bevidst og aktivt vil blive "tilvejebragt af" den registrerede såsom kontooplysninger (f.eks. e-mailadresse, brugernavn, alder) sendt via onlineformularer. Ikke desto mindre hidrører oplysninger "tilvejebragt af" den registrerede også fra observation af dennes aktivitet. Som følge heraf mener WP29, at for at få det mest mulige ud af denne nye ret bør "tilvejebragt af" også omfatte de personoplysninger, der observeres ud fra brugernes aktiviteter såsom rådata behandlet af en intelligent måler eller andre typer tilknyttede objekter[19], aktivitetslogge, webstedshistorik eller søgeaktiviteter.

Denne sidstnævnte oplysningskategori omfatter ikke oplysninger, der er dannet af den dataansvarlige (ved hjælp af de oplysninger, der er observeret eller givet direkte som input) såsom en brugerprofil dannet ved analyse af rådata indsamlet via intelligent måling.

Ved at skelne mellem forskellige oplysningskategorier afhængigt af deres oprindelse kan det afgøres, hvorvidt de er omfattet af retten til dataportabilitet. Følgende kategorier kan kvalificeres som "tilvejebragt af den registrerede":

- **Oplysninger, som den registrerede aktivt og bevidst har leveret** (f.eks. e-mailadresse, brugernavn, alder etc.)
- **Observerede oplysninger, der er leveret af den registrerede i kraft af brugen af tjenesten eller enheden.** De kan f.eks. omfatte en persons søgehistorik, trafikdata og oplysning om placering. Andre rådata kan også være omfattet såsom hjerteslag sporet af kropsbåren elektronik.

I modsætning hertil dannes afledte og hentede oplysninger af den dataansvarlige på grundlag af data, der "tilvejebringes af den registrerede". Resultatet af en vurdering vedrørende en brugers helbred eller en profil, der er oprettet i forbindelse med risikostyring og finansielle reguleringer (f.eks. ved kreditvurdering eller overholdelse af regler om bekæmpelse af hvidvaskning af penge), kan f.eks. ikke i sig selv betragtes om "tilvejebragt af" den registrerede. Selv om disse oplysninger kan være en del af en profil, der opbevares af en dataansvarlig og er udledt eller hentet fra analysen af oplysninger leveret af den registrerede (f.eks. gennem hans aktiviteter), vil disse oplysninger typisk ikke blive betragtet som

[19] Ved at være i stand til at hente oplysninger, der stammer fra observation af den registreredes aktivitet, vil han eller hun også være i stand til få en bedre opfattelse af den dataansvarliges gennemførelsesvalg med hensyn til anvendelsesområdet for de observerede oplysninger og vil få nemmere ved at vælge, hvilke oplysninger han eller hun er villig til at give for at få en lignende service, og blive klar over, i hvor høj grad hans eller hendes ret til privatlivets fred respekteres.

"tilvejebragt af den registrerede" og således ikke falde ind under denne nye rets anvendelsesområde[20].

På grund af det generelle politiske mål med retten til dataportabilitet skal termen "tilvejebragt af den registrerede" fortolkes bredt og bør ikke omfatte "afledte oplysninger" og "hentede oplysninger", der omfatter oplysninger, som er dannet af en tjenesteyder (f.eks. algoritmiske resultater). En dataansvarlig kan udelade de afledte oplysninger, men bør inkludere alle andre personoplysninger, som den registrerede har givet via tekniske hjælpemidler, som den datasansvarlige stiller til rådighed[21].

Termen "tilvejebragt af" omfatter således personoplysninger, der vedrører den registreredes aktivitet eller stammer fra observationen af en fysisk persons adfærd, men omfatter ikke oplysninger, der stammer fra efterfølgende analyse af den pågældende adfærd. I modsætning hertil er alle personoplysninger, der er dannet af den dataansvarlige som en del af databehandlingen, f.eks. ved en personaliserings- eller anbefalingsproces, ved brugerkategorisering eller profilering, oplysninger, som er afledt af eller hentet fra personoplysninger givet af den registrerede, og er ikke omfattet af retten til dataportabilitet.

Tredje betingelse: retten til dataportabilitet må ikke krænke andres rettigheder eller frihedsrettigheder

Med hensyn til personoplysninger vedrørende andre registrerede:

Den tredje betingelse har til formål at undgå hentning og transmission af oplysninger, der indeholder andre registreredes personoplysninger (uden samtykke) til en ny dataansvarlig i tilfælde, hvor disse oplysninger sandsynligvis vil blive behandlet på en måde, der ville krænke andre registreredes rettigheder og frihedsrettigheder (artikel 20, stk. 4, i databeskyttelsesforordningen)[22].

