



Riktlinjer om rätten till dataportabilitet

**Antagna den 13 december 2016
Senast reviderade och antagna den 5 april 2017**

Denna arbetsgrupp inrättades genom artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ för uppgiftsskydd och integritetsskydd. Arbetsuppgifterna finns beskrivna i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

För sekretariatet svarar direktorat C (Grundläggande rättigheter och rättsstatsprincipen) vid Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, Kontor MO59 05/35.

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

INNEHÅLLSFÖRTECKNING

Sammanfattning	3
I. Inledning	3
II. Vad är de viktigaste inslagen i dataportabilitet?	4
III. När ska dataportabilitet tillämpas?	9
IV. Hur ska de allmänna bestämmelserna om utövande av registrerades rättigheter tillämpas på dataportabilitet?	14
V. Hur ska de flyttbara uppgifterna tillhandahållas?	17

Sammanfattning

Genom artikel 20 i dataskyddsförordningen införs en ny rätt till dataportabilitet. Denna rätt är nära besläktad med rätten till tillgång till uppgifter men skiljer sig på en mängd sätt. Rätten till dataportabilitet ger registrerade rätt att få ut de personuppgifter som de har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig. Syftet med denna nya rättighet är att stärka den registrerade och ge honom eller henne större kontroll över de personuppgifter som rör honom eller henne.

Eftersom rätten till dataportabilitet möjliggör direkt överföring av personuppgifter från en personuppgiftsansvarig till en annan är denna rätt även ett viktigt redskap för att stödja det fria flödet av personuppgifter i EU och främja konkurrensen mellan personuppgiftsansvariga. Den kommer att göra det lättare att byta tjänsteleverantör och kommer därför att gynna utvecklingen av nya tjänster inom ramen för strategin för den digitala inre marknaden.

Detta yttrande ger vägledning om hur den rätt till dataportabilitet som införts genom dataskyddsförordningen ska tolkas och genomföras. I yttrandet diskuteras rätten till dataportabilitet och dess räckvidd. Det förtydligas under vilka villkor denna nya rätt gäller, och hänsyn tas till den rättsliga grunden för behandlingen av uppgifter (antingen den registrerades samtycke eller nödvändigheten av att fullgöra ett avtal) och till att denna rätt är begränsad till personuppgifter som den registrerade har tillhandahållit. I yttrandet ges också konkreta exempel och kriterier för att förklara under vilka omständigheter denna rätt ska tillämpas. Artikel 29-gruppen anser att rätten till dataportabilitet omfattar uppgifter som den registrerade medvetet och aktivt har tillhandahållit samt de personuppgifter som den registrerades verksamhet har genererat. Denna nya rätt kan inte undergrävas och begränsas till de personuppgifter som den registrerade direkt har lämnat, exempelvis på ett nätformulär.

Som ett led i god praxis bör personuppgiftsansvariga utveckla metoder för att besvara ansökningar om dataportabilitet, exempelvis ladda ned verktyg och gränssnitt för tillämpningsprogram (API). Personuppgiftsansvariga bör garantera att personuppgifter överförs i ett strukturerat, allmänt använt och maskinläsbart format, och de bör uppmuntras att säkerställa att de uppgifter som överförs inom ramen för en begäran om dataportabilitet överförs i ett kompatibelt format.

Yttrandet hjälper även personuppgiftsansvariga att förstå sina respektive skyldigheter och rekommenderar bästa praxis och verktyg som stöder efterlevnaden av rätten till dataportabilitet. I yttrandet rekommenderas slutligen intressenter inom sektorn och branschorganisationer att tillsammans ta fram en gemensam uppsättning kompatibla standarder och format för att uppfylla de krav som rätten till dataportabilitet innebär.

I. Inledning

Genom artikel 20 i den allmänna dataskyddsförordningen (nedan kallad *dataskyddsförordningen*) införs en ny rätt till dataportabilitet. Denna rätt innebär att registrerade har rätt att få ut de personuppgifter som rör dem och som de har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att hindras. Denna

rätt, som gäller med vissa förbehåll, ger användarna större valmöjligheter, mer kontroll och mer inflytande.

Enskilda som utnyttjade sin rätt till tillgång till uppgifter enligt dataskyddsdirektivet 95/46/EG begränsades av det format som den personuppgiftsansvarige använde när denne lämnade ut den begärda informationen. **Den nya rätten till dataportabilitet syftar till att ge de registrerade mer inflytande över sina egna personuppgifter, eftersom den gör det lättare att flytta, kopiera eller överföra personuppgifter från en it-miljö till en annan** (oavsett om överföringen sker till deras egna system, betrodda tredje parter system eller system som tillhör nya personuppgiftsansvariga).

Genom att bekräfta enskildas personliga rättigheter och kontroll över de personuppgifter som berör dem innebär dataportabiliteten även en möjlighet att förändra balansen i förhållandet mellan registrerade och personuppgiftsansvariga.¹

Även om rätten till överföringen av personuppgifter även kan öka konkurrensen mellan tjänster (genom att göra det lättare att byta tjänst), reglerar dataskyddsförordningen personuppgifter och inte konkurrens. Framför allt begränsas inte de uppgifter som kan överföras i artikel 20 till de uppgifter som är nödvändiga eller användbara för att byta tjänst.²

Även om dataportabilitet är en ny rätt finns eller diskuteras redan andra typer av portabilitet på andra lagstiftningsområden (t.ex. inom ramen för uppsägning av avtal, roamingtjänster på telekomområdet och gränsöverskridande tillgång till tjänster³). De olika typerna av portabilitet kan ge upphov till vissa synergieffekter och fördelar för enskilda om de tillhandahålls inom ramen för en gemensam strategi, även om man bör vara försiktig med att dra allt för långtgående analogier.

Yttrandet ger vägledning till personuppgiftsansvariga så att de kan uppdatera sin praxis, sina processer och sina policyer. Dessutom förtydligas vad dataportabilitet innebär så att registrerade kan utnyttja sin nya rätt på ett effektivt sätt.

II. Vad är de viktigaste inslagen i dataportabilitet?

I artikel 20.1 i dataskyddsförordningen definieras dataportabilitet på följande sätt:

Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta [...]

¹ Det främsta syftet med dataportabilitet är att ge enskilda ökad kontroll över sina personuppgifter och se till att de spelar en aktiv roll i dataekosystemet.

² Tack vare denna rätt kan banker exempelvis erbjuda ytterligare tjänster, som kontrolleras av användaren, genom att använda personuppgifter som ursprungligen samlades in inom ramen för en energitjänst.

³ Se Europeiska kommissionens agenda för en digital inre marknad: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, särskilt den första grundpelaren ”Bättre tillgång till digitala varor och tjänster på nätet”.

- Rätt att få ut personuppgifter

För det första innebär dataportabilitet **rätt för den registrerade att få ut en del av de personuppgifter** som rör honom eller henne och som behandlas av en personuppgiftsansvarig, och att lagra dessa uppgifter för personligt bruk. Lagringen kan ske på en privat enhet eller i ett privat moln, utan att uppgifterna behöver överföras till en annan personuppgiftsansvarig.

