Riktlinjer 01/2022 om registrerades rättigheter – rätt till tillgång

Version 2.1

Antaget den 28 mars 2023

Versionshistorik

Version 1.0	18.1.2022	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	28.3.2023	Antagande av riktlinjerna efter offentligt samråd
Version 2.1	30.5.2024	Mindre korrigeringar

SAMMANFATTNING

De registrerades rätt till tillgång fastställs i artikel 8 i EU-stadgan om de grundläggande rättigheterna. Den har från början varit en del av EU:s rättsliga ram för dataskydd och vidareutvecklas nu genom mer specifika och exakta regler i artikel 15 i den allmänna dataskyddsförordningen.

Syfte och övergripande struktur för rätten till tillgång

Det övergripande syftet med rätten till tillgång är att tillhandahålla enskilda personer tillräcklig, öppen och lättillgänglig information om behandlingen av deras personuppgifter, så att de är medvetna om behandlingen, kan kontrollera att den är laglig samt kan kontrollera att de behandlade uppgifterna är korrekta. Detta kommer att göra det enklare – utan att vara ett villkor – för den enskilde att utöva andra rättigheter, t.ex. rätten till radering eller rättelse.

Rätten till tillgång enligt dataskyddslagstiftningen ska skiljas från liknande rättigheter i andra syften, till exempel rätten till tillgång till offentliga handlingar som syftar till att garantera insyn i offentliga myndigheters beslutsfattande och god förvaltningssed.

Den registrerade behöver däremot inte ange skäl för sin begäran om tillgång och det är inte den personuppgiftsansvariges sak att utreda huruvida denna begäran faktiskt kommer att hjälpa den registrerade att kontrollera att den relevanta behandlingen eller utövandet av andra rättigheter är lagliga. Den personuppgiftsansvarige måste behandla begäran om det inte är uppenbart att begäran görs enligt andra regler än dataskyddsregler.

Rätten till tillgång omfattar följande tre olika komponenter:

- Bekräftelse av huruvida uppgifter om personen har behandlats eller inte.
- Tillgång till dessa personuppgifter.
- Tillgång till information om behandlingen, t.ex. ändamål, kategorier av uppgifter och mottagare, behandlingens varaktighet, de registrerades rättigheter och lämpliga skyddsåtgärder vid överföringar till tredjeland.

Allmänna överväganden om bedömningen av den registrerades begäran

Vid analysen av innehållet i begäran måste den personuppgiftsansvarige bedöma om begäran rör personuppgifter för den person som gör begäran, om begäran omfattas av artikel 15 och om det finns andra, mer specifika, bestämmelser som reglerar tillgången inom en viss sektor. Denne måste också bedöma om begäran avser alla eller endast delar av de uppgifter som behandlas om den registrerade.

Det finns inga särskilda krav på hur begäran ska utformas. Den personuppgiftsansvarige bör tillhandahålla lämpliga och användarvänliga kommunikationskanaler som enkelt kan användas av den registrerade. Den registrerade behöver dock inte använda just dessa kanaler utan kan i stället skicka begäran till den personuppgiftsansvariges officiella kontaktpunkt. Den personuppgiftsansvarige är inte skyldig att agera på begäranden som skickas till slumpmässiga eller uppenbart felaktiga adresser.

Om den personuppgiftsansvarige inte kan identifiera uppgifter som avser den registrerade ska denne informera den registrerade om detta och får vägra tillgång, såvida inte den registrerade tillhandahåller ytterligare information som möjliggör identifiering. Om den personuppgiftsansvarige dessutom hyser tvivel om huruvida den registrerade är den som han eller hon påstår sig vara, får den personuppgiftsansvarige begära ytterligare information för att fastställa den registrerades identitet.

Begäran om ytterligare information måste stå i proportion till den typ av uppgifter som behandlas, den skada som kan uppstå osv. för att undvika orimlig uppgiftsinsamling.

Tillämpningsområdet för rätten till tillgång

Tillämpningsområdet för rätten till tillgång bestäms av begreppet personuppgifter enligt definitionen i artikel 4.1 i dataskyddsförordningen. Förutom grundläggande personuppgifter såsom namn, adress, telefonnummer osv. kan ett stort antal uppgifter omfattas av denna definition, såsom medicinska uppgifter, inköpshistoria, kreditvärdighetsindikatorer, aktivitetsloggar, sökaktiviteter osv. Personuppgifter som har genomgått pseudonymisering är fortfarande personuppgifter, i motsats till anonymiserade uppgifter. Rätten till tillgång avser personuppgifter om den person som gör begäran. Detta bör inte tolkas alltför restriktivt och kan omfatta uppgifter som även rör andra personer, till exempel kommunikationshistorik över inkommande och utgående meddelanden.

Utöver att ge tillgång till personuppgifterna måste den personuppgiftsansvarige lämna ytterligare information om behandlingen och de registrerades rättigheter. Sådan information kan baseras på vad som redan har sammanställts i den personuppgiftsansvariges register över behandling (artikel 30 i dataskyddsförordningen) och i meddelandet om skydd av personuppgifter (artiklarna 13 och 14 i dataskyddsförordningen). Denna allmänna information kan dock behöva uppdateras vid tidpunkten för begäran eller skräddarsys så att den återspeglar den behandling som utförs i förhållande till den specifika person som gör begäran.

Hur man ger tillgång

Metoderna för att ge tillgång kan variera beroende på mängden uppgifter och komplexiteten i den behandling som utförs. Om inget annat uttryckligen anges ska begäran anses gälla *samtliga* personuppgifter som rör den registrerade, men den personuppgiftsansvarige får be att den registrerade preciserar sin begäran om en stor mängd uppgifter behandlas.

Den personuppgiftsansvarige måste söka efter personuppgifter i alla it-system och register som inte är it-system, baserat på sökkriterier som återspeglar hur informationen är strukturerad, till exempel namn och kundnummer. Förmedlingen av uppgifter och annan information om behandlingen måste tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. De mer exakta kraven i detta avseende beror på omständigheterna kring behandlingen av uppgifterna och den registrerades förmåga att uppfatta och förstå kommunikationen (t.ex. med beaktande av om den registrerade är ett barn eller en person med särskilda behov). Om uppgifterna består av koder eller andra ”rådata” kan dessa behöva förklaras för att den registrerade ska förstå.

Den huvudsakliga metoden för att ge tillgång är att den registrerade får en kopia på sina uppgifter, men andra metoder (t.ex. muntlig information och tillgång till webbplatser) kan planeras på förhand om den registrerade begär det. Uppgifterna kan skickas via e-post, förutsatt att alla nödvändiga skyddsåtgärder tillämpas, med hänsyn till exempelvis uppgifternas art, eller på andra sätt, som ett självbetjäningsverktyg.

När det rör sig om stora mängder uppgifter och det skulle vara svårt för den registrerade att förstå informationen om den gavs i en enda volym – särskilt online – kan den lämpligaste åtgärden vara en skiktad strategi. Tillhandahållande av informationen i olika lager kan underlätta den registrerades förståelse av uppgifterna. Den personuppgiftsansvarige måste kunna visa att den skiktade strategin har ett mervärde för den registrerade och alla skikt bör tillhandahållas samtidigt om den registrerade väljer det.

Kopian av uppgifterna och kompletterande information bör tillhandahållas i en beständig form, t.ex. skriftlig text, som kan vara i ett elektroniskt format som är allmänt använt, så att den registrerade enkelt kan ladda ned den. Uppgifterna kan lämnas som en utskrift eller sammanställning så länge som all information finns med och detta inte ändrar eller modifierar innehållet i informationen.

Begäran ska tillmötesgås snarast och under alla omständigheter inom en månad från mottagandet av begäran. Den perioden kan vid behov förlängas med ytterligare två månader, beroende på hur komplicerad begäran är och antalet inkomna begäranden. Den registrerade måste i sådant fall informeras om orsaken till dröjsmålet. Den personuppgiftsansvarige måste vidta de åtgärder som krävs för att hantera begäranden så snart som möjligt och anpassa dessa åtgärder till förutsättningarna för behandlingen. Om uppgifter endast lagras under en mycket kort period måste det finnas åtgärder som garanterar att en begäran om tillgång kan tillmötesgås utan att uppgifterna raderas under tiden som begäran behandlas. Om en stor mängd uppgifter behandlas måste den personuppgiftsansvarige införa rutiner och mekanismer som är anpassade till behandlingens komplexitet.

Bedömningen av begäran bör återspegla situationen vid den tidpunkt då begäran mottogs av den personuppgiftsansvarige. Även uppgifter som kan vara felaktiga eller olagligt behandlade ska lämnas ut. Uppgifter som redan har tagits bort, till exempel i enlighet med en policy för lagring, och därför inte längre är tillgängliga för den personuppgiftsansvarige, kan inte tillhandahållas.

Begränsningar

Dataskyddsförordningen medger vissa begränsningar av rätten till tillgång. Det finns inga ytterligare undantag eller inskränkningar. Rätten till tillgång saknar en allmän reservation mot proportionalitetsprincipen när det gäller de ansträngningar som den personuppgiftsansvarige måste göra för att tillmötesgå den registrerades begäran.

Enligt artikel 15.4 ska rätten att erhålla en kopia inte inverka menligt på andras rättigheter och friheter. Europeiska dataskyddsstyrelsen EDPB anser att dessa rättigheter måste beaktas, inte bara när tillgång beviljas genom att en kopia tillhandahålls, utan även när tillgång till uppgifter tillhandahålls på annat sätt (till exempel på plats). Artikel 15.4 är dock inte tillämplig på den ytterligare information om behandlingen som anges i artikel 15.1 a–h. Den personuppgiftsansvarige måste kunna påvisa att andras rättigheter och friheter skulle påverkas menligt i den konkreta situationen. Om artikel 15.4 tillämpas bör det inte leda till att den registrerades begäran avvisas helt och hållet. Det skulle endast leda till att man utelämnar eller gör de delar oläsliga som kan ha negativa effekter på andras rättigheter och friheter.

Enligt artikel 12.5 i dataskyddsförordningen får personuppgiftsansvariga avvisa begäranden som är uppenbart ogrundade eller orimliga, eller ta ut en rimlig avgift för sådana begäranden. Dessa begrepp måste tolkas snävt. Eftersom det är mycket få förutsättningar som är nödvändiga för begäranden om tillgång är utrymmet för att betrakta en begäran som uppenbart ogrundad ganska begränsat. Orimliga begäranden beror på särdragen i den sektor där den personuppgiftsansvarige är verksam. Ju oftare ändringar görs i den personuppgiftsansvariges databas, desto oftare kan den registrerade få begära tillgång utan att det är orimligt. I stället för att vägra tillgång får den personuppgiftsansvarige besluta att ta ut en avgift av den registrerade. Detta skulle endast vara relevant vid orimliga begäranden, för att täcka de administrativa kostnader som sådana begäranden kan orsaka. Den personuppgiftsansvarige måste kunna visa att en begäran är uppenbart ogrundad eller orimlig.

Begränsningar av rätten till tillgång kan också finnas i medlemsstaternas nationella lagstiftning enligt artikel 23 i dataskyddsförordningen och undantagen i denna. Personuppgiftsansvariga som avser att stödja sig på sådana restriktioner måste noggrant kontrollera kraven i de nationella bestämmelserna

och ta hänsyn till eventuella särskilda villkor. Sådana villkor kan vara att rätten till tillgång endast tillfälligt fördröjs eller att begränsningen endast gäller vissa kategorier av uppgifter.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen.

Det förberedande arbetet med dessa riktlinjer omfattade inhämtande av synpunkter från intressenter, både skriftligen och vid ett särskilt evenemang om registrerades rättigheter, i syfte att identifiera de utmaningar och tolkningsproblem som tillämpningen av de relevanta bestämmelserna i dataskyddsförordningen står inför.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING – ALLMÄNNA OBSERVATIONER

1. I dagens samhälle behandlas personuppgifter av offentliga och privata enheter i många verksamheter för ett brett spektrum av ändamål och på många olika sätt. Enskilda personer kan ofta vara mindre gynnade i fråga om förståelsen av hur deras personuppgifter behandlas, inbegripet den teknik som används i ett särskilt fall, oavsett om det är av en privat eller en offentlig enhet. För att skydda fysiska personers personuppgifter i dessa situationer har dataskyddsförordningen skapat en sammanhängande och stabil rättslig ram som är allmänt tillämplig på olika typer av behandling, inklusive särskilda bestämmelser om de registrerades rättigheter.

2. Rätten till tillgång till personuppgifter är en av de registrerades rättigheter enligt kapitel III i dataskyddsförordningen, liksom rätten till rättelse och radering, rätten till begränsning av behandling, rätten till dataportabilitet, rätten att invända eller rätten att inte bli föremål för automatiserat individuellt beslutsfattande, inbegripet profilering[2]. Den registrerades rätt till tillgång fastställs både i EU:s stadga om de grundläggande rättigheterna[3] och i artikel 15 i dataskyddsförordningen, där den formuleras som rätten till tillgång till personuppgifter och annan relaterad information.