En sådan krænkelse ville eksempelvis opstå, hvis transmissionen af oplysninger fra én dataansvarlig til en anden ville forhindre tredjeparter i af udøve deres rettigheder som registrerede i henhold til databeskyttelsesforordningen (såsom rettigheder til information, indsigt etc.).

Den registrerede, som begynder transmissionen af sine data til en anden dataansvarlig, giver enten sit samtykke til den nye dataansvarlige med hensyn til behandling eller indgår en kontrakt med den pågældende dataansvarlige. Hvis tredjeparters personoplysninger er

[20] Ikke desto mindre kan den registrerede stadig bruge sin "ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne" tillige med oplysning om "forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede" i henhold til artikel 15 i databeskyttelsesforordningen (som vedrører indsigtsret).

[21] Dette omfatter alle oplysninger observeret om den registrerede under de aktiviteter, som oplysningerne indsamles til såsom en transaktionshistorik eller adgangslog. Oplysninger indsamlet via sporing og registrering af den registrerede (såsom en app, der registrerer hjerterytme eller teknologi, der benyttes til at spore browsingadfærd) bør også betragtes som "tilvejebragt af" ham eller hende, selv om oplysningerne ikke transmitteres aktivt eller bevidst.

[22] Punkt 68 fastsætter, at "såfremt et sæt personoplysninger vedrører mere end én registreret, bør retten til at modtage personoplysningerne ikke berøre andre registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning".

omfattet af datasættet, skal behandlingen baseres på et andet retsgrundlag. En legitim interesse kan eksempelvis navnligt forfølges af den dataansvarlige i henhold til artikel 6, stk. 1, litra f), når den dataansvarliges formål er at yde en service over for den registrerede, der gør det muligt for sidstnævnte at behandle personoplysninger udelukkende ud fra et rent personligt eller familiemæssigt perspektiv. De personlige behandlingsaktiviteter, som den registrerede påbegynder, og som vedrører og potentielt påvirker tredjeparter, forbliver dennes ansvar i det omfang, at en sådan behandling ikke på nogen måde er besluttet af den dataansvarlige.

En webmailtjeneste kan f.eks. gøre det muligt at oprette en liste over en registrerets kontakter, venner, slægtninge, familie og et bredere miljø. Eftersom disse oplysninger vedrører (og er dannet af) den identificerbare fysiske person, som ønsker at udøve sin ret til dataportabilitet, bør dataansvarlige transmittere hele listen over indgående og udgående e-mails til den registrerede.

På samme måde kan en registrerets bankkonto indeholde personoplysninger vedrørende transaktioner, som ikke kun vedrører kontohaveren, men også andre fysiske personers transaktioner (f.eks. hvis de har overført penge til kontohaveren). Disse tredjeparters rettigheder og frihedsrettigheder bliver sandsynligvis ikke krænket af transmissionen af bankkontooplysninger til kontohaveren, når der er fremsat en anmodning om portabilitet − forudsat at oplysningerne i begge eksempler bruges til samme formål (dvs. en kontaktadresse, der kun bruges af den registrerede, eller den registreredes bankkontohistorik.

Omvendt vil tredjeparters rettigheder og frihedsrettigheder ikke blive respekteret, hvis den nye dataansvarlige bruger personoplysninger til andre formål, f.eks. hvis den dataansvarlige, der modtager oplysninger, bruger andre fysiske personers personoplysninger fra den registreredes kontaktliste til markedsføringsformål.

For at forhindre krænkelser af involverede tredjeparter er behandling af sådanne personoplysninger derfor kun tilladt i det omfang, at oplysningerne kontrolleres alene af den bruger, der anmoder om dem, og kun administreres ud fra rent personlige eller familiemæssige behov. En "ny" dataansvarlig (til hvem, oplysningerne kan transmitteres efter anmodning fra brugeren), der modtager data, må ikke bruge de transmitterede oplysninger fra tredjepart til egne formål, f.eks. til at foreslå markedsføring af produkter og tjenester over for de andre tredjepartsregistrerede. Disse oplysninger bør eksempelvis ikke bruges til at berige den tredjepartsregistreredes profil og genopbygge hans sociale miljø uden hans kendskab og samtykke[23]. De kan heller anvendes til hentning af oplysninger om sådanne tredjeparter og oprettelse af specifikke profiler, selv om den dataansvarlige allerede er i besiddelse af deres personoplysninger. Ellers vil en sådan behandling sandsynligvis være ulovlig og urimelig, navnlig hvis de pågældende tredjeparter ikke får besked og ikke kan udøve deres ret som registrerede.