I detta avseende kompletterar rätten till dataportabilitet rätten till tillgång till uppgifter. Ett särdrag för dataportabilitet är att dataportabiliteten gör det lätt för de registrerade att själva hantera och vidareutnyttja personuppgifter. Uppgifterna bör fås *”i ett strukturerat, allmänt använt och maskinläsbart format”*. En registrerad kan exempelvis vara intresserad av att ta fram sin aktuella spellista (eller en historik över spelade sånger) från en musikströmningstjänst för att ta reda på hur många gånger han eller hon har lyssnat på vissa sånger eller för att se vilken musik han eller hon vill köpa eller spela på en annan plattform. På samma sätt kanske en registrerad vill ta fram sin lista på kontakter i sin webbmejl-tjänst exempelvis för att sätta samman en bröllopslista, få information om köp med olika lojalitetskort eller beräkna sitt koldioxidavtryck.⁴

- Rätt att överföra personuppgifter från en personuppgiftsansvarig till en annan

För det andra ger artikel 20.1 registrerade **rätt att överföra personuppgifter från en personuppgiftsansvarig till en annan** ”utan att hindras”. Uppgifter kan även överföras direkt från en personuppgiftsansvarig till en annan på begäran av den registrerade när detta är tekniskt möjligt (artikel 20.2). I skäl 68 uppmuntras personuppgiftsansvariga att utveckla kompatibla format som möjliggör dataportabilitet⁵, men personuppgiftsansvariga åläggs inte att införa eller upprätthålla tekniskt kompatibla system för behandling av uppgifter⁶. Dataskyddsförordningen förbjuder emellertid personuppgiftsansvariga att skapa hinder för överföringen.

I huvudsak gör denna aspekt av dataportabiliteten det möjligt för registrerade att inte bara få ut och vidareutnyttja sina uppgifter, utan även att överföra uppgifterna till en annan tjänsteleverantör (antingen inom samma eller en annan sektor). Förutom att ge konsumenterna ökat inflytande genom att förhindra ”inlåsning” av uppgifterna förväntas rätten till dataportabilitet främja innovationsmöjligheter och delning av personuppgifter mellan personuppgiftsansvariga på ett tryggt och säkert sätt och under den registrerades kontroll.⁷ Dataportabilitet kan främja kontrollerad och begränsad delning av personuppgiftsansvändare

⁴ I dessa fall kan den registrerades behandling av uppgifterna antingen falla inom ramen för hushållsverksamhet, om den registrerade kontrollerar all behandling, eller hanteras av en annan part, på den registrerades vägnar. I det sistnämnda fallet bör den andra parten betraktas som personuppgiftsansvarig, även om det endast rör sig om lagring av personuppgifter, och måste därför iakttas de principer och skyldigheter som anges i dataskyddsförordningen.

⁵ Se även avsnitt V.

⁶ Särskild uppmärksamhet bör därför fästas vid formatet på de överförda uppgifterna, så att den registrerade eller en annan personuppgiftsansvarig utan någon större ansträngning garanterat kan vidareutnyttja uppgifterna. Se även avsnitt V.

⁷ Se flera experimentella tillämpningar i Europa, exempelvis [MiData](#) i Förenade kungariket och [MesInfos/SelfData](#) av FING i Frankrike.

mellan organisationer och på så sätt leda till bättre tjänster och kundupplevelser.⁸ Dataportabilitet kan underlätta överföring och vidareutnyttjande av personuppgifter som rör användare mellan de olika tjänster som de är intresserade av.

⁸ De industrier som har vuxit upp kring s.k. egenmätning och sakernas internet har visat fördelarna (och riskerna) med att koppla ihop personuppgifter från olika aspekter av en persons liv, som t.ex. konditionsnivå, aktivitet och kaloriintag, för att ge en mer komplett bild av en persons liv i en enda fil.

- Kontroll

Dataportabilitet garanterar rätten att få ut personuppgifter och behandla dem i enlighet med den registrerades önskemål.⁹

Personuppgiftsansvariga som besvarar en begäran om dataportabilitet är, enligt de villkor som anges i artikel 20, inte ansvariga för den behandling som utförs av den registrerade eller av ett annat företag som tar emot personuppgifter. De agerar på den registrerades vägnar, inbegripet när personuppgifterna överförs direkt till en annan personuppgiftsansvarig. I detta avseende är den personuppgiftsansvarige inte ansvarig för att den mottagande personuppgiftsansvarige följer dataskyddslagstiftningen, eftersom det inte är den översändande personuppgiftsansvarige som väljer vem som ska ta emot uppgifterna. Samtidigt ska den personuppgiftsansvarige införa skyddsmekanismer för att säkerställa att de verkligen agerar på den registrerades vägnar. De kan t.ex. införa förfaranden för att säkerställa att den typ av personuppgifter som översänds verkligen är den typ som den registrerade vill överföra. Detta kan åstadkommas genom att inhämta en bekräftelse från den registrerade, antingen före överföringen eller tidigare, när det ursprungliga samtycket till behandlingen ges eller avtalet ingås.

Personuppgiftsansvariga som besvarar en begäran om dataportabilitet har ingen särskild skyldighet att kontrollera och bekräfta uppgifternas kvalitet innan de överförs. Dessa uppgifter bör givetvis redan vara tillförlitliga och uppdaterade enligt de principer som anges i artikel 5.1 i dataskyddsförordningen. Genom dataportabiliteten åläggs inte heller den personuppgiftsansvarige att lagra personuppgifter längre än nödvändigt eller längre än en viss lagringstid.¹⁰ Det är viktigt att påpeka att det inte finns något krav på att lagra uppgifter under längre tid än de lagringstider som annars gäller, bara för att eventuellt tillmötesgå en framtida begäran om dataportabilitet.

När de begärda personuppgifterna behandlas av ett personuppgiftsbiträde måste det avtal som ingåtts i enlighet med artikel 28 i dataskyddsförordningen innehålla en skyldighet att hjälpa ”den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, (...) att svara på begäran om utövande av den registrerades rättigheter”. Den personuppgiftsansvarige bör därför införa särskilda förfaranden i samarbete med sitt personuppgiftsbiträde för att svara på begäran om dataportabilitet. Vid delad kontroll bör det i ett avtal klart framgå vilket ansvar varje enskild personuppgiftsansvarig har när det gäller handläggningen av en begäran om dataportabilitet.

En mottagande personuppgiftsansvarig¹¹ är dessutom ansvarig för att säkerställa att de flyttbara uppgifter som tillhandahålls är relevanta och inte alltför omfattande för den nya uppgiftsbehandlingen. Om en begäran om dataportabilitet t.ex. görs till en webbmejl tjänst, för att den registrerade ska få tillgång till e-postmeddelanden och kunna skicka dessa till en säker plattform för arkivering, behöver den nye personuppgiftsansvarige inte behandla kontaktuppgifterna till den registrerades kontakter. Om denna information inte är relevant för den nya behandlingen bör den inte sparas och behandlas. I vilket fall som helst är mottagande

⁹ Rätten till dataportabilitet begränsas inte till personuppgifter som är användbara och relevanta för liknande tjänster som tillhandahålls av konkurrenter till den personuppgiftsansvarige.

¹⁰ Om en personuppgiftsansvarig i ovannämnda exempel inte lagrar uppgifter om de låtar som en användare spelar kan dessa personuppgifter inte inkluderas i en begäran om dataportabilitet.

¹¹ Dvs. som får ut personuppgifter efter att den registrerade har gjort en begäran om dataportabilitet till en annan personuppgiftsansvarig.

personuppgiftsansvariga inte skyldiga att godta och behandla personuppgifter som överförs till följd av en begäran om dataportabilitet. Om en registrerad begär överföring av uppgifter om hans eller hennes banktransaktioner till en tjänst som hjälper honom eller henne att föra sin budget, behöver den personuppgiftsansvarige inte heller godta alla uppgifter, eller lagra alla transaktionsdetaljer när de väl har rubricerats för den nya tjänsten. Med andra ord bör endast sådana uppgifter godtas och lagras som är nödvändiga och relevanta för den tjänst som tillhandahålls av den mottagande personuppgiftsansvarige.

En ”mottagande” organisation blir en ny personuppgiftsansvarig för dessa personuppgifter och måste iakttä de principer som anges i artikel 5 i dataskyddsförordningen. Därför måste den ”nya” personuppgiftsansvarige tydligt och direkt ange ändamålet med den nya behandlingen innan en begäran om överföring av de flyttbara uppgifterna i enlighet med kraven på öppenhet i artikel 14.¹² Vad gäller all annan uppgiftsbehandling som utförs under den personuppgiftsansvariges ledning bör den personuppgiftsansvarige tillämpa de principer som anges i artikel 5, nämligen laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, integritet och konfidentialitet, lagringsbegränsning och ansvarsskyldighet.¹³

Personuppgiftsansvariga som lagrar personuppgifter bör vara beredda på att underlätta de registrerades rätt till dataportabilitet. Personuppgiftsansvariga kan även välja att godta uppgifter från en registrerad. De är dock inte skyldiga att göra detta.