3. Enligt dataskyddsförordningen består rätten till tillgång av tre delar, dvs. en bekräftelse på huruvida personuppgifter behandlas, tillgång till dessa och information om själva behandlingen. Den registrerade kan också få en kopia av de behandlade personuppgifterna, fast denna möjlighet är inte ytterligare en registrerad rättighet utan ett sätt att ge tillgång till uppgifterna. Rätten till tillgång kan därför förstås både som den registrerades möjlighet att fråga den personuppgiftsansvarige om personuppgifter om den registrerade håller på att behandlas och som möjligheten att få tillgång till

[1] Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.
[2] Artiklarna 15–22 i dataskyddsförordningen.
[3] Enligt artikel 8.1 i EU-stadgan om de grundläggande rättigheterna har alla rätt till skydd av personuppgifter som rör honom eller henne. Enligt artikel 8.2 andra meningen har alla rätt att få tillgång till uppgifter som har samlats in om honom eller henne och rätt att få dem rättade.

och kontrollera dessa uppgifter. Den personuppgiftsansvarige ska på begäran förse den registrerade med den information som omfattas av artikel 15.1 och 15.2 i dataskyddsförordningen.

4. Utövandet av rätten till tillgång sker både inom ramen för dataskyddslagstiftningen, i enlighet med målen i dataskyddslagstiftningen, och mer specifikt inom ramen för ”fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter”, vilket anges i artikel 1.2 i dataskyddsförordningen. Rätten till tillgång är en viktig del av hela dataskyddssystemet.

5. Det praktiska syftet med rätten till tillgång är att göra det möjligt för fysiska personer att ha kontroll över sina egna personuppgifter[4]. För att uppnå detta mål på ett effektivt sätt i praktiken syftar dataskyddsförordningen till att underlätta genom ett antal garantier som gör det möjligt för den registrerade att enkelt och utan onödiga begränsningar utöva denna rättighet med rimliga intervall och utan alltför stora dröjsmål eller kostnader. Allt detta bör leda till en effektivare tillämpning av den registrerades rätt till tillgång i den digitala tidsåldern, varav en del i vidare bemärkelse är den registrerades rätt att lämna in klagomål till tillsynsmyndigheten samt rätten till ett effektivt rättsskydd[5].

6. När det gäller utvecklingen av rätten till tillgång, som en del av den rättsliga ramen för dataskydd, bör det betonas att den har varit en del av det europeiska dataskyddssystemet från början. Jämfört med direktiv 95/46/EG har standarden för de registrerades rättigheter enligt dataskyddsförordningen både förfinats och stärkts. Detta gäller även rätten till tillgång. Eftersom formerna för rätten till tillgång preciseras närmare i dataskyddsförordningen är denna rättighet också ur rättssäkerhetssynpunkt mer klargörande för både den registrerade och den personuppgiftsansvarige. Dessutom kräver den specifika ordalydelsen i artikel 15, och den exakta tidsfristen för tillhandahållande av uppgifter enligt artikel 12.3 i dataskyddsförordningen, att den personuppgiftsansvarige ska vara beredd på den registrerades förfrågan genom att utarbeta förfaranden för hantering av begäranden.

7. Rätten till tillgång bör inte betraktas separat då den är nära förknippad med andra bestämmelser i dataskyddsförordningen, särskilt dataskyddsprinciper som inbegriper behandlingens korrekthet och laglighet och den personuppgiftsansvariges skyldighet till att tillhandahålla insyn, och med andra rättigheter för registrerade enligt kapitel III i dataskyddsförordningen.

8. Inom ramen för registrerades rättigheter är det också viktigt att framhålla betydelsen av artikel 12 i dataskyddsförordningen, där det fastställs krav på lämpliga åtgärder som den personuppgiftsansvarige ska vidta för att tillhandahålla den information som avses i artiklarna 13 och 14 i dataskyddsförordningen och den information som avses i artiklarna 15–22 och 34 i dataskyddsförordningen. I dessa krav anges i regel formen, sättet och tidsfristen för svar till den registrerade, särskilt för information som riktas till barn.

9. EDPB anser att det är nödvändigt att ge en mer exakt vägledning i fråga om hur rätten till tillgång ska genomföras i olika situationer. Syftet med dessa riktlinjer är att analysera de olika aspekterna av rätten till tillgång. Avsnittet nedan är särskilt ämnat att ge en allmän översikt och förklaring av innehållet i artikel 15, medan de följande avsnitten innehåller en djupare analys av vanliga praktiska frågor och problem vid genomförandet av rätten till tillgång.

[4] Se skälen 7, 68, 75 och 85 i dataskyddsförordningen.
[5] Se kapitel VIII artiklarna 77, 78 och 79 i dataskyddsförordningen.

2 SYFTET MED RÄTTEN TILL TILLGÅNG, STRUKTUREN I ARTIKEL 15 I DATASKYDDSFÖRORDNINGEN OCH ALLMÄNNA PRINCIPER

2.1 Syftet med rätten till tillgång

10. Rätten till tillgång är därför utformad för att göra det möjligt för fysiska personer att ha kontroll över personuppgifter som rör dem, ”för att vara medveten om att behandling sker och kunna kontrollera att den är laglig”[6]. Syftet med rätten till tillgång är närmare bestämt att göra det möjligt för de registrerade att förstå hur deras personuppgifter behandlas samt konsekvenserna av denna behandling, och att de ska kunna kontrollera att de uppgifter som behandlas är korrekta utan att behöva motivera sin avsikt. Syftet med rätten till tillgång är med andra ord att ge enskilda personer tillräcklig, öppen och lätt tillgänglig information om uppgiftsbehandling, oavsett vilken teknik som används, och att göra det möjligt för dem att kontrollera olika aspekter av en viss behandling enligt dataskyddsförordningen (t.ex. laglighet och korrekthet).

11. Den tolkning av dataskyddsförordningen som ges i dessa riktlinjer bygger på EU-domstolens rättspraxis hittills. Med hänsyn till betydelsen av rätten till tillgång kan relaterad rättspraxis förväntas utvecklas avsevärt i framtiden.

12. I enlighet med EU-domstolens beslut[7] syftar rätten till tillgång till att garantera de registrerades rätt till integritet och dataskydd vid behandling av uppgifter som rör dem[8] och kan underlätta utövandet av deras rättigheter som härrör från exempelvis artiklarna 16–19, 21–22 och 82 i dataskyddsförordningen. Utövandet av rätten till tillgång är dock en enskild persons rättighet och inte beroende av utövandet av dessa andra rättigheter, och utövandet av de andra rättigheterna är inte beroende av utövandet av rätten till tillgång.

13. Med tanke på det breda syftet med rätten till tillgång är det inte lämpligt att den personuppgiftsansvarige analyserar syftet med rätten till tillgång som en förutsättning för utövandet av rätten till tillgång som en del av dennes bedömning av begäranden om tillgång. Därför ska personuppgiftsansvariga inte bedöma ”varför” den registrerade begär tillgång, utan endast ”vad” den registrerade begär (se avsnitt 3 om analys av begäran) och huruvida de innehar personuppgifter som rör personen i fråga (se avsnitt 4). Därför ska den personuppgiftsansvarige till exempel inte neka tillgång på grund av eller misstanke om att de begärda uppgifterna kan användas av den registrerade för att försvara sig i domstol i händelse av en uppsägning eller handelstvist med den personuppgiftsansvarige[9]. När det gäller begränsningar och inskränkningar i rätten till tillgång, se avsnitt 6.

Exempel 1: En arbetsgivare avskedar en person. En vecka senare beslutar personen att samla in bevis för att väcka talan om avsked på orättvisa grunder mot sin tidigare arbetsgivare. Med detta i åtanke skriver personen till sin tidigare arbetsgivare och begär tillgång till alla personuppgifter som rör honom eller henne, i egenskap av registrerad, en begäran som den tidigare arbetsgivaren, i egenskap av personuppgiftsansvarig, behandlar.

[6] Skäl 63 i dataskyddsförordningen.
[7] Domstolens dom i mål C-434/16, Nowak, och de förenade målen C-141/12 och C-372/12, YS m.fl.
[8] Domstolens dom i mål C-434/16, Nowak, punkt 56.
[9] Frågor i detta ämne är omstridda i ett mål som väntar på avgörande i EU-domstolen (C-307/22).

Den personuppgiftsansvarige ska inte bedöma den registrerades avsikt, och den registrerade behöver inte ge den personuppgiftsansvarige en anledning till sin begäran. Om begäran uppfyller alla andra krav (se avsnitt 3) måste därför den personuppgiftsansvarige tillmötesgå denna, såvida inte begäran visar sig vara uppenbart ogrundad eller orimlig i enlighet med artikel 12.5 i dataskyddsförordningen (se avsnitt 6.3), vilket den personuppgiftsansvarige måste påvisa.

Avvikelse: Den registrerade utövar rätten att få tillgång till personuppgifter som rör honom eller henne under rättsprocessen. Den nationella lagstiftningen i medlemsstaten, som reglerar anställningsförhållandet mellan den personuppgiftsansvarige och den registrerade, innehåller dock vissa bestämmelser som begränsar omfattningen av den information som ska tillhandahållas eller utbytas mellan parterna till pågående eller framtida rättsliga förfaranden, vilka är tillämpliga på den talan om avsked på orättvisa grunder som den registrerade har väckt. I detta sammanhang, och under förutsättning att dessa nationella bestämmelser uppfyller kraven i artikel 23 i dataskyddsförordningen[10], har den registrerade inte rätt att få mer information från den personuppgiftsansvarige än vad som föreskrivs i medlemsstatens nationella lagstiftning om informationsutbyte mellan parter i rättstvister.

14. Även om syftet med rätten till tillgång är brett visade EU-domstolen gränserna för dataskyddslagstiftningens ansvarsområde och rätten till tillgång. EU-domstolen fann till exempel att syftet med den rätt till tillgång som garanteras genom EU:s dataskyddslagstiftning ska särskiljas från syftet med rätten till tillgång till offentliga handlingar som fastställs i EU:s lagstiftning och nationell lagstiftning, där den sistnämnda rätten har till syfte att ”säkerställa insyn i offentliga myndigheters beslutsprocesser eller att främja goda förvaltningsrutiner”[11], ett mål som inte eftersträvas i dataskyddslagstiftningen. EU-domstolen drog slutsatsen att rätten till tillgång till personuppgifter gäller oavsett om en annan typ av rätt till tillgång i ett annat syfte gäller, t.ex. i samband med ett examensförfarande.

2.2 Strukturen i artikel 15 i dataskyddsförordningen

15. För att besvara en begäran om tillgång och se till att ingen av dess aspekter åsidosätts är det nödvändigt att förstå strukturen i artikel 15 och komponenterna i den rätt till tillgång som fastställs i denna artikel.

16. Artikel 15 kan delas upp i åtta olika delar enligt tabellen nedan:

1.	Bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas.	Artikel 15.1 första halvan av meningen.
2.	Få tillgång till personuppgifterna.	Artikel 15.1, andra halvan av meningen (första delen).
3.	Få tillgång till följande information om behandlingen: a) Ändamålen med behandlingen. b) De kategorier av personuppgifter som behandlingen gäller. c) Mottagare eller kategorier av mottagare.	Artikel 15.1 andra halvan av meningen (andra delen).

[10] EDPB:s riktlinjer 10/2020 om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen, version för offentligt samråd, 18 december 2020.
[11] Domstolens dom i målen C-141/12 och C-372/12, YS m.fl., punkt 47.

	d) Behandlingens planerade varaktighet eller kriterierna för att fastställa varaktigheten. e) Förekomsten av rätten till rättelse, radering, begränsning av behandling och invändningar mot behandling. f) Rätten att inge klagomål till en tillsynsmyndighet. g) All tillgänglig information om källan till uppgifterna, om den inte samlas in från den registrerade. h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering och annan information om detta.	
4.	Information om skyddsåtgärder enligt artikel 46 om personuppgifterna överförs till ett tredjeland eller till en internationell organisation.	Artikel 15.2.
5.	Den personuppgiftsansvariges skyldighet att förse den registrerade med en kopia av de personuppgifter som är under behandling.	Artikel 15.3 första meningen.
6.	Debitering av en rimlig avgift av den personuppgiftsansvarige på grundval av administrativa kostnader för eventuella ytterligare kopior som den registrerade begär.	Artikel 15.3 andra meningen.
7.	Tillhandahållande av information i ett elektroniskt format.	Artikel 15.3 tredje meningen.
8.	Med beaktande av andras rättigheter och friheter.	Artikel 15.4.