Desuden er det en vigtig praksis for alle dataansvarlige (både for parter, der "sender", og parter, der "modtager" oplysninger) at implementere værktøjer, der sætter registrerede i stand til at vælge relevante oplysninger, som de ønsker at modtage og transmittere, og til at

[23] En social netværkstjeneste bør ikke berige sine medlemmers profil ved at bruge personoplysninger, der transmitteres af en registreret som en del af hans ret til dataportabilitet uden at respektere princippet om gennemsigtighed og også sørge for, at de beror på et passende retsgrundlag vedrørende denne specifikke behandling.

udelukke andre fysiske personers oplysninger, hvis det er relevant. Dette vil yderligere hjælpe med at reducere risikoen for tredjeparter, hvis personoplysninger kan overføres.

Desuden bør den dataansvarlige indføre samtykkemekanismer for andre involverede registrerede for at fremme transmissionen af oplysninger i de tilfælde, hvor disse parter er villige til samtykke, f.eks. hvis de også ønsker at flytte deres oplysninger til en anden dataansvarlig. En sådan situation kan f.eks. opstå med sociale netværk, men det er op til dataansvarlige at beslutte, hvilken vigtig praksis der skal følges.

Med hensyn til oplysninger omfattet af intellektuel ejendomsret og forretningshemmeligheder:
Andres rettigheder og frihedsrettigheder er nævnt i artikel 20, stk. 4. Selv om det ikke direkte vedrører portabilitet, kan dette forstås som "herunder forretningshemmeligheder eller intellektuel ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af". Selv om disse rettigheder dog bør overvejes, før en anmodning om dataportabilitet besvares, "bør denne vurdering dog ikke resultere i en afvisning af at give al information til den registrerede". Desuden bør den dataansvarlige ikke afslå en anmodning om dataportabilitet på grundlag af krænkelsen af en anden kontraktmæssig rettighed (f.eks. en udestående fordring eller en handelskonflikt med den registrerede).

Retten til dataportabilitet giver ikke en fysisk person ret til at misbruge oplysninger på en måde, der kunne karakteriseres som en urimelig praksis eller som ville udgøre et misbrug af intellektuelle ejendomsrettigheder.

En potentiel forretningsmæssig risiko kan imidlertid ikke i selv tjene som grundlag for ikke at svare på anmodningen om portabilitet, og dataansvarlige kan transmittere de personoplysninger, der er givet af registrerede på en måde, som ikke offentliggør oplysninger, der er omfattet af forretningshemmeligheder eller intellektuelle ejendomsrettigheder.

IV. Hvordan finder de generelle regler for udøvelsen af registreredes rettigheder anvendelse på dataportabilitet?

- Hvilke forhåndsmeddelelser bør der gives til den registrerede?

For at overholde den nye ret til dataportabilitet skal dataansvarlige informere registrerede om eksistensen af den nye ret til portabilitet. Hvis de pågældende personoplysninger indsamles direkte hos den registrerede, skal det ske "på det tidspunkt, hvor personoplysningerne indsamles". Hvis personoplysningerne ikke indhentes direkte fra den registrerede, skal den dataansvarlige give de oplysninger, der anmodes om i artikel 13, stk. 2, litra b), og artikel 14, stk. 2, litra c).

"Hvis personoplysningerne ikke er indhentet hos den registrerede", kræver artikel 14, stk. 3, at oplysningerne gives inden for en rimelig frist, som ikke overstiger en måned, efter indsamlingen af oplysningerne under den første kommunikation med den registrerede, eller når de fremlægges for tredjepart[24].

Når de giver de ønskede oplysninger, skal dataansvarlige sikre, at de skelner retten til dataportabilitet fra andre rettigheder. Derfor anbefaler WP29 især, at dataansvarlige tydeligt

[24] Artikel 12 kræver, at dataansvarlige giver "enhver meddelelse [...] i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, navnlig når oplysninger specifikt er rettet mod et barn".

forklarer forskellen mellem de typer oplysninger, som en registreret kan modtage via registreredes rettighederne til indsigt og dataportabilitet.

Desuden anbefaler gruppen, at dataansvarlige altid informerer om retten til portabilitet, inden registrerede lukker deres eventuelle konti. Dette gør det muligt at gøre status over deres personoplysninger og nemt transmittere oplysninger til deres egen enhed eller til en anden udbyder, før der indgås en kontrakt.

Endelig anbefaler WP29 som vigtig praksis for dataansvarlige, der "modtager" oplysninger, at registrerede får fyldestgørende oplysninger om personoplysningernes art, hvilket er relevant for udførelsen af deres tjenester. Ud over at understøtte en rimelig behandling gør dette det muligt for brugere at begrænse risiciene for tredjeparter og også enhver anden unødvendig duplikering af personoplysninger, også når der ikke er andre registrerede involveret.