- Dataportabilitet jämförd med andra rättigheter som den registrerade har

När en enskild person utnyttjar sin rätt till dataportabilitet påverkar detta inte hans eller hennes övriga rättigheter (vilket är fallet med andra rättigheter i dataskyddsförordningen). En registrerad kan fortsätta att använda och dra nytta av den personuppgiftsansvariges tjänst även efter att rätten till dataportabilitet har utnyttjats. Dataportabilitet leder inte automatiskt till att uppgifter raderas¹⁴ från den personuppgiftsansvariges system, och påverkar inte den ursprungliga lagringsperioden för de uppgifter som har överförts. Den registrerade kan utnyttja sin rätt så länge den personuppgiftsansvariga fortfarande behandlar uppgifterna.

Om den registrerade vill utnyttja sin rätt till radering (”rätten att bli bortglömd” enligt artikel 17) kan dataportabilitet inte heller användas av en personuppgiftsansvarig som ett sätt att försena eller vägra en sådan radering.

Om en registrerad upptäcker att de personuppgifter som begärts ut enligt rätten till dataportabilitet inte helt och hållet motsvarar hans eller hennes begäran, ska varje ytterligare begäran om personuppgifter enligt den registrerades rätt till tillgång beviljas, i enlighet med artikel 15 i dataskyddsförordningen.

¹² Den nya personuppgiftsansvarige bör dessutom inte behandla personuppgifter som inte är relevanta, och behandlingen måste begränsas till vad som är nödvändigt för de nya ändamålen, även om personuppgifterna är en del av en större uppsättning uppgifter som överförs via en portabilitetsprocess. Personuppgifter som inte är nödvändiga för att uppfylla den nya behandlingens ändamål bör raderas så fort som möjligt.

¹³ När de personuppgifter som översänts inom ramen för utnyttjandet av rätten till dataportabilitet har tagits emot av den personuppgiftsansvarige kan uppgifterna anses ha ”tillhandahållits av” den registrerade och kan på nytt överföras i enlighet med rätten till dataportabilitet, i den mån övriga villkor för att utnyttja denna rätt (dvs. den rättsliga grunden för behandlingen) är uppfyllda.

¹⁴ Se artikel 17 i dataskyddsförordningen.

Om en viss EU-rättsakt eller medlemsstatslag på ett annat område också ger viss rätt att överföra de berörda uppgifterna måste de villkor som anges i den lagstiftningen också beaktas vid beviljandet av en begäran om dataportabilitet enligt dataskyddsförordningen. För det första, om det av den registrerades begäran tydligt framgår att han eller hon inte har för avsikt att utöva rättigheter enligt dataskyddsförordningen, utan snarare rättigheter som enbart grundas på sektorslagstiftning, omfattas en sådan begäran inte av dataskyddsförordningens portabilitetsbestämmelser.¹⁵ Om begäran däremot avser portabilitet enligt dataskyddsförordningen har sådan specifik lagstiftning inte företräde framför en personuppgiftsansvarigs allmänna tillämpning av portabilitetsprincipen. I stället måste man i varje enskilt fall bedöma om, och i så fall hur, sådan specifik lagstiftning kan påverka rätten till dataportabilitet.

III. När ska dataportabilitet tillämpas?

- Vilken behandling omfattas av rätten till dataportabilitet?

För att inte bryta mot dataskyddsförordningen måste personuppgiftsansvariga ha en tydlig rättslig grund för behandlingen av personuppgifter.

Enligt artikel 20.1 a i dataskyddsförordningen måste behandlingen, **för att omfattas av tillämpningsområdet för dataportabilitet**, grundas på

- antingen den registrerades samtycke (enligt artikel 6.1 a eller artikel 9.2 a när det gäller särskilda kategorier av uppgifter),
- eller på ett avtal som den registrerade är part i enligt artikel 6.1 b.

Titlarna på de böcker som en person har köpt från en nätbokhandel eller de låtar som han eller hon har lyssnat på via en musikströmningstjänst är t.ex. exempel på personuppgifter som i regel omfattas av tillämpningsområdet för dataportabilitet, eftersom de behandlas på grundval av fullgörandet av ett avtal som den registrerade är part i.

Genom dataskyddsförordningen införs inte en allmän rätt till dataportabilitet för de fall där behandlingen av personuppgifter inte grundas på samtycke eller avtal.¹⁶ Ett finansinstitut är t.ex. inte skyldigt att besvara en begäran om dataportabilitet beträffande personuppgifter som behandlas som ett led i dess skyldighet att förhindra och upptäcka penningtvätt och annan ekonomisk brottslighet. Dataportabilitet omfattar inte heller yrkesmässiga kontaktuppgifter

¹⁵ Om målet för den registrerades begäran exempelvis är att ge en leverantör av kontoinformationstjänster tillgång till sin bankkontohistorik, för de ändamål som anges i det andra betaltjänstdirektivet (PSD2), bör sådan tillgång beviljas i enlighet med bestämmelserna i det direktivet.

¹⁶ Se skäl 68 och artikel 20.3 i dataskyddsförordningen. I artikel 20.3 och skäl 68 anges att dataportabilitet inte gäller i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, eller när en personuppgiftsansvarig utför uppgifter av allmänt intresse eller fullgör en rättslig förpliktelse. Personuppgiftsansvariga är därför inte skyldiga att tillhandahålla portabilitet i dessa fall. Det är dock god praxis att utveckla processer för att automatiskt besvara en begäran om portabilitet, genom att följa de principer som styr rätten till dataportabilitet. Ett exempel på detta är en statlig tjänst som gör det lätt att ladda ned tidigare inkomstskattedeklarationer. För dataportabilitet som god praxis vid behandling som grundas på den rättsliga grund som innebär att behandlingen måste vara nödvändig för att tillgodose berättigade intressen och för befintliga frivilliga system, se sidorna 47 och 48 i artikel 29-arbetsgruppens yttrande 6/2014 om berättigade intressen (WP217).

som behandlas inom ramen för en affärsrelation, om behandlingen varken grundas på den registrerades samtycke eller på ett avtal som han eller hon är part i.

När det gäller anställdas uppgifter gäller rätten till dataportabilitet endast om behandlingen grundas på ett avtal som den registrerade är part i. I många fall anses inte samtycke ha getts frivilligt i detta sammanhang, på grund av maktobalansen mellan arbetsgivare och anställd.¹⁷ Viss behandling av anställdas personuppgifter grundas i stället på den rättsliga grunden berättigat intresse, eller är nödvändig för att fullgöra specifika rättsliga förpliktelser på sysselsättningsområdet. I praktiken berör rätten till dataportabilitet av anställdas personuppgifter viss behandling (t.ex. lön och ersättningar, intern rekrytering), men i många andra situationer måste man från fall till fall bedöma huruvida alla villkor för att tillämpa rätten till dataportabilitet är uppfyllda.

Slutligen gäller rätten till dataportabilitet endast om behandlingen av uppgifterna ”sker automatiserat”. De flesta pappersakter omfattas därför inte.

- Vilka personuppgifter måste ingå?

Enligt artikel 20.1 ska uppgifter för att omfattas av tillämpningsområdet för rätten till dataportabilitet vara

- personuppgifter som rör den registrerade, och
- som han eller hon har *tillhandahållit* den personuppgiftsansvarige.