Alla delar av artikel 15.1 och 15.2 definierar tillsammans innehållet i rätten till tillgång, medan artikel 15.3 behandlar villkoren för tillgång, utöver de allmänna kraven i artikel 12 i dataskyddsförordningen. Artikel 15.4 kompletterar de gränser och begränsningar som fastställs i artikel 12.5 i dataskyddsförordningen för alla registrerades rättigheter, med särskilt fokus på andras rättigheter och friheter i samband med tillgång.

2.2.1 Definiera innehållet i rätten till tillgång

17. Artikel 15.1 och 15.2 innehåller följande tre aspekter: För det första bekräftelse av huruvida den begärandes personuppgifter behandlas, om ja, för det andra tillgång till dessa uppgifter, och för det tredje information om behandlingen. De kan betraktas som tre olika komponenter som tillsammans bygger upp rätten till tillgång.

2.2.1.1 Bekräftelse på huruvida personuppgifter håller på att behandlas

18. När de registrerade begär tillgång till personuppgifter måste de först få veta om den personuppgiftsansvarige behandlar uppgifter som rör dem eller inte. Denna information utgör följaktligen den första delen av rätten till tillgång enligt artikel 15.1. Om den personuppgiftsansvarige inte behandlar personuppgifter som rör den registrerade som begär tillgång ska den information som tillhandahålls begränsas till att bekräfta att inga personuppgifter som rör den registrerade håller på att behandlas. Om den personuppgiftsansvarige behandlar uppgifter om den begärande måste den personuppgiftsansvarige bekräfta detta för denne. Denna bekräftelse kan meddelas separat eller ingå som en del av informationen om de personuppgifter som behandlas (se nedan).

2.2.1.2 Tillgång till de personuppgifter som behandlas

19. Tillgång till personuppgifter är den andra delen av rätten till tillgång enligt artikel 15.1 och utgör kärnan i denna rättighet. Den rör begreppet personuppgifter enligt definitionen i artikel 4.1 i dataskyddsförordningen. Förutom grundläggande personuppgifter som namn och adress kan en obegränsad mängd uppgifter omfattas av denna definition, förutsatt att de omfattas av dataskyddsförordningens materiella tillämpningsområde, särskilt när det gäller hur de behandlas (artikel 2 i dataskyddsförordningen). Tillgång till personuppgifter syftar här på tillgången till de faktiska personuppgifterna, inte bara en allmän beskrivning av uppgifterna eller enbart en hänvisning till de kategorier av personuppgifter som behandlas av den personuppgiftsansvarige. Om inga begränsningar eller inskränkningar gäller[12] har de registrerade rätt att få tillgång till alla behandlade uppgifter som rör dem, eller till delar av uppgifterna, beroende på omfattningen av begäran (se avsnitt 2.3.1). Skyldigheten att ge tillgång till uppgifterna beror inte på uppgifternas art eller källa. Det gäller i sin helhet även i fall där den begärande ursprungligen hade försett den personuppgiftsansvarige med uppgifterna, eftersom syftet är att den registrerade ska få information om den personuppgiftsansvariges faktiska behandling av dessa uppgifter. Omfattningen av personuppgifter enligt artikel 15 förklaras i detalj i avsnitten 4.1 och 4.2.

2.2.1.3 Information om behandlingen och om registrerades rättigheter

20. Den tredje delen av rätten till tillgång är den information om behandlingen och de registrerades rättigheter som den personuppgiftsansvarige måste tillhandahålla enligt artikel 15.1 a–h och 15.2. Sådan information kan baseras på text som exempelvis hämtats från den personuppgiftsansvariges meddelande om integritetsskydd[13] eller från den personuppgiftsansvariges register över behandling som avses i artikel 30 i dataskyddsförordningen, men kan behöva uppdateras och anpassas till den registrerades begäran. Informationens innehåll och grad av specifikation beskrivs närmare i avsnitt 4.3.

2.2.2 Bestämmelser om villkor

21. Artikel 15.3 kompletterar kraven på villkoren för svar på begäran om tillgång enligt artikel 12 i dataskyddsförordningen med vissa specifikationer i samband med begäranden om tillgång.

2.2.2.1 Tillhandahållande av en kopia

22. Enligt artikel 15.3 första meningen i dataskyddsförordningen ska den personuppgiftsansvarige tillhandahålla en kostnadsfri kopia av de personuppgifter som behandlingen avser. Kopian avser därför endast den andra delen av rätten till tillgång (tillgång till de personuppgifter som behandlas, se ovan). Den personuppgiftsansvarige måste se till att den första kopian är kostnadsfri, även om denne anser att kostnaden för reproduktion är hög (exempel: kostnader för att tillhandahålla en kopia av inspelningen av ett telefonsamtal).

23. Skyldigheten att tillhandahålla en kopia ska inte tolkas som en ytterligare rättighet för den registrerade, utan som ett villkor för att ge tillgång till uppgifterna. Det stärker rätten till tillgång till uppgifterna[14] och hjälper till att tolka denna rätt eftersom det klargörs att tillgången till uppgifterna enligt artikel 15.1 omfattar fullständig information om alla uppgifter och inte kan tolkas som att endast en sammanfattning av uppgifterna beviljas. Samtidigt är skyldigheten att tillhandahålla en kopia inte

[12] Se avsnitt 6 i dessa riktlinjer.
[13] För information om detta, se artikel 29-gruppen, WP260 rev.01, 11 april 2018, Guidelines on transparency under Regulation 2016/679 – godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB*).
[14] Skyldigheten att tillhandahålla en kopia nämndes inte i dataskyddsdirektivet 95/46/EG.

avsedd att vidga omfattningen av rätten till tillgång: Den avser (endast) en kopia av de personuppgifter som håller på att behandlas, inte nödvändigtvis en reproduktion av originalhandlingarna (se avsnitt 5, punkt 152). Generellt sett är det ingen ytterligare information som ska ges till den registrerade när denne tillhandahåller en kopia: Omfattningen av den information som ska ingå i kopian är den samma som för tillgången till uppgifterna enligt 15.1 (andra delen av den rätt till tillgång som avses ovan, se punkt 19), vilket innehåller all information som krävs för att den registrerade ska kunna förstå och kontrollera att behandlingen är laglig[15].

24. Skyldigheten att tillhandahålla en kopia enligt artikel 15.3 är uppfylld mot bakgrund av ovanstående, och om tillgång till uppgifterna i den mening som avses i artikel 15.1 ges genom att en kopia tillhandahålls. Skyldigheten att tillhandahålla en kopia tjänar det målet att den registrerade genom rätten till tillgång kan bli medveten om och kontrollera att behandlingen är laglig (skäl 63). För att uppnå detta mål ska den registrerade i de flesta fall inte bara ta del av informationen som hastigast. Därför måste den registrerade få tillgång till informationen genom att erhålla en kopia av personuppgifterna.

25. Mot bakgrund av ovanstående ska begreppet kopia tolkas i vidare bemärkelse och gäller för olika typer av tillgång till personuppgifter, så länge kopian är fullständig (dvs. omfattar alla personuppgifter som begärs) och möjlig för den registrerade att bevara. Kravet på att tillhandahålla en kopia innebär således att informationen om den person som gör begäran lämnas till den registrerade på ett sätt som gör det möjligt för den registrerade att bevara all information och återkomma till den.

26. Trots denna breda förståelse av begreppet kopia, och med hänsyn till att det är det främsta sättet på vilket tillgång bör ges, kan det under vissa omständigheter vara lämpligt med andra former. Ytterligare förklaringar om kopior och andra sätt att ge tillgång ges i avsnitt 5, särskilt 5.2.2–5.2.5.

2.2.2.2 Tillhandahålla ytterligare kopior

27. Artikel 15.3 andra meningen gäller situationer där den registrerade ber den personuppgiftsansvarige om mer än en kopia, till exempel om den första kopian gått förlorad eller blivit skadad, eller om den registrerade vill vidarebefordra en kopia till en annan person eller en tillsynsmyndighet. Om ytterligare kopior måste tillhandahållas av den personuppgiftsansvarige på begäran av den registrerade fastställs i artikel 15.3 att den personuppgiftsansvarige får ta ut en rimlig avgift på grundval av administrativa kostnader (artikel 15.3 andra meningen).

28. Om den registrerade begär ytterligare en kopia efter att den första begäran gjordes kan frågor uppstå om huruvida detta bör betraktas som en ny begäran eller om den registrerade vill ha en ytterligare kopia av uppgifterna i den mening som avses i artikel 15.3 andra meningen, i vilket fall en avgift för en ytterligare kopia kan tas ut. Svaret på dessa frågor beror enbart på innehållet i begäran: Begäran ska tolkas som en begäran om ytterligare en kopia, i den mån den avser samma behandling av personuppgifter som den förra begäran i fråga om tid och omfattning. Om den registrerades syfte är att få information om uppgifter som behandlats vid en annan tidpunkt eller om begäran avser en annan uppsättning uppgifter än den som begärdes från början, är dock rätten att erhålla en kostnadsfri kopia enligt artikel 15.3 återigen tillämplig. Detta gäller även i fall där den registrerade har gjort en första begäran strax innan. En registrerad får utöva sin rätt till tillgång genom en efterföljande begäran och erhålla en kostnadsfri kopia, såvida inte begäran anses vara orimlig enligt artikel 12.5, då det är möjligt att ta ut en rimlig avgift i enlighet med artikel 12.5 a (om repetitiva begärandens orimliga art, se avsnitt 6).

[15] Frågor i ämnet för denna punkt är omstridda i ett mål som väntar på avgörande i EU-domstolen (C-487/21).

Exempel 2: En kund skickar en begäran om tillgång till ett handelsföretag. Ett år efter svaret från företaget inkommer samma kund med en begäran om tillgång enligt artikel 15 till samma företag. Oavsett huruvida det har förekommit nya affärstransaktioner eller andra kontakter mellan parterna sedan den tidigare begäran, ska denna andra begäran betraktas som en ny begäran. Även om företagets behandling av uppgifterna inte har ändrats – vilket inte nödvändigtvis är uppenbart för den registrerade – har den registrerade rätt att få en kostnadsfri kopia av uppgifterna.

Variation 1: Även om kunden i ovanstående fall ställer den nya begäran till exempel redan en vecka efter den första begäran, kan denna mycket väl betraktas som en ny begäran enligt artikel 15.1 och 15.3 första meningen, såvida den inte ska tolkas som en ren påminnelse om den första begäran. När det gäller det korta intervallet, och beroende på de särskilda omständigheterna i den nya begäran, är det orimliga enligt artikel 12.5 i förordningen omstritt (se avsnitt 6).

Variation 2: Begäran om en ”ny kopia” av den information som redan hade lämnats i form av en kopia som svar på en tidigare begäran, till exempel om kunden förlorat den kopia som tidigare mottagits, bör naturligtvis betraktas som en begäran om ytterligare en kopia, eftersom den avser den tidigare begäran i fråga om omfattning och tidpunkt för behandlingen.

29. Om den registrerade upprepar en första begäran om tillgång på grund av att det mottagna svaret inte var fullständigt eller att inga skäl har angivits för ett avslag, ska denna begäran inte betraktas som en ny begäran, eftersom den endast är en påminnelse om en första ouppfylld begäran.

30. När det gäller fördelning av kostnaderna vid begäran om ytterligare en kopia fastställs i artikel 15.3 att den personuppgiftsansvarige får ta ut en rimlig avgift på grundval av de administrativa kostnader som orsakas av begäran. Detta innebär att de administrativa kostnaderna är ett relevant kriterium för att fastställa avgiftsnivån. Samtidigt bör avgiften vara rimlig, med hänsyn till vikten av rätten till tillgång som en grundläggande rättighet för den registrerade. Den personuppgiftsansvarige ska inte överföra administrativa omkostnader eller andra allmänna kostnader till den registrerade utan inrikta sig på de specifika kostnader som orsakats av tillhandahållandet av ytterligare en kopia. Under detta förfarande bör den personuppgiftsansvarige använda personal och materiella resurser på ett effektivt sätt för att hålla nere kostnaderna för kopian, även om den personuppgiftsansvarige tar hjälp externt.

31. Om den personuppgiftsansvarige beslutar att ta ut en avgift bör denne i förväg ange att en avgift kommer att tas ut och – så exakt som möjligt – ange vilka kostnader som den har för avsikt att debitera, så att den registrerade får möjlighet att ta ställning till om begäran ska vidhållas eller dras tillbaka.