- **Hvordan kan den dataansvarlige identificere den registrerede, før han besvarer dennes anmodning?**

Der findes ingen foreskrevne krav i databeskyttelsesforordningen om, hvordan den registrerede kan autentificeres. Ikke desto mindre fastsætter artikel 12, stk. 2, i databeskyttelsesforordningen, at den dataansvarlige ikke må afvise at efterkomme den registreredes anmodning om at udøve sine rettigheder (herunder retten til dataportabilitet), medmindre vedkommende behandler personoplysninger til et formål, der ikke kræver identifikation af en registreret, og det kan påvises, at vedkommende ikke er i stand til at identificere den registrerede. I henhold til artikel 11, stk. 2, kan den registrerede imidlertid i sådanne tilfælde give flere oplysninger for at muliggøre identifikation af ham eller hende. Desuden fastsætter artikel 12, stk. 6, at hvis en dataansvarlig har begrundet mistanke om identiteten af en registreret, kan denne anmode om yderligere oplysninger for at bekræfte den registreredes identitet. Hvis en registreret giver yderligere oplysninger, der muliggør identifikation, må den dataansvarlige ikke afslå at efterkomme anmodningen. Hvis oplysninger og data, der er indsamlet online, forbindes til pseudonymer eller unikke identifikatorer, kan datasansvarlige gennemføre passende procedurer, der sætter en fysisk person i stand til at anmode om dataportabilitet og modtage oplysninger, der vedrører ham eller hende. I alle tilfælde skal dataansvarlige etablere en procedure for bekræftelse på ægthed for med sikkerhed at kunne fastslå identiteten af den registrerede, som anmoder om sine personlige oplysninger eller mere generelt udøver de rettigheder, som databeskyttelsesforordningen indrømmer.

Disse procedurer eksisterer ofte allerede. De registrerede er ofte allerede autentificeret af den dataansvarlige før indgåelse af en kontrakt eller indhentning af samtykke til behandling. Som følge heraf kan de personoplysninger, der bruges til registrering af den pågældende fysiske person ved behandlingen, også bruges som bevis for at autentificere den registrerede til portabilitetsformål[25].

I disse tilfælde kræves der måske en anmodning om bevis for de registreredes juridiske identitet, mens verificering muligvis ikke er relevant for at vurdere forbindelsen mellem oplysningerne og den pågældende fysiske person, eftersom en sådan forbindelse ikke vedrører den officielle eller juridiske identitet. I det væsentlige kan den dataansvarliges mulighed for at

[25] F.eks. når databehandlingen er knyttet til en brugerkonto, forudsat at det relevante login og adgangskoden kan være nok til identificering af den registrerede.

anmode om yderligere oplysninger for at identificere en persons identitet ikke føre til overdrevne krav og til indhentning af personoplysninger, som ikke er relevante eller nødvendige for at styrke forbindelsen mellem den fysiske person og de personoplysninger, der anmodes om.

I mange tilfælde er sådanne bekræftelsesprocedurer allerede iværksat. Der anvendes f.eks. ofte brugernavne og adgangskoder for at give fysiske personer adgang til data på e-mailkonti, sociale netværkskonti og konti til forskellige andre tjenester, hvor fysiske personer vælger at bruge nogle af disse uden at afsløre deres fulde navn og identitet.

Hvis størrelsen af de oplysninger, som den registrerede har anmodet om, gør transmissionen via internettet problematisk, kan den dataansvarlige frem for at tillade en udvidet tidsperiode på højst tre måneder for at imødekomme anmodningen[26] også overveje alternative måder at sende oplysninger på, f.eks. ved hjælp af streaming eller lagring på CD, DVD eller andre fysiske medier, således at personoplysninger kan transmitteres direkte til en anden dataansvarlig (i henhold til artikel 20, stk. 2, i databeskyttelsesforordningen, hvis det er teknisk muligt).

- **Hvad er tidsfristen for at besvare en anmodning om portabilitet?**

Artikel 12, stk. 3, kræver, at den dataansvarlige giver "oplysninger om truffen foranstaltning" til den registrerede "uden unødig forsinkelse" og under alle omstændigheder "senest en måned efter modtagelsen af anmodningen". Denne periode på en måned kan udvides til højst tre måneder i komplicerede tilfælde, forudsat at den registrerede er blevet informeret om grunden til en sådan forsinkelse inden for én måned fra den oprindelige anmodning.

Dataansvarlige, der driver informationssamfundstjenester, vil sandsynligvis blive bedre rustede til at være i stand til at imødekomme anmodninger inden for en meget kort tidsperiode. For at leve op til brugernes forventninger er det god praksis at definere tidsrammen for, hvornår en anmodning om dataportabilitet typisk kan besvares, og meddele dette til de registrerede.

Dataansvarlige, der nægter at besvare anmodninger om portabilitet skal i henhold til artikel 12, stk. 4, underrette den registrerede om "årsagen til ikke at træffe foranstaltning og om muligheden for at indgive en klage til en tilsynsmyndighed og indbringe sagen for en retsinstans" senest en måned efter modtagelse af anmodningen.