I artikel 20.4 anges dessutom att iakttagandet av denna rätt inte får påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Första villkoret: personuppgifter som rör den registrerade

Endast personuppgifter omfattas av tillämpningsområdet för en begäran om dataportabilitet. Uppgifter som är avidentifierade¹⁸ eller inte rör den registrerade omfattas därför inte. Pseudonymiserade uppgifter som tydligt kan kopplas till en registrerad (t.ex. genom att han eller hon tillhandahåller respektive identifikator, se artikel 11.2) omfattas emellertid.

I många fall behandlar personuppgiftsansvariga information som innehåller personuppgifter om flera registrerade. I så fall bör de personuppgiftsansvariga inte tolka frasen ”personuppgifter som rör den registrerade” alltför restriktivt. Register över telefonsamtal, ip-meddelanden eller ip-telefoni kan (i prenumerantens kontohistorik) innehålla detaljer om tredje parter som deltagit i inkommande och utgående samtal. Även om registren därför innehåller personuppgifter beträffande flera personer bör prenumeranter kunna få ut dessa uppgifter som svar på en begäran om dataportabilitet, eftersom uppgifterna (också) rör den registrerade. Om sådana uppgifter emellertid överförs till en ny personuppgiftsansvarig bör denna nya personuppgiftsansvarige inte behandla dem för ändamål som skulle påverka dessa tredje parter rättigheter och friheter på ett ogynnsamt sätt (se det tredje villkoret nedan).

Andra villkoret: uppgifter som den registrerade har tillhandahållit

¹⁷ Vilket artikel 29-arbetsgruppen redogjorde för i sitt yttrande 8/2001 av den 13 september 2001 (WP48).

¹⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_sv.pdf

Det andra villkoret begränsar tillämpningsområdet till uppgifter som den registrerade har ”tillhandahållit”.

Det finns gott om exempel på personuppgifter som den registrerade medvetet och aktivt har ”tillhandahållit”, såsom kontouppgifter (t.ex. e-postadress, användarnamn, ålder) som lämnats via nätformulär. De uppgifter som den registrerade har ”tillhandahållit” är emellertid även resultatet av observationer av hans eller hennes aktivitet. Artikel 29-arbetsgruppen anser därför att för att denna rätt ska få sitt fulla värde måste ”tillhandahållit” även inbegripa de personuppgifter som kan observeras från användarnas aktivitet, t.ex. rådata som behandlats av en smart mätare eller andra typer av uppkopplade föremål¹⁹, aktivitetsloggar, historik över besökta webbplatser eller sökhistorik.

Sistnämnda kategori av uppgifter inbegriper inte uppgifter som skapas av den personuppgiftsansvarige (med hjälp av uppgifter som observerats eller som tillhandahållits direkt), exempelvis en användarprofil som skapats genom att analysera rådata från smarta mätare.

En åtskillnad kan göras mellan olika kategorier av uppgifter, beroende på deras ursprung, för att avgöra om de omfattas av rätten till dataportabilitet. Följande kategorier kan klassificeras som uppgifter som ”den registrerade har tillhandahållit”:

- **Uppgifter som den registrerade aktivt och medvetet har tillhandahållit** (exempelvis e-postadress, användarnamn, ålder etc.).
- **Observerade uppgifter som den registrerade har tillhandahållit genom användning av tjänsten eller enheten.** Dessa kan t.ex. inbegripa en persons sökhistorik, trafikuppgifter och platsuppgifter. De kan även inbegripa andra rådata som den hjärtfrekvens som mätts upp av en bärbar pulsmätare.

Avledda och härledda uppgifter skapas däremot av den personuppgiftsansvarige på grundval av de uppgifter som ”den registrerade har tillhandahållit”. Resultatet av en bedömning av en användares hälsa eller den profil som skapats inom ramen för riskhantering och finanslagstiftning (t.ex. att ge ett kreditbetyg eller följa regler för att förhindra penningtvätt) kan inte i sig anses ha ”tillhandahållits av” den registrerade. Även om sådana uppgifter kan ingå i en profil som den personuppgiftsansvarige har sparat och är avledda eller härledda från analysen av de uppgifter som den registrerade har tillhandahållit (t.ex. genom sina handlingar), betraktas de vanligtvis inte som uppgifter som ”den registrerade har tillhandahållit” och omfattas därför inte av tillämpningsområdet för denna nya rätt.²⁰

Med tanke på det politiska syftet med rätten till dataportabilitet måste i regel begreppet ”som den registrerade har tillhandahållit” ges en vid tolkning, och detta begrepp bör inte omfatta ”avledda uppgifter” eller ”härledda uppgifter”, vilket inbegriper personuppgifter som skapats

¹⁹ Genom att kunna ta fram uppgifter som är ett resultat av observationer av den registrerades aktivitet får den registrerade även en bättre bild av de val som den personuppgiftsansvarige har gjort beträffande räckvidden för de observerade uppgifterna, och har större möjligheter att välja vilka uppgifter som han eller hon är villig att tillhandahålla för att få en liknande tjänst, och blir mer medveten om i vilken utsträckning hans eller hennes personliga integritet respekteras.

²⁰ Den registrerade kan trots det fortfarande utnyttja sin ”rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna” och information om ”förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade”, enligt artikel 15 i dataskyddsförordningen (som rör den registrerades rätt till tillgång).

av en tjänsteleverantör (exempelvis algoritmer). En personuppgiftsansvarig kan exkludera sådana avledda uppgifter men bör inte inkludera alla andra personuppgifter som den registrerade har tillhandahållit via tekniska medium som den personuppgiftsansvarige har tillhandahållit.²¹

Begreppet ”tillhandahållit” inbegriper därför personuppgifter som rör den registrerades aktivitet eller följer av observationer av en persons beteende, men inbegriper inte uppgifter som följer av senare analyser av det beteendet. Uppgifter som har skapats av den personuppgiftsansvarige som ett led i behandlingen av uppgifter, t.ex. genom en individanpassnings- eller rekommendationsprocess, genom kategorisering av användare eller genom profilering är däremot uppgifter som är härledda eller avledda från de personuppgifter som den registrerade har tillhandahållit. De omfattas därför inte av rätten till dataportabilitet.

Tredje villkoret: rätten till dataportabilitet får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt

Personuppgifter som rör andra registrerade:

Syftet med det tredje villkoret är att undvika att uppgifter som innehåller personuppgifter om andra registrerade (som inte har gett sitt samtycke) tas fram och överförs till en ny personuppgiftsansvarig i situationer där dessa uppgifter troligen kommer att behandlas på ett sätt som skulle påverka andra registrerades rättigheter och friheter på ett ogynnsamt sätt (artikel 20.4 i dataskyddsförordningen).²²

Ett exempel på en sådan ogynnsam påverkan är exempelvis om överföringen av uppgifter från en personuppgiftsansvarig till en annan skulle hindra tredje parter från att utöva sina rättigheter som registrerade enligt dataskyddsförordningen (rätten till information, rätten till tillgång etc.).

En registrerad som inleder överföring av sina uppgifter till en annan personuppgiftsansvarig samtycker till den nya personuppgiftsansvariges behandling eller ingår ett avtal med denna personuppgiftsansvarige. Om personuppgifter från tredje part ingår i uppsättningen uppgifter måste en annan rättslig grund för behandlingen åberopas. Den personuppgiftsansvarige kan t.ex. ha ett berättigat intresse enligt artikel 6.1 f, särskilt när målet för den personuppgiftsansvarige är att tillhandahålla en tjänst till den registrerade som gör det möjligt för den sistnämnda personen att behandla personuppgifter som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Den behandling som inleds av den registrerade inom ramen för en verksamhet av privat natur som rör och potentiellt kan påverka tredje part är fortfarande hans eller hennes ansvar, i den utsträckning ett beslut om en sådan behandling inte på något sätt fattas av den personuppgiftsansvarige.