2.2.2.3 Tillhandahållande av information i ett elektroniskt format som är allmänt använt

32. Vid en begäran i ett elektroniskt format ska informationen om möjligt tillhandahållas på elektronisk väg, såvida inte den registrerade begär något annat (se artikel 12.3 i dataskyddsförordningen). Artikel 15.3 tredje meningen kompletterar detta krav i samband med begäran om tillgång genom att ange att den personuppgiftsansvarige dessutom är skyldig att tillhandahålla svaret i ett elektroniskt format som är allmänt använt, såvida inte den registrerade begär något annat. Artikel 15.3 förutsätter att det kommer att vara möjligt för personuppgiftsansvariga som kan ta emot elektroniska förfrågningar att lämna svar på begäran i ett elektroniskt format som är allmänt använt (för detaljer se avsnitt 5.2.5). Denna bestämmelse avser all information som måste lämnas i enlighet med artikel 15.1 och 15.2. Om den registrerade lämnar in en begäran om tillgång på elektronisk väg måste därför all information tillhandahållas i ett elektroniskt format som är allmänt använt. Frågor kring formatet utvecklas närmare i avsnitt 5. Den personuppgiftsansvarige bör som alltid vidta lämpliga säkerhetsåtgärder, framför allt när det gäller särskilda kategorier av personuppgifter (se 2.3.4 nedan).

2.2.3 Eventuella begränsningar av rätten till tillgång

33. Slutligen föreskrivs en särskild begränsning i artikel 15.4 när det gäller rätten till tillgång. Där konstateras att en eventuell negativ inverkan på andras rättigheter och friheter måste beaktas. Frågor som gäller omfattningen och konsekvenserna av denna begränsning samt ytterligare begränsningar och inskränkningar som anges i artikel 12.5 eller artikel 23 i dataskyddsförordningen förklaras i avsnitt 6.

2.3 Allmänna principer för rätten till tillgång

34. När registrerade gör en begäran om tillgång till sina uppgifter måste den information som avses i artikel 15 i dataskyddsförordningen i princip alltid tillhandahållas i sin helhet. Om den personuppgiftsansvarige behandlar uppgifter om den registrerade ska den personuppgiftsansvarige därför tillhandahålla all den information som avses i artikel 15.1 och, i tillämpliga fall, den information som avses i artikel 15.2. Den personuppgiftsansvarige måste vidta de åtgärder som krävs för att se till att informationen är fullständig, korrekt och aktuell, och att den är så nära databehandlingen som möjligt vid tidpunkten för mottagandet av begäran[16]. Om två eller flera personuppgiftsansvariga behandlar uppgifter gemensamt påverkar fördelningen mellan de gemensamt personuppgiftsansvarigas respektive ansvar i fråga om utövandet av den registrerades rättigheter inte de registrerades rättigheter gentemot den personuppgiftsansvarige till vilken de riktar sin begäran, särskilt inte när det gäller svar på begäranden om tillgång[17].

2.3.1 Informationens fullständighet

35. De registrerade har, med de undantag som anges nedan, rätt att få fullständig information om alla uppgifter som rör dem (för närmare uppgifter om omfattningen, se avsnitt 4.2). Om den registrerade inte uttryckligen begär något annat ska en begäran om utövande av rätten till tillgång förstås i allmänna termer vilket omfattar alla personuppgifter som rör den registrerade[18]. En begränsad tillgång till en del av informationen kan övervägas i följande fall:

a) Den registrerade har uttryckligen begränsat begäran till en delmängd. För att undvika tillhandahållande av ofullständig information får den personuppgiftsansvarige endast beakta denna begränsning av den registrerades begäran om det är säkert att en sådan tolkning motsvarar den registrerades önskemål (se avsnitt 3.1.1, punkt 51). Den registrerade ska i princip inte behöva upprepa sin begäran om överföring av alla uppgifter som den registrerade har rätt att erhålla.

b) I situationer där den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade kan den personuppgiftsansvarige hysa tvivel om huruvida en begäran om tillgång, som uttrycks i högst allmänna termer, verkligen syftar till att få information om alla typer av uppgifter som behandlas eller om den personuppgiftsansvariges alla verksamhetsgrenar i detalj. Dessa tvivel kan särskilt uppstå i situationer där det inte funnits möjlighet att förse de registrerade med verktyg för att specificera sin begäran från början eller där den registrerade inte använde sig av dem. Den personuppgiftsansvarige står då inför problemet hur man kan ge ett fullständigt svar samtidigt som man undviker att skapa ett överflöde av information för den registrerade som denne inte är intresserad av och inte kan hantera på ett effektivt sätt. Det kan finnas sätt att lösa detta problem, beroende på omständigheterna och de

[16] För vägledning om lämpliga åtgärder, se avsnitt 5 punkterna 123–129.
[17] EDPB:s *Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR*, punkt 162f. Personuppgiftsbiträdet måste bistå den personuppgiftsansvarige, se punkt 129 ovan.
[18] Mer information finns i avsnitt 5.2.3 nedan om skiktad strategi.

tekniska möjligheterna, till exempel genom att tillhandahålla ett självbetjäningsverktyg i onlinesammanhang (se avsnitt 5 om den skiktade strategin). Om sådana lösningar inte är tillämpliga kan en personuppgiftsansvarig som behandlar en stor mängd information om den registrerade begära att den registrerade specificerar den information eller behandling som begäran avser innan informationen lämnas (se skäl 63 i dataskyddsförordningen). Exempel på detta kan vara ett företag med flera verksamhetsområden eller en offentlig myndighet med olika administrativa enheter, om den personuppgiftsansvarige konstaterar att ett stort antal uppgifter om den registrerade behandlas inom dessa grenar. Dessutom kan en stor mängd uppgifter behandlas av personuppgiftsansvariga som samlar in uppgifter om den registrerades frekventa aktiviteter under en längre tidsperiod.

Exempel 3: En offentlig myndighet behandlar uppgifter om den registrerade på flera avdelningar som rör olika sammanhang. Dokumenthantering och -arkivering behandlas delvis på icke-automatiserade sätt och de flesta av uppgifterna lagras endast i pappersdokument. När det gäller den allmänna ordalydelsen i en begäran tvivlar den offentliga myndigheten på att den registrerade är medveten om omfattningen av begäran, särskilt de olika typer av behandling som den skulle omfatta, mängden information och det sidantal som den registrerade skulle erhålla.

Exempel 4: Ett stort försäkringsbolag får en allmän begäran om tillgång via brev från en person som har varit kund i många år. Även om borttagningsfristerna respekteras fullt ut behandlar företaget en stor mängd uppgifter som rör kunden, eftersom behandling fortfarande är påkallad för att uppfylla avtalsförpliktelser som härrör från avtalsförhållandet med kunden (t.ex. fortsatta skyldigheter, kommunikation om kontroversiella frågor med kunden och med tredje part, …) eller för att uppfylla rättsliga skyldigheter (arkiverade uppgifter som måste lagras för skatteändamål osv.). Försäkringsbolaget kan hysa tvivel om huruvida begäran, som gjordes i mycket allmänna ordalag, verkligen avser alla typer av dessa uppgifter. Detta kan vara särskilt problematiskt om försäkringsbolaget endast har en postadress till den registrerade och därför måste skicka all information på papper. Samma tvivel kan aktualiseras när informationen tillhandahålls på annat sätt.

Om den personuppgiftsansvarige i sådana fall beslutar att be den registrerade specificera sin begäran, för att fullgöra sin skyldighet att underlätta utövandet av rätten till tillgång (artikel 12.2 i dataskyddsförordningen), ska den personuppgiftsansvarige samtidigt lämna meningsfull information om sin behandling som kan beröra den registrerade, genom att informera om relevanta grenar av sin verksamhet, databaser osv.

Exempel 5: I ett anställningsförhållande, vid en allmänt formulerad begäran om tillgång, är det inte uppenbart att den anställde vill ha alla uppgifter om användarinloggning, uppgifter om tillgång till en arbetsplats, uppgifter om avräkning för måltider, uppgifter om löneutbetalningar osv. En begäran om specifikation från arbetsgivaren skulle till exempel kunna leda till klargörandet att den anställde är intresserad av att förstå eller kontrollera till vem dennes prestationsbedömning har vidarebefordrats. Utan en begäran om specificering skulle den anställde få en stor mängd information, varav de flesta uppgifter inte är av intresse för denne. Samtidigt skulle arbetsgivaren behöva lämna information om de olika sammanhang för behandling som kan beröra den anställde för att den anställde skulle kunna specificera sin begäran på ett vettigt sätt.

Det är viktigt att understryka att en begäran om specificering inte ska ha till syfte att begränsa svaret på begäran om tillgång och inte får användas för att dölja information om uppgifterna eller behandlingen som rör den registrerade. Om en registrerad som har ombetts att specificera omfattningen av sin begäran bekräftar att han eller hon söker alla personuppgifter som rör honom eller henne måste den personuppgiftsansvarige naturligtvis tillhandahålla dem i sin helhet.

Under alla omständigheter bör den personuppgiftsansvarige alltid kunna visa att sättet att hantera en begäran har till syfte att i möjligaste mån främja rätten till tillgång och att det är i linje med dennes skyldighet att underlätta den registrerades utövande av sina rättigheter (artikel 12.2 i dataskyddsförordningen). Om inte annat följer av dessa principer kan den personuppgiftsansvarige invänta den registrerades svar innan ytterligare uppgifter tillhandahålls i enlighet med den registrerades önskemål, om den personuppgiftsansvarige har gett den registrerade en tydlig översikt över alla behandlingar som kan beröra den registrerade, särskilt sådana som den registrerade kanske inte har förväntat sig. Det gäller även om den personuppgiftsansvarige har gett tillgång till alla uppgifter som den registrerade tydligt avsåg, och om denna information dessutom har kombinerats med en tydlig indikation på hur man får tillgång till de återstående delarna av de registrerade uppgifterna.

c) Undantag eller begränsningar av rätten till tillgång gäller (se avsnitt 6 nedan). I sådana fall bör den personuppgiftsansvarige noggrant kontrollera vilka delar av informationen som undantaget avser och tillhandahålla all information som inte omfattas av undantaget. En bekräftelse av behandlingen av personuppgifter i sig (komponent 1) kan till exempel inte påverkas av undantaget. Till följd av detta måste information lämnas om alla personuppgifter och all information som avses i artikel 15.1 och 15.2 och inte berörs av undantaget eller begränsningen.

2.3.2 Informationens korrekthet

36. Informationen i kopian av personuppgifterna till den registrerade måste omfatta den faktiska information eller de faktiska personuppgifter som finns om den registrerade. Detta inbegriper skyldigheten att lämna information om uppgifter som är felaktiga och om databehandling som inte, eller inte längre, är laglig. Den registrerade kan till exempel använda rätten till tillgång för att ta reda på källan till felaktiga uppgifter som sprids mellan olika personuppgiftsansvariga. Om den personuppgiftsansvarige korrigerade felaktiga uppgifter innan den registrerade informerades om dem skulle den registrerade fråntas denna möjlighet. Detsamma gäller vid olaglig behandling. Möjligheten att få vetskap om olaglig behandling som rör den registrerade är ett av huvudsyftena med rätten till tillgång. Skyldigheten att informera om behandlingens varaktiga status påverkar inte den personuppgiftsansvariges skyldighet att upphöra med olaglig behandling eller att korrigera felaktiga uppgifter. Frågor om i vilken ordning dessa skyldigheter ska uppfyllas besvaras nedan.

2.3.3 Tidsreferenspunkt för bedömningen

37. Bedömningen av de uppgifter som behandlas ska så nära som möjligt spegla den situation som råder då den personuppgiftsansvarige tar emot begäran och svaret bör omfatta alla uppgifter som finns tillgängliga vid den tidpunkten. Detta innebär att den personuppgiftsansvarige måste försöka ta reda på all uppgiftsbehandling som rör den registrerade utan onödigt dröjsmål. Personuppgiftsansvariga behöver därför inte lämna personuppgifter som de tidigare har behandlat men som de inte längre har tillgång till[19]. Till exempel kan den personuppgiftsansvarige ha tagit bort personuppgifter i enlighet med sin policy för lagring av uppgifter och/eller lagstadgade bestämmelser och kan därför inte längre tillhandahålla de begärda personuppgifterna. I detta sammanhang bör det erinras om att den tid under vilken uppgifterna lagras bör fastställas i enlighet med artikel 5.1 e i dataskyddsförordningen, eftersom all lagring av uppgifter ska kunna motiveras sakligt.

[19] Se i detta avseende ytterligare förtydliganden i avsnitt 4 i dessa riktlinjer samt i Europeiska unionens domstols dom av den 7 maj 2009, College van burgemeester en wethouders van Rotterdam/M. E. Rijkeboer, C-553/07, om rätten till tillgång till information om mottagare eller kategorier av mottagare i förfluten tid.