Dataansvarlige skal respektere forpligtelsen til at svare inden for den givne periode, selv om det vedrører en afvisning. Med andre ord kan den dataansvarlige ikke forblive tavs, når han bliver bedt om at svare på en anmodning om dataportabilitet.

- **I hvilke tilfælde kan en anmodning om dataportabilitet afvises, eller hvornår kan der opkræves et gebyr?**

Artikel 12 forbyder den dataansvarlige at opkræve gebyr for levering af personoplysningerne, medmindre den dataansvarlige kan påvise, at anmodningerne er åbenbart grundløse eller overdrevne "især fordi de gentages". For informationssamfundstjenester, der specialiserer sig i automatisk behandling af personoplysninger og implementerer automatiske systemer såsom

[26] Artikel 12, stk. 3: "Den dataansvarlige oplyser den registrerede om foranstaltninger, der træffes på baggrund af en anmodning".

programmeringsgrænseflader for applikationer (API'er)[27] kan gøre udvekslingen med den registrerede nemmere og på den måde mindske den potentielle byrde på grund af de gentagne anmodninger. Der skulle derfor være meget få tilfælde, hvor dataansvarlige ville være i stand til at retfærdiggøre en afvisning af at levere de ønskede oplysninger, selv når det drejer sig om mange anmodninger om dataportabilitet.

Desuden bør der ikke tages hensyn til de samlede omkostninger for processer til besvarelse af anmodninger ved bestemmelse af en anmodnings maksimumstørrelse. Faktisk fokuserer artikel 12 i databeskyttelsesforordningen på anmodninger fra én registreret og ikke det samlede antal anmodninger, som den dataansvarlige modtager. Som følge heraf bør de samlede systemimplementeringsomkostninger ikke opkræves af de registrerede eller bruges som undskyldning for at afvise en anmodning om portabilitet.

V. Hvordan skal de flytbare data leveres?

- Hvilke midler forventes det, at de dataansvarlige implementerer til levering af data?

Artikel 20, stk. 1, i databeskyttelsesforordningen fastsætter, at registrerede har ret til at transmittere oplysninger til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til.

En sådan hindring kan karakteriseres som en juridisk, teknisk eller økonomisk hindring fra den dataansvarliges side for undgå eller bremse den registreredes eller en anden dataansvarligs indsigt, transmission eller videreanvendelse. En sådan hindring kunne f.eks. være: gebyrer for levering af oplysninger, mangel på interoperabilitet eller adgang til et dataformat eller API eller det leverede format, for stor forsinkelse eller besvær med at hente hele datasættet, bevidst forplumring af datasættet eller specifik og uretmæssig eller ekstremt store krav om sektorbestemt standardisering eller akkreditering[28].

Artikel 20, stk. 2, forpligter også dataansvarlige til at transmittere de flytbare data direkte til andre dataansvarlige, "hvis det er teknisk muligt".

Den tekniske gennemførlighed af transmissionen fra én dataansvarlig til en anden under den registreredes kontrol bør vurderes fra sag til sag. I punkt 68 præciseres det yderligere, hvad "teknisk muligt" er, idet det indikerer, at "det bør ikke skabe en forpligtelse for dataansvarlige til at indføre eller opretholde behandlingssystemer, som er teknisk kompatible".

Dataansvarlige forventes at transmittere personoplysninger i et interoperabelt format, selv om dette ikke forpligter dataansvarlige til at understøtte disse formater. Direkte transmission fra én dataansvarlige til en anden kunne derfor forekomme, når kommunikation mellem to systemer er mulig, på en sikker måde[29], og når det system, der modtager oplysninger, teknisk

[27] Programmeringsgrænseflade for applikationer (API) betyder grænseflader for applikationer eller webtjenester, der stilles til rådighed for dataansvarlige, således at andre systemer eller programmer kan koble sig på og arbejde med deres systemer.

[28] Der kan opstå nogle retlige forhindringer som dem, der vedrører andres rettigheder og frihedsrettigheder som nævnt i artikel 20, stk. 4, eller dem, der vedrører sikkerheden af den dataansvarliges egne systemer. Det er den dataansvarliges ansvar at retfærdiggøre, hvorfor sådanne forhindringer ville være retlige, og hvorfor de ikke udgør en hindring, jf. artikel 20, stk. 1.

[29] Gennem en autentificeret kommunikation med det nødvendige niveau af datakryptering.

set er i stand til at modtage indkommende oplysninger. Hvis tekniske forhindringer forbyder direkte transmission, skal den dataansvarlige forklare disse forhindringer for de registrerede, eftersom hans beslutning ellers vil få samme virkning, som hvis han afslår at træffe foranstaltninger i anledning af den registreredes anmodning (artikel 12, stk. 4).