²¹ Detta inbegriper alla observerade uppgifter om den registrerade under dennes aktiviteter för det ändamål för vilket uppgifterna samlas in, t.ex. en transaktionshistorik eller åtkomstlogg. Uppgifter som samlats in genom att övervaka och registrera den registrerades aktivitet (t.ex. genom en app som registrerar hjärtslag eller teknik som används för att följa webbläsarbeteende) bör också betraktas som att de har ”tillhandahållits” av den registrerade även om uppgifterna inte har överförts på ett aktivt eller medvetet sätt.

²² I skäl 68 anges följande: ”Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning.”

En webb mejltjänst kan exempelvis göra det möjligt att skapa en förteckning över den registrerades kontakter, vänner, släktingar och vidare bekantskapskrets. Eftersom dessa uppgifter rör (och skapats av) den identifierbara person som vill utöva sin rätt till dataportabilitet bör personuppgiftsansvariga överföra hela förteckningen över inkommande och utgående e-postmeddelanden till den registrerade.

På samma sätt kan en registrerads bankkonto innehålla personuppgifter om inte bara kontoinnehavarens transaktioner utan även andra personers transaktioner (t.ex. om de har överfört pengar till den registrerade). Dessa tredje parter rättigheter och friheter påverkas sannolikt inte ogynnsamt av överföringen av kontoinformationen till kontoinnehavaren när en begäran om dataportabilitet görs – förutsatt att uppgifterna i båda exemplen används för samma ändamål (dvs. en kontaktadress som endast används av den registrerade eller en historik över kontohändelser på den registrerades bankkonto.

Däremot respekteras tredje parter rättigheter och friheter inte om de nya personuppgiftsansvariga använder personuppgifterna för andra ändamål, dvs. om den mottagande personuppgiftsansvarige i marknadsföringssyfte använder personuppgifter från andra personer i den registrerades förteckning över kontakter.

För att förhindra negativa effekter för berörda tredje parter är behandlingen av sådana personuppgifter bara tillåten i den mån uppgifterna kontrolleras av den användare som har lämnat in begäran om dataportabilitet och endast hanteras för privata behov eller hushållsbehov. En mottagande ”ny” personuppgiftsansvarig (till vilken uppgifterna kan överföras på begäran av användaren) får inte använda de överförda tredjepartsuppgifterna för sina egna privata syften, t.ex. för att marknadsföra varor och tjänster till dessa registrerade tredje parter. Uppgifterna bör exempelvis inte användas för att göra den registrerade tredje partens profil mer omfattande och bygga om hans eller hennes sociala miljö, utan denna persons kännedom och samtycke.²³ Uppgifterna kan inte heller användas för att ta fram information om sådana tredje parter och skapa specifika profiler, även om deras personuppgifter redan finns hos den personuppgiftsansvarige. En sådan behandling skulle sannolikt vara olaglig och orättvis, särskilt om de berörda tredje parterna inte har underrättats och inte kan utöva sina rättigheter som registrerade.

Vidare är det vedertagen praxis bland alla personuppgiftsansvariga (både ”översändande” och ”mottagande” parter) att ha verktyg som gör det möjligt för registrerade att välja ut de relevanta uppgifter de vill få ut och överföra och, i förekommande fall, undanta andra personers uppgifter. Detta kommer ytterligare att minska riskerna för tredje parter vars personuppgifter eventuellt överförs.

De personuppgiftsansvariga bör dessutom tillämpa en samtyckesmekanism för andra berörda personer, för att göra det lättare att överföra uppgifter i situationer där parterna är villiga att ge sitt samtycke, t.ex. om de också vill flytta sina uppgifter till någon annan personuppgiftsansvarig. En sådan situation kan t.ex. uppstå i samband med sociala nätverk, men det är upp till de personuppgiftsansvariga att bestämma vilken vedertagen praxis som ska följas.

²³ En social nätverkstjänst bör inte göra sina medlemmars profil mer omfattande genom att använda personuppgifter som överförts av en registrerad som ett led i hans eller hennes rätt till dataportabilitet, om de inte respekterar öppenhetensprincipen och även ser till att den specifika behandlingen grundas på en lämplig rättslig grund.

Uppgifter som omfattas av immateriell äganderätt och affärshemligheter:

Andras rättigheter och friheter nämns i artikel 20.4. Även om detta inte direkt kan kopplas till portabilitet kan det förstås som ”inklusive affärshemligheter eller immateriell äganderätt och särskilt den upphovsrätt som skyddar programvaran”. Även om dessa rättigheter bör beaktas innan man svarar på en begäran om dataportabilitet, ”bör dessa överväganden inte resultera i en vägran att tillhandahålla information till den registrerade”. Den personuppgiftsansvarige bör dessutom inte avslå en begäran om dataportabilitet på grund av att en annan avtalsrättslig rättighet kränks (exempelvis en utestående skuld, eller en handelskonflikt med den registrerade).

Rätten till dataportabilitet ger inte en enskild rätt att missbruka informationen på ett sätt som kan klassificeras som en orättvis praxis eller ett intrång i immateriella rättigheter.

En potentiell affärsrisk får dock inte i sig anföras som skäl för att inte besvara en begäran om dataportabilitet, och personuppgiftsansvariga kan överföra personuppgifter som tillhandahållits av registrerade i ett format som inte röjer information som omfattas av affärshemligheter eller immateriella rättigheter.

IV. Hur ska de allmänna bestämmelserna om utövande av registrerades rättigheter tillämpas på dataportabilitet?

- Vilken förhandsinformation ska den registrerade ges?

För att iakttä den nya rätten till dataportabilitet måste personuppgiftsansvariga informera registrerade om att denna nya rätt till portabilitet finns. Om de berörda uppgifterna samlas in direkt från den registrerade måste detta ske ”när personuppgifterna erhålls”. Om personuppgifterna inte har erhållits från den registrerade måste den personuppgiftsansvarige tillhandahålla den information som krävs enligt artikel 13.2 b och artikel 14.2 c.

Om personuppgifterna inte har erhållits från den registrerade ska informationen enligt artikel 14.3 tillhandahållas inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad från det att uppgifterna erhållits, vid tidpunkten för den första kommunikationen eller när uppgifterna lämnas ut till tredje part.²⁴

När personuppgiftsansvariga tillhandahåller den erforderliga informationen måste de säkerställa att de skiljer mellan rätten till dataportabilitet och andra rättigheter. Artikel 29-arbetsgruppen rekommenderar därför att personuppgiftsansvariga tydligt förklarar skillnaderna mellan de typer av uppgifter som en registrerad kan få ut via rätten till tillgång och rätten till dataportabilitet.

Arbetsgruppen rekommenderar dessutom att personuppgiftsansvariga alltid inkluderar information om rätten till dataportabilitet innan registrerade avslutar eventuella konton. Detta gör det möjligt för användare att få en uppfattning om sina personuppgifter och enkelt överföra uppgifterna till sin egen enhet eller till en annan leverantör innan ett avtal sägs upp.

Som ett exempel på god praxis för ”mottagande” personuppgiftsansvariga rekommenderar artikel 29-arbetsgruppen slutligen att registrerade ges fullständig information om naturen på

²⁴ Enligt artikel 12 ska personuppgiftsansvariga tillhandahålla ”all kommunikation [...] i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn”.

personuppgifter som är relevant för utförandet av deras tjänster. Detta understryker inte bara vikten av rättvis behandling utan ger användare möjlighet att begränsa riskerna för tredje parter och all annan onödig dubbling av personuppgifter, även när ingen annan registrerad är inblandad.