38. Samtidigt ska den personuppgiftsansvarige i förväg vidta de åtgärder som krävs för att underlätta utövandet av rätten till tillgång och för att kunna behandla sådana begäranden så snart som möjligt (se artikel 12.3) och innan uppgifterna måste tas bort. När det handlar om korta lagringstider bör därför de åtgärder som vidtas för att besvara begäran anpassas till lämplig lagringstid för att underlätta utövandet av rätten till tillgång och för att undvika att det blir omöjligt för gott att ge tillgång till de uppgifter som behandlas vid tidpunkten för begäran[20]. I vissa fall kan det inte desto mindre vara omöjligt att besvara en begäran innan uppgifterna är planerade för borttagning. Om en personuppgiftsansvarig exempelvis i samband med att denne besvarar en begäran så snabbt som möjligt hämtar personuppgifter som planerats för borttagning följande dag, kan den personuppgiftsansvarige behöva lite extra tid för att ta ställning till om det behöver göras en redigering för att skydda andras friheter, innan en kopia av personuppgifterna lämnas ut till begäranden. Om uppgifterna har hämtats inom den planerade lagringsperioden får den personuppgiftsansvarige fortsätta behandla uppgifterna i syfte att fullgöra sin skyldighet att besvara begäran. I dessa fall kan behandlingen baseras på artikel 6.1 c i kombination med artikel 15 i dataskyddsförordningen och dess varaktighet måste uppfylla kraven i artikel 12.3 i dataskyddsförordningen[21]. Tillämpningen av denna rättsliga grund är begränsad till behandling av de uppgifter som identifierats som nödvändiga för att besvara den konkreta begäran och ska inte användas som motivering för en allmän förlängning av lagringstiderna.

39. Dessutom ska den personuppgiftsansvarige inte avsiktligen kringgå skyldigheten att tillhandahålla de begärda personuppgifterna genom att radera eller ändra personuppgifter som svar på en begäran om tillgång (se 2.3.2). Om den personuppgiftsansvarige under behandlingen av begäran om tillgång upptäcker felaktiga uppgifter eller olaglig behandling måste den personuppgiftsansvarige bedöma behandlingens status och informera den registrerade om denna innan denne fullgör sina andra skyldigheter. För att undvika behovet av ytterligare kommunikation om detta och för att det ska vara förenligt med principen om insyn bör det ligga i den personuppgiftsansvariges intresse att lägga till information om efterföljande rättelser eller borttaganden.

Exempel 6: En personuppgiftsansvarig besvarar en begäran om tillgång och inser att en ansökan från den registrerade om en ledig tjänst i den personuppgiftsansvariges företag har lagrats längre än lagringsperioden. I detta fall kan den personuppgiftsansvarige inte först ta bort den och sedan svara den registrerade att inga uppgifter (som rör ansökan) har behandlats. Denne måste ge tillgång först och ta bort uppgifterna efteråt. För att förhindra en efterföljande begäran om radering rekommenderas att information läggs till om denna omständighet och tidpunkten för borttagandet.

För att följa principen om insyn bör personuppgiftsansvariga informera den registrerade från och med den specifika tidpunkt för behandlingen som den personuppgiftsansvariges svar avser. I vissa fall, till exempel i samband med en tät kommunikation, kan ytterligare behandling eller ändringar av uppgifterna ske mellan denna referenspunkt, där behandlingen bedömdes, och den personuppgiftsansvariges svar. Om den personuppgiftsansvarige har kännedom om sådana ändringar

[20] Till exempel kan införandet av ett självbetjäningsverktyg som gör det möjligt för den registrerade att enkelt få tillgång till de begärda personuppgifterna och ett system för anmälan som gör den personuppgiftsansvarige beredd på en begäran som rör personuppgifter med korta lagringstider övervägas för att underlätta snabba åtgärder.

[21] Detta påverkar inte en efterföljande behandling av uppgifter för bevisändamål i samband med hanteringen av begäran om tillgång under en lämplig tidsperiod.

rekommenderas att information om dessa ändringar och information om ytterligare behandling som krävs för att begäran ska kunna besvaras inkluderas i svaret.

2.3.4 Överensstämmelse med datasäkerhetskraven

40. Eftersom överföring och tillhandahållande av personuppgifter till den registrerade är en behandlingsåtgärd är den personuppgiftsansvarige alltid skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att sörja för en säkerhetsnivå som är lämplig med hänsyn till risken i samband med behandlingen (se artiklarna 5.1 f, 24 och 32 i dataskyddsförordningen). Detta gäller oberoende av sättet på vilket tillgången ges. Vid icke-elektronisk överföring av uppgifterna till den registrerade får den personuppgiftsansvarige, beroende på de risker som behandlingen medför, överväga att använda rekommenderad post eller, alternativt, erbjuda, men inte ålägga, den registrerade att hämta dokumentet mot underskrift direkt från en av den personuppgiftsansvariges enheter. Om informationen i enlighet med artikel 12.1 och 12.3 tillhandahålls på elektronisk väg ska den personuppgiftsansvarige välja elektroniska medel som uppfyller kraven på datasäkerhet. Även om en kopia av uppgifterna lämnas i ett elektroniskt format som är allmänt använt (se artikel 15.3) ska den personuppgiftsansvarige beakta kraven på datasäkerhet när denne väljer hur det elektroniska dokumentet ska överföras till den registrerade. Detta kan inbegripa kryptering, lösenordsskydd osv. För att underlätta tillgången till krypterade uppgifter bör den personuppgiftsansvarige se till att lämplig information görs tillgänglig så att den registrerade kan få tillgång till den avkrypterade informationen. Om datasäkerhetskraven skulle kräva fullständig kryptering av e-post, men den personuppgiftsansvarige endast kan skicka ett vanligt e-postmeddelande, måste den personuppgiftsansvarige använda andra sätt, som att skicka en usb-sticka med (rekommenderad) post till den registrerade.

3 ALLMÄNNA ÖVERVÄGANDEN AVSEENDE BEDÖMNINGEN AV BEGÄRAN OM TILLGÅNG

3.1 Inledning

41. När den personuppgiftsansvarige tar emot en begäran om tillgång till personuppgifter måste denne bedöma varje begäran individuellt. Den personuppgiftsansvarige ska bland annat beakta följande frågor som utvecklas närmare i nedanstående punkter: Huruvida begäran rör personuppgifter som är kopplade till den begärande personen och vem den personen är. Detta avsnitt syftar till att klargöra vilka delar av begäran om tillgång som den personuppgiftsansvarige bör beakta när denne gör sin bedömning och diskutera möjliga scenarier för en sådan bedömning samt dess konsekvenser. När den personuppgiftsansvarige bedömer en begäran om tillgång till personuppgifter ska denne också, i enlighet med artikel 12.2 i dataskyddsförordningen, beakta skyldigheten att underlätta utövandet av den registrerades rättigheter, samtidigt som hänsyn tas till lämplig säkerhet för personuppgifterna[22].

[22] Den personuppgiftsansvarige ska sörja för lämplig säkerhet för personuppgifterna, i enlighet med integritets- och konfidentialitetsprincipen (artikel 5.1 f i dataskyddsförordningen), genom att vidta lämpliga tekniska och organisatoriska åtgärder enligt artikel 32 i dataskyddsförordningen som utarbetats i artikel 24 i dataskyddsförordningen. Den personuppgiftsansvarige ska kunna visa att denne säkerställer en adekvat dataskyddsnivå i enlighet med principen om ansvarsskyldighet (se även Artikel 29-arbetsgruppens yttrande 3/2010 om principen om ansvarsskyldighet, antaget den 13 juli 2010, 00062/10/EN WP 173 och EDPB:s *Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR*).

42. Därför bör de personuppgiftsansvariga vara proaktivt redo att hantera begäranden om tillgång till personuppgifter. Detta innebär att den personuppgiftsansvarige bör vara beredd att ta emot en begäran, bedöma den ingående (denna bedömning är föremål för detta avsnitt av riktlinjerna) och utan onödigt dröjsmål lämna ett lämpligt svar till den begärande. Det sätt på vilket de personuppgiftsansvariga kommer att förbereda sig för att tillgodose begäranden om tillgång bör vara adekvat och proportionerligt och beroende av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, i enlighet med artikel 24 i dataskyddsförordningen. Beroende på omständigheterna i fallet kan de personuppgiftsansvariga till exempel åläggas att genomföra ett lämpligt förfarande på ett sätt som garanterar uppgifternas säkerhet utan att hindra utövandet av den registrerades rättigheter.

3.1.1 Analys av innehållet i begäran

43. Den saken kan bedömas mer specifikt genom att följande frågor ställs:

a) Berör begäran personuppgifter?

44. Enligt dataskyddsförordningen ska begäran endast omfatta personuppgifter[23]. En begäran om information som rör andra frågor, inbegripet allmän information om den personuppgiftsansvarige, dennes affärsmodeller eller behandling som inte rör personuppgifter, ska därför inte betraktas som en begäran enligt artikel 15 i dataskyddsförordningen. Dessutom kommer en begäran om information om anonyma uppgifter, eller uppgifter som inte rör den begärande personen eller den person på vars vägnar den bemyndigade personen gjort en begäran, inte att omfattas av rätten till tillgång. Denna fråga kommer att analyseras närmare i avsnitt 4.

45. Till skillnad från anonyma uppgifter (som inte är personuppgifter) är pseudonymiserade uppgifter personuppgifter som kan tillskrivas en fysisk person genom användning av ytterligare information[24]. Pseudonymiserade uppgifter som kan tillskrivas en registrerad – t.ex. när den registrerade tillhandahåller en identifierare som gör en identifiering möjlig, eller när den personuppgiftsansvarige kan koppla uppgifterna till den begärande personen på egen hand – ska därför beaktas inom ramen för begäran[25].

b) Avser begäran den begärande personen (eller den person på vars vägnar den behöriga personen gör begäran)?

46. Som en generell regel får en begäran endast avse uppgifter om den person som gör begäran. Tillgång till andra personers uppgifter kan endast begäras efter beviljat tillstånd[26].

Exempel 7: Den registrerade X arbetar som avdelningschef på ett företag som upplåter parkeringsplatser åt sina chefer på en företagsparkering. Trots att den registrerade X har en egen parkeringsplats så är det utrymmet ofta upptaget när denne anländer till kontoret till sitt andra skift. Eftersom situationen upprepas, och för att identifiera den förare som olovligen utnyttjar den registrerades plats, ber denne den personuppgiftsansvarige för videoövervakningssystemet som

[23] Om begäran inte omfattar även icke personuppgifter som är oupplösligt förenade med den registrerades personuppgifter. Ytterligare förklaringar finns i punkt 100.

[24] Se skäl 26 i dataskyddsförordningen. Ytterligare förklaringar om begreppen anonyma uppgifter och pseudonymiserade uppgifter finns i artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, s. 18–21.

[25] Artikel 29-arbetsgruppen, WP242 rev.01, 5 april 2017, Riktlinjer om rätten till dataportabilitet – godkänd av EDPB (nedan kallade *artikel 29-gruppens riktlinjer om rätten till dataportabilitet*), s. 9.

[26] Se avsnitt 3.4 (”Begäranden som görs via tredje part/fullmaktsinnehavare”).

bevakar kontorets parkeringsplats om tillgång till förarens personuppgifter. I ett sådant fall kommer den registrerade X:s begäran inte att vara en begäran om tillgång till egna personuppgifter, eftersom begäran inte rör den begärande personens uppgifter utan en annan persons uppgifter – och därför bör det inte betraktas som en begäran enligt artikel 15 i dataskyddsförordningen.

c) Gäller andra bestämmelser än dataskyddsförordningen om tillgång till en viss kategori av uppgifter?

47. De registrerade behöver inte ange den rättsliga grunden i sin begäran. Om de registrerade klargör att deras begäran grundar sig på sektorsspecifik lagstiftning eller nationell lagstiftning som reglerar den specifika frågan om tillgång till vissa kategorier av uppgifter, och inte på dataskyddsförordningen, ska en sådan begäran i tillämpliga fall granskas av den personuppgiftsansvarige i enlighet med sådana sektorsspecifika eller nationella bestämmelser. Utifrån relevant nationell lagstiftning kan personuppgiftsansvariga ofta åläggas att lämna separata svar som vart och ett behandlar de särskilda krav som fastställs i de olika lagstiftningsakterna. Detta bör inte förväxlas med nationell lagstiftning eller EU-lagstiftning som fastställer begränsningar av rätten till tillgång vilken måste följas när man besvarar begäranden om tillgång.