På et teknisk niveau bør dataansvarlige undersøge og vurdere to forskellige og supplerende stier for at stille flytbare data til rådighed for registrerede eller andre dataansvarlige:

- en direkte transmission af det samlede datasæt af flytbare data (eller flere uddrag af dele af det globale datasæt)
- et automatiseret værktøj, der gør det muligt at uddrage relevante oplysninger.

Den anden måde foretrækkes muligvis af dataansvarlige i tilfælde af komplekse og store datasæt, da det sætter dem i stand til at uddrage alle dele af datasættet, som er relevante for den registrerede i forbindelse med hans eller hendes anmodning, kan hjælpe med at minimere risikoen og muligvis gøre det muligt at bruge datasynkroniseringsmekanismer[30] (f.eks. i forbindelse med en regelmæssig kommunikation mellem dataansvarlige). Det kan være en bedre måde at sikre overensstemmelse på for den "nye" dataansvarlige og ville udgøre god praksis med hensyn til at reducere trusler mod privatlivets fred fra den første dataansvarliges side.

Disse to forskellige og muligvis supplerende måder at levere relevante flytbare data på kunne implementeres ved at stille oplysninger til rådighed gennem forskellige ressourcer såsom sikker udveksling af meddelelser, en SFTP-server, en sikker WebAPI eller WebPortal. Registrerede bør være i stand til at gøre brug af et personligt datalager, et personligt informationsstyringssystem[31] eller andre slags betroede tredjeparter for at opbevare personoplysninger og give dataansvarlige tilladelse til at få adgang til og behandle personoplysningerne som krævet.

- **Hvad er det forventede dataformat?**

databeskyttelsesforordningen stiller krav til dataansvarlige om at levere de personoplysninger, som den fysiske person anmoder om, i et format, der understøtter videreanvendelse. Særligt artikel 20, stk. 1, i databeskyttelsesforordningen anfører, at personoplysninger skal gives "i et struktureret, almindeligt anvendt og maskinlæsbart format". Punkt 68 indeholder en yderligere præcisering af, at dette format skal være interoperabelt, en term, der defineres[32] i EU som:

> *det forhold, at adskilte og forskelligartede organisationer er i stand til at interagere med henblik på at nå gensidigt fordelagtige og vedtagne fælles mål, herunder også, at organisationerne udveksler information og viden, via de forretningsprocesser, de understøtter, gennem dataudveksling mellem deres respektive IKT-systemer.*

[30] Synkroniseringsmekanismen kan hjælpe med at opfylde de generelle forpligtelser i henhold til artikel 5 i databeskyttelsesforordningen, som fastsætter, at "personoplysninger skal være (...) korrekte og, om nødvendigt, ajourførte"

[31] Se f.eks. EDPS' udtalelse 9/2016 om personlige informationsstyringssystemer (PIMS), som er tilgængelig på https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

[32] Artikel 2 i Europa-Parlamentets og Rådets afgørelse nr. 922/2009/EF af 16. september 2009 om interoperabilitetsløsninger for europæiske offentlige myndigheder (ISA) EUT L 260 af 3.10.2009, s. 20.

Termerne "struktureret", "almindeligt anvendt" og "maskinlæsbart" er et sæt af minimale krav, der skulle gøre interoperabilitet af dataformatet leveret af den dataansvarlige nemmere. På den måde er "struktureret, almindeligt anvendt og maskinlæsbart" specifikationer for midlerne, hvorimod interoperabilitet er det ønskede resultat.

I punkt 21 i direktiv 2013/37/EU[33, 34] defineres "maskinlæsbar" som:

> *et filformat, som er struktureret på en sådan måde, at softwareapplikationer nemt kan identificere, genkende og uddrage specifikke data af interesse, herunder individuelle oplysninger og deres interne struktur. Data kodet i filer, der er struktureret i et maskinlæsbart format, er maskinlæsbare data. Maskinlæsbare formater kan være åbne eller lukkede de kan være formelle standarder eller ej. Dokumenter, der er kodet i et filformat, som begrænser en sådan automatisk behandling, fordi data ikke kan eller ikke uden problemer kan uddrages af sådanne dokumenter, bør ikke betragtes som dokumenter i maskinlæsbart format. Medlemsstaterne bør, hvor det er hensigtsmæssigt, tilskynde til brug af åbne maskinlæsbare formater.*

På grund af den lange række af mulige datatyper, der kunne behandles af en dataansvarlig, pålægger databeskyttelsesforordningen ikke specifikke anbefalinger til formatet af de personoplysninger, der skal leveres. Det mest passende format vil være forskelligt fra sektor til sektor, og passende formater eksisterer muligvis allerede, men bør altid vælges med det formål, at de er forståelige og giver den registrerede en høj grad af dataportabilitet. Som sådan ville formater, der er underlagt dyre licensbegrænsninger, ikke blive betragtet som en tilstrækkelig fremgangsmåde.