- **Hur kan den personuppgiftsansvarige identifiera den registrerade innan den personuppgiftsansvarige svarar på den registrerades begäran?**

Dataskyddsförordningen innehåller inte några preskriptiva krav på hur autentiseringen av registrerade ska gå till. I artikel 12.2 i dataskyddsförordningen anges dock att den personuppgiftsansvarige inte får vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter (inbegripet rätten till dataportabilitet) om inte den personuppgiftsansvarige behandlar personuppgifter för ett ändamål som inte kräver att en registrerad identifieras och den personuppgiftsansvarige kan visa att han eller hon inte är i stånd att identifiera den registrerade. Enligt artikel 11.2 kan emellertid den registrerade i en sådan situation tillhandahålla ytterligare information som gör identifieringen möjlig. I artikel 12.6 föreskrivs dessutom att om en personuppgiftsansvarig har rimliga skäl att betvivla identiteten hos en registrerad kan den personuppgiftsansvarige begära ytterligare information som gör identifieringen av den registrerade möjlig. Om en registrerad tillhandahåller ytterligare information som gör identifiering möjlig får den personuppgiftsansvarige inte vägra att tillmötesgå en sådan begäran. Om information och uppgifter som samlats in på nätet kopplas till pseudonymer eller unika identifikatorer kan personuppgiftsansvariga tillämpa lämpliga förfaranden för att göra det möjligt för en person att lämna en begäran om dataportabilitet och få ut uppgifter som rör honom eller henne. I alla händelser måste personuppgiftsansvariga tillämpa ett autentiseringsförfarande för att utan tvivel kunna fastställa identiteten på en registrerad som begär att få ut sina personuppgifter eller mer allmänt utövar de rättigheter som han eller hon tillförsäkrats genom dataskyddsförordningen.

Sådana förfaranden finns ofta redan. Den personuppgiftsansvarige autentiserar ofta de registrerade redan innan de ingår ett avtal eller innan deras samtycke till behandlingen inhämtas. De personuppgifter som används för att registrera den person som berörs av behandlingen kan följaktligen även användas för att autentisera den registrerade för portabilitetsändamål.²⁵

Även om den tidigare identifieringen av de registrerade i en sådan situation kan kräva en begäran om att de ska styrka sin juridiska identitet, är en sådan verifiering kanske inte relevant för att bedöma kopplingen mellan uppgifterna och den berörda personen. En sådan koppling har nämligen inget att göra med den officiella eller juridiska identiteten. Den personuppgiftsansvariges möjlighet att begära ytterligare information för att bedöma någons identitet får med andra ord inte leda till överdrivna krav och till insamling av personuppgifter som inte är relevanta eller nödvändiga för att styrka kopplingen mellan den enskilda personen och de begärda personuppgifterna.

I många fall finns det redan sådana autentiseringsförfaranden. Användarnamn och lösenord används exempelvis ofta för att göra det möjligt för enskilda att få tillgång till sina uppgifter i e-postkonton, sociala nätverkskonton och konton som används för en mängd andra tjänster,

²⁵ När behandlingen av uppgifterna exempelvis är kopplad till ett användarkonto kan det räcka att relevant användarnamn och lösenord tillhandahålls för att den registrerade ska kunna identifieras.

varav några som personer väljer att använda utan att avslöja sitt fullständiga namn eller sin identitet.

Om omfattningen av de uppgifter som den registrerade begärt gör det svårt att överföra uppgifterna via internet kan den personuppgiftsansvariga, i stället för att förlänga fristen för att tillmötesgå begäran med upp till tre månader²⁶, även vara tvungen att överväga alternativa metoder för att tillhandahålla uppgifterna. Det kan exempelvis handla om att använda sig av strömning eller om att spara uppgifterna på en cd, dvd eller något annat fysiskt medium som gör det möjligt att överföra personuppgifterna direkt till en annan personuppgiftsansvarig (enligt artikel 20.2 i dataskyddsförordningen när detta är tekniskt möjligt).

- Vad är tidsfristen för att besvara en portabilitetsbegäran?

I artikel 12.3 anges att den personuppgiftsansvarige ”utan onödigt dröjsmål” och under alla omständigheter ”senast en månad efter att ha mottagit begäran” ska tillhandahålla den registrerade ”information om de åtgärder som vidtagits”. Denna period får förlängas i upp till tre månader vid en komplicerad begäran, förutsatt att den registrerade har underrättats om skälen till förseningen inom en månad från den ursprungliga begäran.

Personuppgiftsansvariga som tillhandahåller it-tjänster är sannolikt bättre rustade att snabbt tillmötesgå en begäran. För att möta användares förväntningar är det i regel god praxis att definiera inom vilka tidsramar en begäran om dataportabilitet vanligtvis besvaras och meddela de registrerade detta.

Personuppgiftsansvariga som vägrar att besvara en begäran om portabilitet ska enligt artikel 12.4 informera den registrerade om ”orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning” senast en månad efter att ha mottagit begäran.

Personuppgiftsansvariga måste respektera skyldigheten att svara inom en viss tid, även om begäran avslås. Med andra ord får inte den personuppgiftsansvarige underlåta att agera när han eller hon ombeds att besvara en begäran om dataportabilitet.

- När kan en begäran om dataportabilitet avslås eller en avgift tas ut?

Artikel 12 förbjuder den personuppgiftsansvarige att ta ut en avgift för att tillhandahålla personuppgifterna, om inte den personuppgiftsansvarige kan visa att begärandena är uppenbart oggrundade eller orimliga, ”särskilt på grund av deras repetitiva art”. För it-tjänster som specialiserar sig på automatiserad behandling av personuppgifter kan automatiserade system som gränssnitt för tillämpningsprogram (API)²⁷ underlätta utbytet med de registrerade, och således minska de bördor som repetitiva begäranden kan resultera i. Därför bör det endast i undantagsfall vara möjligt för den personuppgiftsansvarige att motivera en vägran att lämna ut den begärda informationen, även vid en stor mängd olika begäranden om dataportabilitet.

²⁶ Artikel 12.3: ”Den personuppgiftsansvarige ska [...] tillhandahålla den registrerade information om de åtgärder som vidtagits”.

²⁷ Med gränssnitt för tillämpningsprogram (API) avses de gränssnitt för tillämpningsprogram eller webbtjänster som den personuppgiftsansvarige ställer till förfogande så att andra system eller tillämpningsprogram kan kopplas till och fungera ihop med deras system.

Dessutom ska den samlade kostnaden för att besvara begäranden om dataportabilitet inte beaktas för att avgöra om en begäran är orimlig. Artikel 12 i dataskyddsförordningen inriktas nämligen på begäranden från en registrerad och inte på det totala antalet begäranden som en personuppgiftsansvarig tar emot. Av detta följer att de totala genomförandekostnaderna varken bör tas ut av registrerade eller användas för att motivera en vägran att besvara begäranden om dataportabilitet.

V. Hur ska de flyttbara uppgifterna tillhandahållas?

- Vilka metoder förväntas den personuppgiftsansvarige använda för att tillhandahålla uppgifter?

Enligt artikel 20.1 i dataskyddsförordningen har registrerade rätt att överföra uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta.

Sådana hinder kan utgöras av juridiska, tekniska eller ekonomiska hinder som den personuppgiftsansvarige har skapat för att inte bevilja eller försena den registrerades eller en annan personuppgiftsansvarigs tillgång, överföring eller vidareutnyttjande. Exempel på sådana hinder är avgifter för att lämna ut uppgifter, bristande kompatibilitet eller tillgång till ett dataformat eller gränssnitt för tillämpningsprogram eller det tillhandahållna formatet, orimliga förseningar eller åtgärder som gör det orimligt svårt att ta fram hela uppsättningen uppgifter, medvetet göra uppsättningen uppgifter förvillande eller specifika och otillbörliga eller orimliga sektoriella standardiserings- eller ackrediteringskrav.²⁸

I artikel 20.2 åläggs personuppgiftsansvariga dessutom att överföra de flyttbara uppgifterna direkt till andra personuppgiftsansvariga ”när detta är tekniskt möjligt”.

Frågan om det är tekniskt möjligt att överföra uppgifter från en personuppgiftsansvarig till en annan, under den registrerades kontroll, bör bedömas från fall till fall. I skäl 68 görs ett ytterligare förtydligande av gränserna för vad som är ”tekniskt möjligt” och anges att rätten att överföra och ta emot uppgifter inte innebär ”någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla”.