48. Om den personuppgiftsansvarige hyser tvivel om vilken rätt den registrerade vill utöva, rekommenderas att den registrerade som gör begäran ombeds förklara föremålet för sin begäran. Sådan korrespondens med den registrerade ska inte påverka den personuppgiftsansvariges skyldighet att agera utan onödigt dröjsmål[27]. Om den personuppgiftsansvarige, i fall där det råder tvivel, ber den registrerade om en ytterligare förklaring och inte får något svar bör den personuppgiftsansvarige, med beaktande av skyldigheten att underlätta utövandet av personens rätt till tillgång, tolka informationen i den första begäran och agera på grundval av den. I enlighet med principen om ansvarsskyldighet kan den personuppgiftsansvarige fastställa en lämplig tidsram inom vilken den registrerade får lämna ytterligare förklaringar. När den personuppgiftsansvarige fastställer tidsramen bör denne lämna tillräckligt med tid för att begäran ska kunna tillgodoses efter att tidsfristen har löpt ut och därför överväga hur lång tid det objektivt sett krävs för att sammanställa och tillhandahålla de begärda uppgifterna när närmare information har (eller inte har) tillhandahållits av den registrerade.

49. Om begäran omfattas av dataskyddsförordningen åsidosätter förekomsten av sådan specifik lagstiftning inte den allmänna tillämpningen av rätten till tillgång, i enlighet med dataskyddsförordningen. Det kan finnas begränsningar som fastställs i EU-lagstiftning eller nationell lagstiftning, när dessa medges enligt artikel 23 i dataskyddsförordningen (se avsnitt 6.4).

d) Faller begäran inom tillämpningsområdet för artikel 15?

50. Det bör noteras att dataskyddsförordningen inte inför några formella krav för personer som begär tillgång till uppgifter. För att framställa en begäran om tillgång räcker det att de begärande personerna anger att de vill veta vilka av deras personuppgifter som den personuppgiftsansvarige behandlar. Den personuppgiftsansvarige kan därför inte vägra att tillhandahålla uppgifterna genom att hänvisa till att uppgifter om den rättsliga grunden för begäran saknas, särskilt inte att det saknas en särskild hänvisning till rätten till tillgång eller till dataskyddsförordningen.

För att göra en begäran bör det till exempel räcka att den begärande personen anger att

- de vill få tillgång till de personuppgifter som rör dem,

[27] Se ytterligare vägledning om val av tidpunkt i avsnitt 5.3.

- de utövar sin rätt till tillgång eller
- att de vill veta vilken information om dem som den personuppgiftsansvarige behandlar.

Man bör ha i åtanke att sökande kanske inte känner till dataskyddsförordningens labyrinter. Därför är det tillrådligt att visa fördragsamhet med personer som utövar sin rätt till tillgång, särskilt när den utövas av minderåriga. Såsom anges ovan rekommenderas den personuppgiftsansvarige att vid tveksamheter be den registrerade som gör en begäran specificera föremålet för sin begäran.

e) Vill de registrerade få tillgång till hela eller delar av den information som behandlas om dem?

51. Dessutom måste den personuppgiftsansvarige bedöma om begärandena som gjorts av de registrerade avser hela eller delar av den information som behandlats om dem. Varje begränsning av tillämpningsområdet för en begäran till en särskild bestämmelse i artikel 15 i dataskyddsförordningen, som de registrerade gör, måste vara tydlig och entydig. Om de registrerade till exempel ordagrant kräver ”information om de uppgifter som behandlas i samband med dem”, bör den personuppgiftsansvarige anta att de registrerade avser att utöva sin fulla rätt enligt artikel 15.1–15.2 i dataskyddsförordningen. En sådan begäran bör inte tolkas som att de registrerade endast vill ta emot de kategorier av personuppgifter som är under behandling och avstå från sin rätt att ta emot de uppgifter som anges i artikel 15.1 a–h. Detta skulle till exempel vara annorlunda om de registrerade, beträffande de uppgifter som de anger, vill ha tillgång till personuppgifternas källa eller ursprung eller till den angivna lagringsperioden. I ett sådant fall får den personuppgiftsansvarige begränsa sitt svar till den specifika information som begärs.

3.1.2 Formen för begäran

52. Som tidigare påpekats innehåller dataskyddsförordningen inga krav på registrerade när det gäller formen för begäran om tillgång till personuppgifter. Därför finns det i princip inga krav enligt dataskyddsförordningen som de registrerade måste iaktta när de väljer vilken kommunikationskanal de använder för att komma i kontakt med den personuppgiftsansvarige.

53. Europeiska dataskyddsstyrelsen EDPB uppmanar personuppgiftsansvariga att tillhandahålla de lämpligaste och mest användarvänliga kommunikationskanalerna, i linje med artikel 12.2 och artikel 25 i dataskyddsförordningen, för att underlätta för den registrerade att göra en effektiv begäran. Om en registrerad gör en begäran med hjälp av en kommunikationskanal som tillhandahålls av den personuppgiftsansvarige[28] men som skiljer sig från den gängse, ska en sådan begäran i allmänhet anses vara giltig ändå och den personuppgiftsansvarige bör hantera en sådan begäran i enlighet därmed (se exemplen nedan). De personuppgiftsansvariga bör göra rimliga insatser för att säkerställa att utövandet av den registrerades rättigheter underlättas (t.ex. om en registrerad skickar en begäran om tillgång till en anställd som är ledig kan ett automatiskt svar som informerar den registrerade om en alternativ kommunikationskanal för denna begäran vara en rimlig insats).

54. Det bör noteras att den personuppgiftsansvarige inte är skyldig att agera på en begäran som skickats till en slumpmässig eller felaktig e-postadress (eller postadress), som inte tillhandahållits direkt av den personuppgiftsansvarige, eller till någon kommunikationskanal som uppenbarligen inte är avsedd att

[28] Detta kan till exempel omfatta den personuppgiftsansvariges kontaktvägar som anges i dennes kommunikation som är riktad direkt till registrerade eller kontaktuppgifter som tillhandahålls offentligt av den personuppgiftsansvarige, t.ex. i integritetspolicyn eller andra obligatoriska rättsliga meddelanden från den personuppgiftsansvarige (t.ex. kontaktinformation till ägare eller företag på en webbplats).

ta emot begäranden som avser den registrerades rättigheter, under förutsättning att den personuppgiftsansvarige har tillhandahållit en lämplig kommunikationskanal som den registrerade kan använda.

55. Den personuppgiftsansvarige är inte heller skyldig att agera på en begäran som skickats till e-postadressen till en anställd hos personuppgiftsansvarig som inte deltar i behandlingen av begäranden som rör registrerades rättigheter (t.ex. chaufförer, städpersonal osv.). En sådan begäran ska inte anses vara giltig om den personuppgiftsansvarige tydligt har tillhandahållit en lämplig kommunikationskanal för registrerade. Om den registrerade skickar en begäran till en anställd hos den personuppgiftsansvarige som har tilldelats den registrerade som ordinarie kontaktperson (t.ex. en personlig kontoansvarig vid en bank eller en fast konsult hos en mobiltelefonoperatör), bör dock en sådan kontakt inte betraktas som slumpmässig och den personuppgiftsansvarige bör göra rimliga ansträngningar för att hantera en sådan begäran så att den kan omdirigeras till kontaktpunkten och besvaras inom de tidsfrister som föreskrivs i dataskyddsförordningen.

56. EDPB rekommenderar ändå, som god praxis, att personuppgiftsansvariga inför lämpliga mekanismer som underlättar utövandet av registrerades rättigheter, bland annat system för automatiskt svar som informerar om personalfrånvaro och en lämplig alternativ kontakt och, om möjligt, mekanismer för att förbättra den interna kommunikationen mellan anställda om begäranden som mottagits av dem som kanske inte är behöriga att hantera sådana.

Exempel 8: Den personuppgiftsansvarige C tillhandahåller, både på sin webbplats och i meddelandet om integritetsskydd, två e-postadresser – den personuppgiftsansvariges allmänna e-postadress: CONTACT@C.COM och e-postadressen till den personuppgiftsansvariges kontaktpunkt för dataskydd: QUERIES@C.COM. Dessutom anger den personuppgiftsansvarige C på sin webbplats att enskilda personer bör vända sig till kontaktpunkten för dataskydd via den angivna e-postadressen för att lämna in eventuella förfrågningar eller göra en begäran om behandling av personuppgifter. Den registrerade skickar ändå en begäran till den personuppgiftsansvariges allmänna e-postadress: CONTACT@C.COM.

I sådana fall bör den personuppgiftsansvarige göra rimliga ansträngningar för att andra serviceenheter ska få kännedom om begäran, som gjorts via det allmänna e-postmeddelandet, så att den kan omdirigeras till kontaktpunkten för dataskydd och besvaras inom de tidsfrister som föreskrivs i dataskyddsförordningen. Dessutom har den personuppgiftsansvarige inte rätt att förlänga tidsfristen för att besvara en begäran, enbart på grund av att den registrerade har skickat en begäran till den personuppgiftsansvariges allmänna e-postadress i stället för till den personuppgiftsansvariges e-postadress för dataskydd.

Exempel 9: Personuppgiftsansvarig Y har ett nätverk av friskvårdsanläggningar. Personuppgiftsansvarig Y anger på sin webbplats och i meddelandet om integritetsskydd till friskvårdsanläggningarnas kunder att enskilda personer som vill lämna in förfrågningar eller göra en begäran som rör behandling av personuppgifter får kontakta personuppgiftsansvarig på följande e-postadress: QUERIES@Y.COM. Den registrerade skickar dock en begäran till en e-postadress som finns i omklädningsrummet, där han hittat ett meddelande med texten ”Om du inte är nöjd med städningen av rummet, kontakta oss på: CLEANERS@Y.COM”, vilket är e-postadressen till den städpersonal som är anställd av Y. Städpersonalen är uppenbarligen inte involverad i hanteringen av frågor som rör utövandet av de registrerades – friskvårdsanläggningens kunders – rättigheter. Även om e-postadressen fanns tillgänglig i friskvårdsanläggningens lokaler kunde den registrerade inte rimligen förvänta sig att detta var en lämplig kontaktadress för sådana begäranden, eftersom det tydligt

informerades på webbplatsen och i meddelandet om integritetsskydd om vilken kommunikationskanal som skulle användas för att utöva de registrerades rättigheter.

57. Datumet för den personuppgiftsansvariges mottagande av begäran är i regel utlösande för den period på en månad under vilken den personuppgiftsansvarige ska lämna information om åtgärder som vidtagits beträffande en begäran, i enlighet med artikel 12.3 i dataskyddsförordningen (ytterligare vägledning om tidpunkt ges i avsnitt 5.3). EDPB anser att det är god praxis för de personuppgiftsansvariga att skriftligen bekräfta mottagandet av begäranden, t.ex. genom att skicka e-postmeddelanden (eller information per post, i förekommande fall) till de begärande personer som bekräftar att deras begäran har mottagits och att perioden på en månad löper från dag X till dag Y.

3.2 Identifiering och autentisering

58. För att säkerställa säkerheten vid behandlingen och minimera risken för otillåtet utlämnande av personuppgifter måste den personuppgiftsansvarige kunna ta reda på vilka uppgifter som avser den registrerade (identifiering) och bekräfta identiteten hos den personen (autentisering).

59. Det är värt att erinra om att den personuppgiftsansvarige inte behöver bibehålla identifieringen av en registrerad enbart i syfte att efterleva de registrerades rättigheter när det ändamål för vilket personuppgifterna behandlas inte eller inte längre kräver detta, även mot bakgrund av principen om uppgiftsminimering. Sådana situationer behandlas i artikel 11.1 i dataskyddsförordningen.

60. Det anges i artikel 12.2 i dataskyddsförordningen att den personuppgiftsansvarige inte får vägra att tillmötesgå den registrerades begäran att utöva sina rättigheter, såvida inte den personuppgiftsansvarige behandlar personuppgifter för ett ändamål som inte kräver identifiering av den registrerade och visar att denne inte kan identifiera den registrerade. Under sådana omständigheter kan den registrerade ändå besluta att tillhandahålla ytterligare information som möjliggör denna identifiering (artikel 11.2 i dataskyddsförordningen)[29].

61. Den personuppgiftsansvarige är inte skyldig att inhämta sådan ytterligare information för att identifiera den registrerade enbart i syfte att tillmötesgå den registrerades begäran, även mot bakgrund av principen om uppgiftsminimering. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat som stöd för utövandet av sina rättigheter (skäl 57 i dataskyddsförordningen).

Exempel 10: C är personuppgiftsansvarig för de uppgifter som behandlas i samband med videoövervakningen av en byggnad. I enlighet med artikel 11.1 i dataskyddsförordningen är den personuppgiftsansvarige inte skyldig att identifiera alla personer som har registrerats av en säkerhetskamera som en del av övervakningen (syftet kräver inte identifiering). Den personuppgiftsansvarige tar emot en begäran om tillgång till personuppgifter från en person som hävdar att de har spelats in av den personuppgiftsansvariges videoövervakning. Den personuppgiftsansvariges åtgärder beror på den ytterligare information som lämnas. Om den begärande personen anger en viss dag och tid när kamerorna kan ha spelat in händelsen i fråga är det troligt att den personuppgiftsansvarige kommer att kunna tillhandahålla dessa uppgifter (artikel 11.2 i dataskyddsförordningen). Om den personuppgiftsansvarige inte kan identifiera den registrerade (t.ex. om det är omöjligt för den personuppgiftsansvarige att vara säker på att en begärande person faktiskt är den registrerade eller om begäran t.ex. rör en lång period av inspelningar och en personuppgiftsansvarig inte kan behandla en så stor uppgiftsmängd) får den personuppgiftsansvarige

[29] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 13.

vägra att vidta åtgärder om denne visar att den registrerade inte kan identifieras (artikel 12.2 i dataskyddsförordningen).