I punkt 68 præciseres det, at "*Den registreredes ret til at transmittere eller modtage personoplysninger vedrørende vedkommende bør ikke skabe en forpligtelse for dataansvarlige til at indføre eller opretholde behandlingssystemer, som er teknisk kompatible*". **Portabilitet har således til formål at producere interoperabilitetssystemer, ikke kompatible systemer**[35].

Personoplysninger forventes at blive leveret i formater, der har et højt niveau af abstraktion fra interne eller beskyttede formater. Som sådan indebærer dataportabilitet et yderligere lag af databehandling for dataansvarlige, således at oplysninger kan uddrages fra platformen, og personoplysninger kan filtreres fra uden for anvendelsesområdet af portabilitet såsom afledte oplysninger eller oplysninger vedrørende sikkerhedssystemer. På denne måde tilskyndes dataansvarlige til at identificere oplysninger i forvejen, som er inden for anvendelsesområdet af portabilitet i deres egne systemer. Denne yderligere databehandling betragtes om et supplement til hoveddatabehandlingen, eftersom den ikke udføres med et nyt formål for øje defineret af den dataansvarlige.

Hvis der ikke er nogen formater, der er almindeligt anvendt for en given branche eller i en given kontekst, **bør dataansvarlige levere personoplysninger i almindeligt anvendte åbne**

[33] Ændring af direktiv 2003/98/EF om videreanvendelse af den offentlige sektors informationer.
[34] EU-ordlisten (http://eur-lex.europa.eu/eli-register/glossary.html) indeholder en yderligere præcision af forventninger, der vedrører det koncept, der er anvendt i denne vejledning såsom *maskinlæsbar, interoperabilitet, åbent format, standard, metadata*.
[35] ISO/IEC 2382-01 definerer interoperabilitet som følger: "Evnen til at kommunikere, udføre programmer eller overføre data mellem forskellige funktionelle enheder på en måde, der kræver, at brugeren har lidt eller ingen viden om de unikke egenskaber ved disse enheder".

formater (f.eks. XML, JSON, CSV, …) sammen med brugbare **metadata i den bedst mulige granulering,** mens der opretholdes et højt niveau af abstraktion. Som sådan bør der anvendes passende metadata for at opnå en præcis beskrivelse af de udvekslede oplysninger. Denne metadata bør vær nok til at muliggøre funktionen og videreanvendelsen af oplysningerne, men naturligvis uden at afsløre forretningshemmeligheder. Det er derfor ikke sandsynligt, at de PDF-versioner af en e-mailindbakke, som en fysisk person får, ville være tilstrækkeligt strukturerede eller beskrivende til, at indbakkeoplysningerne nemt kunne videreanvendes. E-mailoplysninger bør i stedet leveres i et format, som bevarer alle metadata, hvilket muliggør effektiv videreanvendelse af oplysningerne. Når den dataansvarlige vælger et dataformat til levering af personoplysningerne, bør han overveje, hvordan dette format ville påvirke eller forhindre en fysisk persons ret til at videreanvende oplysningerne. I tilfælde hvor en dataansvarlig er i stand til at tilbyde den registrerede valgmuligheder med hensyn til det foretrukne format af personoplysningerne, bør der gives en tydelig forklaring på indflydelsen af valget. Behandling af yderligere metadata med det ene formål, at der muligvis er brug for dem, eller at de kræves for at svare på en anmodning om dataportabilitet, udgør ikke nogen legitim grund til en sådan behandling.

WP29 opfordrer indtrængende til samarbejde mellem aktører fra industrien og brancheforeninger om et fælles sæt af interoperable standarder og formater for at kunne leve op til kravet om retten til dataportabilitet. Denne udfordring er også blevet taget op af den europæiske interoperabilitetsramme (EIF), som har skabt en fælles tilgang til interoperabilitet for organisationer, som i fællesskab ønsker at levere offentlig service. Inden for sit anvendelsesområde fastsætter rammen et sæt fælles elementer såsom vokabular, begreber, principper, politikker, vejledninger, anbefalinger, standarder, specifikationer og praksisser[36].

- **Hvordan håndterer man en stor eller kompleks samling af personoplysninger?**

databeskyttelsesforordningen forklarer ikke, hvordan man håndterer udfordringen med besvarelse, når der opstår en stor datasamling, en kompleks datastruktur eller andre tekniske problemer, som kan skabe vanskeligheder for dataansvarlige eller registrerede.