Personuppgiftsansvariga förväntas överföra personuppgifter i ett kompatibelt format, även om detta inte innebär att andra personuppgiftsansvariga är skyldiga att stödja dessa format. Direkt överföring från en personuppgiftsansvarig till en annan skulle därför kunna ske när kommunikation mellan två system är möjlig, på ett säkert sätt²⁹, och när det mottagande systemet rent tekniskt är i stånd att ta emot de inkommande uppgifterna. Om tekniska begränsningar omöjliggör direkt överföring ska den personuppgiftsansvariga förklara dessa begränsningar för de registrerade, eftersom hans eller hennes beslut annars får en liknande effekt som en vägran att vidta åtgärder på den registrerades begäran (artikel 12.4).

²⁸ Vissa berättigade hinder kan förekomma, exempelvis de hinder kopplade till andras rättigheter och friheter som nämns i artikel 20.4 eller hinder kopplade till säkerheten i den personuppgiftsansvariges egna system. Det ankommer på den personuppgiftsansvarige att motivera varför sådana hinder är berättigade och varför de inte utgör hinder i den mening som avses i artikel 20.1.

²⁹ Genom en autentiserad kommunikation med lämplig krypteringsnivå.

På en teknisk nivå bör personuppgiftsansvariga undersöka och bedöma två olika och kompletterande metoder för att göra flyttbara uppgifter tillgängliga för registrerade eller andra personuppgiftsansvariga:

- Direkt överföring av hela uppsättningen flyttbara uppgifter (eller flera utdrag ur hela uppsättningen uppgifter).
- Ett automatiseringsverktyg som gör det möjligt att extrahera relevanta uppgifter.

Den andra metoden kan eventuellt vara att föredra för personuppgiftsansvariga i ärenden som rör komplexa och stora uppsättningar uppgifter, eftersom den gör det möjligt att extrahera varje del av uppsättningen uppgifter som är relevant för den registrerade i samband med hans eller hennes begäran. Metoden kan dessutom bidra till att minimera riskerna och göra det möjligt att använda synkroniseringsmekanismer³⁰ (t.ex. i samband med regelbunden kommunikation mellan personuppgiftsansvariga). Detta skulle kunna vara ett bättre sätt att säkerställa efterlevnaden för den ”nya” personuppgiftsansvarige, och ett bra sätt för den ursprungliga personuppgiftsansvarige att minska integritetsriskerna.

Dessa två och eventuellt kompletterande metoder för att tillhandahålla relevanta flyttbara uppgifter kan genomföras genom att göra uppgifter tillgängliga på olika sätt, exempelvis med hjälp av säker meddelandehantering (secure messaging), en SFTP-server, ett säkert webbaserat gränssnitt för tillämpningsprogram (WebAPI) eller en webbportal. Registrerade bör ges möjlighet att använda en lagringsplats för personuppgifter, ett system för personlig informationshantering³¹ eller andra former av betrodda tredje parter, för att inneha och lagra personuppgifterna och bevilja personuppgiftsansvariga åtkomst till och tillåtelse att behandla personuppgifterna när så krävs.

- **Vad är det förväntade dataformatet?**

Genom dataskyddsförordningen åläggs personuppgiftsansvariga att tillhandahålla de personuppgifter som en person har begärt i ett format som stöder vidareutnyttjande. Framför allt anges det i artikel 20.1 i dataskyddsförordningen att personuppgifter ska tillhandahållas ”i ett strukturerat, allmänt använt och maskinläsbart format”. I skäl 68 förtydligas detta ytterligare genom att det slås fast att detta format bör vara kompatibelt, ett begrepp som i EU definierats³² på följande sätt:

förmågan hos olika och olikartade organisationer att interagera i riktning mot ömsesidigt fördelaktiga och överenskomna gemensamma mål, inbegripet informations- och kunskapsdelning mellan organisationerna via de verksamhetsprocesser de stöder, genom utbyte av uppgifter mellan deras respektive IKT-system.

Begreppen ”strukturerat”, ”allmänt använt” och ”maskinläsbart” är minimikrav som bör underlätta kompatibiliteten hos det dataformat som den personuppgiftsansvariga

³⁰ En synkroniseringsmekanism kan bidra till att fullgöra de allmänna skyldigheterna enligt artikel 5 i dataskyddsförordningen, nämligen att personuppgifterna ”ska vara korrekta och (...) uppdaterade”.

³¹ För system för personlig informationshantering (PIMS), se exempelvis EDPS yttrande 9/2016 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 Europaparlamentets och rådets beslut nr 922/2009/EG av den 16 september 2009 om lösningar för att uppnå interoperabilitet mellan europeiska offentliga förvaltningar (ISA) (EUT L 260, 3.10.2009, s. 20).

tillhandahåller uppgifterna i. I så mening är ”strukturerat, allmänt använt och maskinläsbart” en specificering av medlen, medan kompatibiliteten är det eftersträlvade målet.

I skäl 21 i direktiv 2013/37/EU^{33,34} definieras ”maskinläsbart format” på följande sätt:

ett filformat som är strukturerat på så sätt att datorprogram enkelt kan identifiera, känna igen och extrahera specifika uppgifter, inklusive enskilda faktauppgifter, och dessas interna struktur. Maskinläsbara data är data kodade i filer som är strukturerade i ett maskinläsbart format. Maskinläsbara format kan vara öppna eller proprietära; de kan, men behöver inte, vara formella standarder. Handlingar bör inte anses vara i maskinläsbart format om de är kodade i ett filformat som begränsar automatisk behandling på grund av att data inte alls, eller endast med svårighet, kan extraheras från dessa handlingar. Medlemsstaterna bör, när så är lämpligt, uppmuntra användningen av öppna, maskinläsbara format.

Eftersom en mängd olika uppgiftstyper skulle kunna behandlas av en personuppgiftsansvarig föreskriver dataskyddsförordningen inte några särskilda rekommendationer om formatet på de personuppgifter som ska tillhandahållas. Vilket format som är lämpligast kommer att variera mellan olika sektorer, och det kan redan finnas lämpliga format. I så fall bör dessa alltid väljas för att uppfylla målet om tolkningsbarhet och ge den registrerade en hög grad av dataportabilitet. Format som omfattas av dyra licensieringsbegränsningar ska inte anses lämpliga.

I skäl 68 förtydligas att ”[d]en registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla”. **Syftet med portabiliteten är därför att skapa driftskompatibla system, inte fullständigt kompatibla system.**³⁵

Personuppgifter förväntas tillhandahållas i format med en hög abstraktionsnivå i förhållande till interna proprietära format. Dataportabilitet innebär därför en extra behandlingsnivå för de personuppgiftsansvariga. De måste nämligen extrahera uppgifter från plattformen och filtrera bort personuppgifter som faller utanför tillämpningsområdet för portabiliteten, som t.ex. avledda uppgifter eller uppgifter som rör systemsäkerhet. På detta sätt uppmuntras personuppgiftsansvariga att i förväg identifiera uppgifter som faller inom tillämpningsområdet för portabilitet i deras egna system. Denna extra behandling av uppgifterna betraktas som ett komplement till huvudbehandlingen, eftersom den inte genomförs för att uppfylla ett nytt ändamål som definierats av den personuppgiftsansvarige.

När inga format är allmänt använda inom en viss sektor eller ett visst sammanhang, **bör personuppgiftsansvariga tillhandahålla personuppgifter med hjälp av allmänt använda öppna format (t.ex. XML, JSON, CSV osv.) tillsammans med användbara metadata med maximal detaljrikedom**, och samtidigt behålla en hög abstraktionsnivå. Metadata bör därför användas för att på ett korrekt sätt beskriva betydelsen av den information som utbyts.