Exempel 11: En personuppgiftsansvarig C behandlar personuppgifter för att hantera beteendereklam till sina webbanvändare. Personuppgifter som samlas in för beteendereklam samlas vanligtvis in med hjälp av kakor och associeras med pseudonymiska slumpmässiga identifierare. En registrerad herr X utövar sin rätt att få tillgång i förhållande till C via C:s webbplats. C kan identifiera herr X exakt och se den registrerades beteendereklam genom att länka herr X:s terminalutrustning till sin reklamprofil med de angivna kakorna i terminalen. C bör då också kunna identifiera herr X för att bevilja honom tillgång till hans personuppgifter, eftersom det finns en länk mellan de uppgifter som behandlas och den registrerade. Med beaktande av principerna i dataskyddsförordningen skulle ovanstående exempel därför inte omfattas av artikel 11 i dataskyddsförordningen. I exemplet ovan kräver C:s syften att den registrerade identifieras, medan artikel 11 i dataskyddsförordningen gäller en behandlingssituation som inte kräver identifiering där en personuppgiftsansvarig inte är skyldig att behandla ytterligare uppgifter i den mening som avses i artikel 11.1 i dataskyddsförordningen enbart för att kunna uppfylla kraven i dataskyddsförordningen. I vissa fall bör därför inga ytterligare uppgifter begäras för att den registrerades rättigheter ska kunna utövas.

Men om herr X försöker utöva sin rätt till tillgång direkt via e-post eller reguljär post kommer C i detta sammanhang inte att ha något annat val än att be herr X tillhandahålla ”ytterligare information” (artikel 12.6 i dataskyddsförordningen) för att kunna identifiera den reklamprofil som är kopplad till herr X. I detta fall är den kompletterande informationen den identifierare av kakor som lagras i terminalutrustningen hos herr X.

62. Om det visar sig vara omöjligt att identifiera den registrerade (artikel 11 i dataskyddsförordningen) måste den personuppgiftsansvarige om möjligt informera den registrerade om detta, eftersom den personuppgiftsansvarige ska svara på den registrerades begäran utan onödigt dröjsmål och ange skäl i de fall där denne inte avser att tillmötesgå en sådan begäran. Denna information behöver endast tillhandahållas ”om möjligt”, eftersom den personuppgiftsansvarige kanske inte kan informera den registrerade om denne inte kan identifieras.

63. Oavsett om behandlingen kräver identifiering eller inte får den personuppgiftsansvarige begära att ytterligare information lämnas som krävs för att bekräfta den registrerades identitet, om den personuppgiftsansvarige har rimliga tvivel om identiteten hos den fysiska person som gör begäran (artikel 12.6 i dataskyddsförordningen).

64. Dataskyddsförordningen innehåller inga krav på hur den registrerade ska autentiseras. I artiklarna 11 och 12 i dataskyddsförordningen anges dock villkoren för utövandet av alla registrerades rättigheter, inbegripet rätten till tillgång till personuppgifter.

65. Man bör ha i åtanke att den personuppgiftsansvarige i regel inte kan begära fler personuppgifter än vad som är nödvändigt för att möjliggöra denna autentisering, och att användningen av sådan information strikt bör begränsas till att uppfylla de registrerades begäran.

66. Autentiseringsförfaranden finns ofta redan mellan de registrerade och de personuppgiftsansvariga. De personuppgiftsansvariga får använda dessa autentiseringsförfaranden för att fastställa identiteten hos de registrerade som begär sina personuppgifter eller utövar de rättigheter som beviljas i

dataskyddsförordningen[30]. I annat fall bör personuppgiftsansvariga införa ett autentiseringsförfarande för att göra detta[31].

67. Om den personuppgiftsansvarige begär eller får den ytterligare information av den registrerade som krävs för att bekräfta den registrerades identitet, ska den personuppgiftsansvarige vid varje enskilt tillfälle bedöma vilken information som gör det möjligt att bekräfta den registrerades identitet och eventuellt ställa kompletterande frågor till den begärande personen eller begära att den registrerade lägger fram ytterligare identifieringsuppgifter, om detta är proportionerligt (se avsnitt 3.3).

68. För att göra det möjligt för den registrerade att tillhandahålla den ytterligare information som krävs för att identifiera dennes uppgifter bör den personuppgiftsansvarige informera den registrerade om vilken typ av ytterligare information som krävs för identifiering. Sådan ytterligare information bör inte vara mer än den information som ursprungligen behövdes för att autentisera den registrerade. Generellt sett får den personuppgiftsansvariges möjlighet att begära ytterligare information för att bedöma den registrerades identitet inte leda till orimliga krav och insamling av personuppgifter som inte är relevanta eller nödvändiga för att styrka kopplingen mellan den enskilda personen och de begärda personuppgifterna[32].

69. Om den information som samlas in online är kopplad till pseudonymer eller andra unika identifierare kan den personuppgiftsansvarige därför införa lämpliga förfaranden som gör det möjligt för den begärande personen att göra en begäran om tillgång till uppgifter och ta emot de uppgifter som rör dem[33].

Exempel 12: Den registrerade fröken X begär tillgång till sina uppgifter i ett samtal med en konsult från ett elbolag som hon har ingått avtal med. Konsulten, som hyser tvivel om identiteten hos den person som gör begäran, genererar i företagets system en engångskod som skickas till användarens mobilnummer som uppgavs när kontot inrättades, som en del av det dubbla kontrollsystemet, en åtgärd som bör anses vara proportionerlig i detta fall.

3.3 Proportionalitetsbedömning avseende autentisering av den begärande personen

70. Om den personuppgiftsansvarige har rimliga skäl att tvivla på den begärande personens identitet får denne, såsom anges ovan, begära ytterligare information för att bekräfta den registrerades identitet. Den personuppgiftsansvarige måste ändå samtidigt se till att inte samla in fler personuppgifter än vad som är nödvändigt för att möjliggöra en autentisering av den begärande personen. Den personuppgiftsansvarige ska därför göra en proportionalitetsbedömning som tar hänsyn till den typ av personuppgifter som behandlas (t.ex. särskilda kategorier av uppgifter eller inte), typen av begäran, det sammanhang inom vilket begäran görs samt eventuell skada som skulle kunna uppstå till följd av otillbörligt röjande. Vid bedömningen av proportionaliteten bör man komma ihåg att undvika orimlig uppgiftsinsamling och samtidigt säkerställa en adekvat säkerhetsnivå vid databehandlingen.

71. Den personuppgiftsansvarige bör införa ett autentiseringsförfarande för att vara säker på identiteten hos de personer som begär tillgång till sina uppgifter[34] och sörja för säkerheten i behandlingen under

[30] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 14.
[31] Se ytterligare vägledning beträffande autentisering i avsnitt 3.3.
[32] Se ovan, s. 14.
[33] Se ovan, s. 13–14.
[34] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 14.

hela hanteringen av en begäran om tillgång i enlighet med artikel 32 i dataskyddsförordningen, t.ex. en säker kanal där de registrerade kan lämna ytterligare information. Den metod som används för autentisering bör vara relevant, lämplig, proportionell och förenlig med principen om uppgiftsminimering. Om den personuppgiftsansvarige inför belastande åtgärder som syftar till att autentisera den registrerade måste denne motivera detta på lämpligt sätt och säkerställa efterlevnaden av alla grundläggande principer, inklusive uppgiftsminimering och skyldigheten att underlätta utövandet av registrerades rättigheter (artikel 12.2 i dataskyddsförordningen).

72. I ett online-sammanhang kan autentiseringsmekanismen innehålla samma uppgifter för behörighet som den registrerade använder för att logga in på den onlinetjänst som den personuppgiftsansvarige erbjuder (skäl 57 i dataskyddsförordningen)[35].

73. I praktiken finns det ofta autentiseringsförfaranden och personuppgiftsansvariga behöver inte införa ytterligare skyddsåtgärder för att förhindra otillåten tillgång till tjänster. För att enskilda personer ska kunna få tillgång till uppgifterna på sina konton (t.ex. ett e-postkonto, ett konto i sociala nätverk eller onlinebutiker) är det högst sannolikt att personuppgiftsansvariga begär loggning i form av användarens inloggning och lösenord, vilket i sådana fall bör vara tillräckligt för att autentisera en registrerad[36]. Dessutom är de registrerade ofta redan autentiserade av den personuppgiftsansvarige innan ett avtal ingås eller deras samtycke inhämtas till behandlingen, och de personuppgifter som används för att registrera den berörda personen vid behandlingen kan därför också användas som bevis för att autentisera den registrerade för tillgångsändamål[37]. Följaktligen är det oproportionerligt att kräva en kopia av en identitetshandling om den registrerade som gör en begäran redan har autentiserats av den personuppgiftsansvarige.

74. Det bör poängteras att användningen av en kopia av en identitetshandling som en del av autentiseringsprocessen skapar en risk för säkerheten för personuppgifterna och kan leda till otillåten eller olaglig behandling, och som sådan bör den anses olämplig, såvida den inte är nödvändig, passande och i linje med nationell lagstiftning. I sådana fall bör personuppgiftsansvariga ha infört system som säkerställer en säkerhetsnivå som är lämplig för att minska de högre riskerna för den registrerades rättigheter och friheter när sådana uppgifter tas emot. Det är också viktigt att notera att autentisering med hjälp av ett identitetskort inte nödvändigtvis är till nytta online (t.ex. genom användning av pseudonymer) om den berörda personen inte kan bidra med annan bevisning, t.ex. ytterligare egenskaper som matchar användarkontot.

75. Med tanke på att många företag (t.ex. hotell, banker, biluthyrningsfirmor) begär kopior av sina kunders id-kort bör det i allmänhet inte anses vara ett lämpligt sätt för autentisering. Alternativt kan den personuppgiftsansvarige vidta en snabb och effektiv säkerhetsåtgärd för att identifiera en registrerad utifrån den autentisering som tidigare har utförts, t.ex. via e-post eller SMS som innehåller bekräftelselänkar, säkerhetsfrågor eller bekräftelsekoder[38].

76. Information på id-handlingen som inte är nödvändig för att bekräfta den registrerades identitet, t.ex. referens- och serienummer, nationalitet, längd, ögonfärg, foto och ett maskinläsbart fält, kan – utifrån

---

[35] Se ytterligare vägledning om autentiseringsmetoder i EDPB:s riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter, antagna den 14 januari 2021, s. 30–31, och i EDPB:s *riktlinjer 02/2021 för användning av virtuella röstassistenter*, version 2.0, antagna den 7 juli 2021, avsnitt 3.7.

[36] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 14.

[37] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 14.

[38] Se även Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

en bedömning från fall till fall – redigeras eller döljas av den registrerade innan handlingen lämnas till den personuppgiftsansvarige, utom i de fall där nationell lagstiftning kräver en fullständig oredigerad kopia av identitetshandlingen (se punkt 78 nedan). I allmänhet räcker datum för utfärdande eller sista giltighetsdag, utfärdande myndighet och fullständig namnmatchning med onlinekontot för att den personuppgiftsansvarige ska kunna kontrollera identiteten, alltid under förutsättning att kopians äkthet och förhållandet till sökanden säkerställs. Ytterligare information, såsom den registrerades födelsedatum, kan endast krävas om risken för felaktig identitet kvarstår, om den personuppgiftsansvarige kan jämföra den med den information som denne redan behandlar.

77. För att följa principen om uppgiftsminimering bör den personuppgiftsansvarige informera den registrerade om vilken information som inte behövs och om möjligheten att redigera eller dölja dessa delar av id-handlingen. I sådana fall, om den registrerade inte vet hur eller inte kan redigera sådan information, är det god praxis för den personuppgiftsansvarige att redigera den vid mottagandet av handlingen, om detta är möjligt för den personuppgiftsansvarige, med beaktande av de medel som står till den personuppgiftsansvariges förfogande under de givna omständigheterna.

Exempel 13: Användaren fröken Y har skapat ett lösenordsskyddat konto i onlinearkivet och angett sin e-post och/eller sitt användarnamn. Därefter begär kontoinnehavaren information av personuppgiftsansvarige om huruvida denne behandlar hennes personuppgifter och begär i sådant fall tillgång till dessa inom det tillämpningsområde som anges i artikel 15. Den personuppgiftsansvarige begär en identitetshandling av den person som gör begäran för att bekräfta hennes identitet. Den personuppgiftsansvariges agerande i detta fall är oproportionerligt och leder till onödig datainsamling.