I alle tilfælde er det afgørende, at den fysiske person er i stand til fuldt ud at forstå definition, skema og struktur i forbindelse med de personoplysninger, som den dataansvarlige kunne levere. F.eks. kunne oplysninger først leveres i kort form ved hjælp af dashboards, der gør det muligt for den registrerede at overføre personoplysninger i delmængder frem for i deres helhed. Den dataansvarlige bør give en oversigt "i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog" (se artikel 12, stk. 1, i databeskyttelsesforordningen) på en måde, således at den registrerede altid har klar information om, hvilke oplysninger der skal downloades eller transmitteres til en anden dataansvarlig i forbindelse med et givet formål. Registrerede bør f.eks. være i stand til at bruge softwareprogrammer for nemt at kunne identificere, genkende og behandle specifikke oplysninger derfra.

Som nævnt ovenfor kan en dataansvarlig besvare anmodninger om dataportabilitet på en praktisk måde ved at tilbyde en passende sikker og dokumenteret API. Dette kan sætte fysiske personer i stand til at fremsætte den dataansvarliges anmodninger om deres personoplysninger via deres egen eller tredjeparts software eller give tilladelse til, at andre gør det på deres vegne

[36] Kilde: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

(herunder en anden dataansvarlig) som fastsat i artikel 20, stk. 2, i databeskyttelsesforordningen. Ved at give adgang til oplysninger via en ekstern tilgængelig API kan det også være muligt at tilbyde et mere sofistikeret adgangssystem, der sætter fysiske personer i stand til at fremsætte efterfølgende anmodninger om oplysninger, enten som komplet filhentning eller som deltafunktion, der kun indeholder ændringer siden sidste filhentning, uden at disse yderligere anmodninger bliver besværlige for den dataansvarlige.

- **Hvordan kan flytbare data sikres?**

Generelt bør dataansvarlige garantere "tilstrækkelig sikkerhed for personoplysningerne, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger" i henhold til artikel 5, stk. 1, litra f), i databeskyttelsesforordningen.

Transmissionen af personoplysninger til den registrerede kan imidlertid også føre til nogle sikkerhedsmæssige problemer:

Hvordan kan dataansvarlige sikre, at personoplysninger leveres på en sikker måde til den rette person?

Eftersom formålet med dataportabilitet er at få personoplysninger ud af den dataansvarliges informationssystem, kan transmissionen udgøre en mulig risiko med hensyn til de pågældende oplysninger (navnlig ved brud på datasikkerheden under transmissionen). Den dataansvarlige er ansvarlig for at træffe alle de nødvendige sikkerhedsforanstaltninger og ikke kun at sørge for sikker transmission (ved hjælp af end-to-end-datakryptering) til den rette destination (ved hjælp af stærke autentifikationsforanstaltninger), men også at fortsætte med at beskytte de personoplysninger, der forbliver i systemet, og sørge for klare procedurer i forbindelse med eventuelle brud på datasikkerheden[37]. Som sådan bør dataansvarlige vurdere de særlige risici, der er forbundet med dataportabilitet, og træffe de fornødne foranstaltninger for at begrænse dem.

Sådanne risikobegrænsende foranstaltninger kunne omfatte: brug af yderligere autentifikationsoplysninger (i tilfælde hvor den registrerede allerede skal autentificeres) såsom en fælles hemmelighed eller andre autentificeringsfaktorer såsom en engangsadgangskode; udsættelse eller frysning af transmissionen, hvis der er mistanke om, at kontoen er kompromitteret; autentificering ved mandat såsom tokenbaserede ægthedsbekræftelser i tilfælde af direkte transmission fra den dataansvarlige til en anden dataansvarlig.

Sådanne sikkerhedsforanstaltninger må ikke være obstruktive og må ikke forhindre brugere i at udøve deres rettigheder, f.eks. ved at pålægge yderligere omkostninger.

Hvordan hjælper man brugere med at sikre deres personoplysninger i deres egne systemer?

Når brugerne henter deres personoplysninger fra en onlinetjeneste, er der altid risiko for, at de lagrer dem i mindre sikre systemer end det, der leveres af tjenesten. Den registrerede, som anmoder om oplysningerne, er ansvarlig for at træffe de rette foranstaltninger for at sikre personoplysningerne i sit eget system. Han bør imidlertid gøres opmærksom på dette for at

[37] I overensstemmelse med direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

sikre beskyttelse af de oplysninger, han modtager. Som et eksempel på førende god praksis kan dataansvarlige også anbefale passende format(er), krypteringsværktøjer og andre sikkerhedsforanstaltninger, som kan hjælpe den registrerede med at nå dette mål.

* * *

Udfærdiget i Bruxelles, den 13. december 2016

På gruppens vegne
Forkvinden
Isabelle FALQUE-PIERROTIN

Som senest revideret og vedtaget den 5. april 2017

På gruppens vegne
Forkvinden
Isabelle FALQUE-PIERROTIN