³³ Om ändring av direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn.

³⁴ I EU-ordlistan (<http://eur-lex.europa.eu/eli-register/glossary.html>) ges ytterligare förtydliganden av de begrepp som används i denna vägledning, som t.ex. maskinläsbar, kompatibilitet, öppet format, standard, metadata.

³⁵ I ISO/IEC 2382-01 definieras driftskompatibilitet som olika enheters förmåga att kommunicera, köra program eller överföra data på ett sätt som innebär att användaren behöver liten eller ingen kännedom om dessa enheters unika egenskaper.

Metadatan bör vara tillräcklig för att använda uppgifterna i avsett syfte och vidareutnyttja dem, dock givetvis utan att avslöja affärshemligheter. Om en person tillhandahålls PDF-versioner av en e-postbrevlåda är detta sannolikt inte tillräckligt strukturerat och beskrivande för att enkelt kunna vidareutnyttja uppgifterna i e-postbrevlådan. E-postuppgifterna bör i stället tillhandahållas i ett format som bevarar alla metadata, så att uppgifterna verkligen kan vidareutnyttjas. När den personuppgiftsansvarige väljer i vilket format personuppgifterna ska tillhandahållas bör han eller hon därför ta hänsyn till hur detta format skulle hindra den enskilda personens rätt att vidareutnyttja uppgifterna. Om en personuppgiftsansvarig kan ge den registrerade ett val beträffande i vilket format denne vill få ut personuppgifterna bör en tydlig förklaring av vilka effekter valet får tillhandahållas. Att behandla ytterligare metadata endast för att dessa eventuellt kan behövas eller vara önskvärda för att besvara en begäran om dataportabilitet utgör inte en berättigad grund för en sådan behandling.

Artikel 29-arbetsgruppen förordar starkt samarbete mellan intressenter inom sektorn och branschorganisationer för att tillsammans ta fram en gemensam uppsättning kompatibla standarder och format för att uppfylla de krav som rätten till dataportabilitet innebär. Denna utmaning har även diskuterats av den europeiska interoperabilitetsramen (EIF) som har kommit överens om en interoperabilitetsstrategi för organisationer som gemensamt vill tillhandahålla offentliga tjänster. Inom ramen för sitt tillämpningsområde fastställer interoperabilitetsramen en uppsättning gemensamma inslag som t.ex. vokabulär, begrepp, principer, policyer, riktlinjer, rekommendationer, standarder, specifikationer och praxis.³⁶

- Hur ska en stor eller komplicerad insamling av personuppgifter hanteras?

I dataskyddsförordningen förklaras inte hur man ska klara den utmaning som det innebär att besvara en begäran om dataportabilitet som rör insamling av stora mängder uppgifter, uppgifter med en komplicerad struktur eller andra tekniska frågor som kan skapa problem för personuppgiftsansvariga eller registrerade.

Det är emellertid alltid viktigt att den enskilde verkligen förstår definitionen av, formen på och strukturen hos de personuppgifter som den personuppgiftsansvarige skulle kunna tillhandahålla. Uppgifter kan t.ex. inledningsvis tillhandahållas i en översiktlig form med hjälp av resultattavlor som gör det möjligt för den registrerade att flytta en deluppsättning personuppgifter snarare än alla uppgifter. Den personuppgiftsansvarige bör ge en översikt över uppgifterna ”i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk” (se artikel 12.1 i dataskyddsförordningen) på ett sådant sätt att den registrerade alltid har klart för sig vilka uppgifter som han eller hon kan ladda ned eller överföra till en annan personuppgiftsansvarig för ett visst ändamål. Registrerade bör t.ex. ha möjlighet att använda programapplikationer som gör det lätt att identifiera, känna igen och behandla specifika uppgifter.

En praktisk metod som en personuppgiftsansvarig kan använda sig av för att besvara begäranden om dataportabilitet kan som påpekades ovan vara att erbjuda en lämpligt säkrat och dokumenterat gränssnitt för tillämpningsprogram. Detta skulle kunna göra det möjligt för enskilda att hos den personuppgiftsansvariga begära att få ut sina personuppgifter via sitt eget eller en tredje parts program eller ge andra tillåtelse att göra detta för deras räkning (inbegripet en annan personuppgiftsansvarig) i enlighet med artikel 20.2 i

³⁶ Källa: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

dataskyddsförordningen. Genom att bevilja tillgång till uppgifter via ett externt åtkomligt gränssnitt för tillämpningsprogram kan dessutom ett mer sofistikerat åtkomstsystem eventuellt tillhandahållas, som gör det möjligt för enskilda att senare inte ytterligare begäranden om uppgifter, antingen i form av komplett nedladdning eller som en deltafunktion som endast innehåller de ändringar som gjorts sedan den senaste nedladdningen, utan att den börda som dessa ytterligare begäranden resulterar i blir alltför betungande för den personuppgiftsansvarige.

- Hur kan flyttbara uppgifter säkras?

Enligt artikel 5.1 f i dataskyddsförordningen bör personuppgiftsansvariga i regel garantera ”lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder”.

Överföringen av personuppgifter till den personuppgiftsansvarige kan också ge upphov till en del säkerhetsproblem:

Hur kan personuppgiftsansvariga säkerställa att personuppgifter lämnas på ett säkert sätt till rätt person?

Eftersom syftet med dataportabilitet är att få ut personuppgifter från den personuppgiftsansvariges informationssystem kan överföringen av dessa uppgifter bli en tänkbar riskkälla (framför allt när det gäller personuppgiftsincidenter under överföringen). Den personuppgiftsansvarige ansvarar för att vidta alla säkerhetsåtgärder som behövs för att inte bara säkerställa att alla personuppgifter överförs på ett säkert sätt (med hjälp av kryptering från början till slut eller datakryptering) och till rätt destination (med hjälp av starka autentiseringsåtgärder), utan även för att fortsätta att skydda de personuppgifter som finns kvar i systemet och tillämpa transparenta förfaranden för att hantera eventuella personuppgiftsincidenter.³⁷ Personuppgiftsansvariga bör därför bedöma de särskilda risker som är kopplade till dataportabilitet och vidta lämpliga åtgärder för att reducera riskerna.

Om den registrerade redan måste autentiseras kan sådana riskreduceringsåtgärder inbegripa användning av ytterligare autentiseringsinformation (som t.ex. en delad hemlighet), eller en annan autentiseringsfaktor (som t.ex. ett engångslösenord), uppskjutning eller frysning av överföringen vid misstanke om att kontot har komprometterats. Vid en direkt överföring från en personuppgiftsansvarig till en annan bör autentisering genom mandat, exempelvis tokenbaserad autentisering, användas.

Sådana säkerhetsåtgärder får inte till sin natur vara hämmande och får inte hindra användare från att utöva sina rättigheter, t.ex. genom att påföra dem ytterligare kostnader.

Hur ska man hjälpa användare att säkra lagringen av sina personuppgifter i sina egna system?

När användare tar fram personuppgifter från en nättjänst finns det alltid en risk för att användarna lagrar dem i ett mindre säkert system än det system som används av tjänsten i fråga. Den registrerade som begär ut uppgifterna ansvarar för att identifiera de rätta åtgärderna för att säkra personuppgifter i sitt eget system. Han eller hon bör emellertid

³⁷ I enlighet med direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

uppmärksammas på problemet för att kunna vidta åtgärder för att skydda den information som har erhållits. Som ett exempel på ledande praxis kan personuppgiftsansvariga också rekommendera lämpliga format, krypteringsverktyg och andra säkerhetsåtgärder för att hjälpa den registrerade att uppfylla detta mål.

* * *

Utfärdade i Bryssel den 13 december 2016

På arbetsgruppens vägnar
Isabelle Falque-Pierrotin
Ordförande

Senast reviderade och antagna den 5 april 2017

På arbetsgruppens vägnar
Isabelle Falque-Pierrotin
Ordförande