För att bekräfta identiteten hos den begärande personen och samtidigt förhindra onödig datainsamling skulle den personuppgiftsansvarige i stället kunna kräva att hon autentiserar sig genom att logga in på kontot eller ställa (icke-påträngande) säkerhetsfrågor till henne, som endast den registrerade kan veta svaret på, eller använda den multifaktorautentisering som konfigurerades när den registrerade registrerade sitt konto, eller använda andra befintliga kommunikationsmedel som man vet tillhör den registrerade, såsom e-postadress eller telefonnummer, för att skicka ett lösenord för åtkomst.

Exempel 14: En bankkund, herr Y, planerar att skaffa en konsumentkredit. För detta ändamål går herr Y till en bankfilial för att få den information, inklusive hans personliga uppgifter, som krävs för att bedöma hans kreditvärdighet. För att kontrollera den registrerades identitet ber konsulten om en certifiering från en notarie av den registrerades identitet för att kunna förse honom med den begärda informationen.

Den personuppgiftsansvarige ska inte kräva en notariebekräftelse av identiteten, annat än om det är nödvändigt, lämpligt och i linje med nationell lagstiftning (t.ex. om en person tillfälligt saknar identitetshandling och det krävs bevis på den registrerades identitet enligt nationell lagstiftning för att en rättsakt ska kunna upprättas). Denna praxis utsätter de begärande personerna för extra kostnader och lägger en alltför stor börda på de registrerade, vilket hindrar dem från att utöva sin rätt till tillgång.

78. Utan att det påverkar tillämpningen av ovannämnda allmänna principer kan autentisering på grundval av en id-handling under vissa omständigheter vara en motiverad och proportionell åtgärd, i synnerhet för enheter som behandlar särskilda kategorier av personuppgifter eller utför databehandling som kan utgöra en risk för den registrerade (t.ex. medicinsk information eller hälsoinformation). Samtidigt bör man komma ihåg att vissa nationella bestämmelser föreskriver begränsningar för behandling av uppgifter i offentliga handlingar, inbegripet handlingar som bekräftar en persons identitet (även på

grundval av artikel 87 i dataskyddsförordningen). Begränsningar av behandlingen av uppgifter från sådana dokument kan särskilt gälla skanning eller kopiering av id-kort eller behandling av officiella personliga id-nummer[39].

79. Mot bakgrund av ovanstående måste den personuppgiftsansvarige, om en id-handling begärs (och detta är både i linje med nationell lagstiftning och motiverat och proportionellt enligt dataskyddsförordningen), införa skyddsåtgärder för att förhindra en olaglig behandling av id-handlingen. Oberoende av eventuella tillämpliga nationella bestämmelser om id-autentisering kan detta inbegripa att avstå från att göra en kopia eller ta bort en kopia av id-handlingen omedelbart efter det att den registrerades identitet har autentiserats. Detta beror på att vidare lagring av en kopia av en id-handling sannolikt kommer att innebära en överträdelse av principerna om ändamålsbegränsning och lagringsminimering (artikel 5.1 b och e i dataskyddsförordningen) och dessutom nationell lagstiftning om behandling av det nationella id-numret (artikel 87 i dataskyddsförordningen). EDPB rekommenderar, som god praxis, att den personuppgiftsansvarige, efter att ha kontrollerat id-kortet, gör en anteckning, t.ex. ”id-kort har kontrollerats” för att undvika onödig kopiering eller lagring av kopior av id-kort.

3.4 Begäranden som görs via tredje part/fullmaktsinnehavare

80. Även om rätten till tillgång i allmänhet utövas av de registrerade som den hänför sig till, är det möjligt för en tredje part att göra en begäran på den registrerades vägnar. Detta kan bland annat gälla åtgärder genom en fullmaktsinnehavare eller förmyndare på minderårigas vägnar, samt åtgärder genom andra enheter via onlineportaler. I vissa fall kan identiteten hos den person som är bemyndigad att utöva rätten till tillgång och bemyndiganden att agera på den registrerades vägnar kräva kontroll, där det är lämpligt och proportionerligt (se avsnitt 3.3 ovan)[40]. Det bör erinras om att det kan innebära en personuppgiftsincident om personuppgifter görs tillgängliga för någon som inte har rätt att få tillgång till dem[41].

81. Därvid bör hänsyn tas till nationella lagar som reglerar juridiskt ombud (t.ex. fullmakter), med särskilda krav på att ett bemyndigande ska visas vid inlämnande av en begäran på den registrerades vägnar, eftersom dataskyddsförordningen inte reglerar denna fråga. I enlighet med principen om ansvarsskyldighet och andra dataskyddsprinciper ska personuppgiftsansvariga kunna visa att det finns ett relevant bemyndigande för att lämna in en begäran på den registrerades vägnar och att ta emot den begärda informationen, utom när den nationella lagstiftningen säger något annat (t.ex. när nationell lagstiftning innehåller särskilda regler om advokaters tillförlitlighet) där den personuppgiftsansvarige får kontrollera fullmaktsinnehavarens identitet (t.ex. när advokater kontrollerar inskrivningen i advokatyrket). Det rekommenderas därför att lämplig dokumentation samlas in i detta avseende, i fråga om de tidigare angivna allmänna reglerna om identitetsbekräftelse för en fysisk person som gör en begäran, och om den personuppgiftsansvarige hyser rimliga tvivel om identiteten hos en person som agerar på den registrerades vägnar ska denne begära ytterligare information för att bekräfta denna persons identitet.

[39] Flera medlemsstater har infört begränsningar i sina nationella bestämmelser i det avseendet och som exempel angett att kopiering av id-kort endast är laglig om den sker som en direkt följd av bestämmelserna i en rättsakt.

[40] När det gäller tidsfristerna för utövande av rätten till tillgång när den personuppgiftsansvarige behöver ytterligare information, se punkt 157.

[41] Artiklarna 4.12 i dataskyddsförordningen.

82. Utövandet av rätten till tillgång till personuppgifter för avlidna personer utgör ett annat exempel på tillgång för en tredje part, annan än den registrerade, men i skäl 27 anges att dataskyddsförordningen inte är tillämplig på avlidna personers personuppgifter. Frågan behandlas därför i nationell lagstiftning och medlemsstaterna får utfärda bestämmelser om behandling av avlidna personers personuppgifter. Man bör dock ha i åtanke att uppgifterna dessutom kan avse nu levande tredje personer, t.ex. i samband med begärd tillgång till en avliden persons korrespondens. Sådana uppgifters konfidentialitet måste fortfarande skyddas.

3.4.1 Utövande av rätten till tillgång på barns vägnar

83. Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om risker, följder och skyddsåtgärder som gäller deras rättigheter i fråga om behandling av personuppgifter[42]. All information och kommunikation till ett barn, där personuppgifter om ett barn behandlas, ska uttryckas på ett tydligt språk så att barnet lätt kan förstå[43].

84. Barn är registrerade i sig själva och som sådana tillhör rätten till tillgång barnet. Beroende på barnets mognad och förmåga kan barnet behöva en tredje part som agerar på barnets vägnar, t.ex. personen med föräldraansvar.

85. Barnets bästa bör vara en ledande omständighet i alla beslut som fattas i fråga om utövandet av rätten till tillgång i samband med barn, särskilt när rätten till tillgång utövas på barnets vägnar, till exempel av personen med föräldraansvar.

86. På grund av det särskilda skyddet av barns personuppgifter i dataskyddsförordningen ska den personuppgiftsansvarige vidta lämpliga åtgärder för att undvika att en minderårigs personuppgifter röjs för en obehörig person (se även avsnitt 3.4 ovan).

87. Slutligen bör rätten för personen med föräldraansvar att agera på barnets vägnar inte förväxlas med exempel utanför dataskyddslagstiftningen, där nationell lagstiftning kan ge personen med föräldraansvar rätt att begära och ta emot information om barnet (t.ex. om barnets prestation i skolan).

3.4.2 Utövande av rätten till tillgång via portaler/kanaler som tillhandahålls av tredje part

88. Det finns företag som tillhandahåller tjänster som gör det möjligt för registrerade att begära tillgång via en portal. Den registrerade loggar in och får tillgång till en portal genom vilken de t.ex. kan skicka in en begäran om tillgång, begära rättelse av uppgifter eller radering av uppgifter från olika personuppgiftsansvariga. Olika frågor uppstår till följd av användningen av portaler som tillhandahålls av en tredje part.

89. Det första som personuppgiftsansvariga måste ta itu med i den situationen är att säkerställa att tredje part har rätt att agera på den registrerades vägnar, eftersom de måste se till att inga uppgifter lämnas ut till obehöriga parter.

---

[42] Skäl 38 i dataskyddsförordningen. Det framgår av EDPB:s arbetsprogram att avsikten är att ge vägledning om barns uppgifter. En sådan handling förväntas ge mer vägledning om under vilka förhållanden ett barn kan utöva sin egen rätt till tillgång och när personen med föräldraansvar kan utöva rätten till tillgång på barnets vägnar.
[43] Skäl 58 i dataskyddsförordningen. EDPB:s riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, avsnitt 7.

90. Dessutom måste en personuppgiftsansvarig som tar emot en begäran via en sådan portal alltid hantera begäran i rimlig tid[44]. Den personuppgiftsansvarige är dock inte skyldig att tillhandahålla uppgifterna enligt artikel 15 i dataskyddsförordningen direkt i portalen, om den personuppgiftsansvarige till exempel konstaterar att säkerhetsåtgärderna är otillräckliga eller anser det lämpligt att använda ett annat sätt att lämna ut uppgifter till den registrerade. Under sådana omständigheter, där den personuppgiftsansvarige har andra förfaranden för hantering av begäranden om tillgång på ett effektivt och säkert sätt, kan den personuppgiftsansvarige tillhandahålla den begärda informationen genom dessa.

4 TILLÄMPNINGSOMRÅDET FÖR TILLGÅNG OCH DE PERSONUPPGIFTER OCH DEN INFORMATION SOM AVSES

91. Syftet med detta avsnitt är att belysa definitionen av personuppgifter (4.1) och klargöra omfattningen av den information som är föremål för rätten till tillgång rent generellt (4.2 och 4.3). Det bör noteras att omfattningen av begreppet personuppgifter och därmed skillnaden mellan personuppgifter och andra uppgifter ingår i den bedömning som personuppgiftsansvarig gör för att identifiera omfattningen av de uppgifter som den registrerade har rätt att få tillgång till[45].

92. Som ett preliminärt övervägande bör det erinras om att rätten till tillgång endast kan utövas med avseende på behandling av personuppgifter som omfattas av dataskyddsförordningens materiella och territoriella tillämpningsområde. Personuppgifter som inte behandlas automatiskt eller som inte ingår i eller kommer att ingå i ett register enligt artikel 2.1 i dataskyddsförordningen eller som behandlas av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll enligt artikel 2.2 i dataskyddsförordningen omfattas därför inte av rätten till tillgång.

4.1 Definition av personuppgifter

93. Artikel 15.1 och 15.3 i dataskyddsförordningen hänvisar till ”personuppgifter” respektive ”personuppgifter som är under behandling”. Tillämpningsområdet för rätten till tillgång avgörs därför i första hand av omfattningen av begreppet personuppgifter enligt definitionen i artikel 4.1 i dataskyddsförordningen[46]. Begreppet personuppgifter har redan varit föremål för flera av artikel 29-

[44] Angående tidsfristerna för utövande av rätten till tillgång när den personuppgiftsansvarige behöver ytterligare information se punkt 157.

[45] I enlighet med principen om inbyggt integritetsskydd är en sådan analys en del av bedömningen av lämpliga åtgärder och skyddsåtgärder för att skydda principerna om dataskydd och de registrerades rättigheter, som utförs vid tidpunkten för ”fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen”, där t.ex. en kortare svarstid när de registrerade utövar sina rättigheter kan vara ett av måtten. Ytterligare förklaringar finns i riktlinjerna 4/2019 om artikel 25 om inbyggt dataskydd och dataskydd som standard.

[46] Enligt artikel 4.1 i dataskyddsförordningen avses med ”personuppgifter” ”varje upplysning som avser en identifierad eller identifierbar fysisk person (*en registrerad*), en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

arbetsgruppens[47] dokument[48] och har tolkats av EU-domstolen, bland annat inom ramen för rätten till tillgång enligt artikel 12 i direktiv 95/46/EG.

94. Artikel 29-gruppen ansåg att definitionen av personuppgifter i direktiv 95/46/EG avspeglar EU:s lagstiftares intention med en bred definition av ”personuppgifter”[49]. Enligt dataskyddsförordningen avser definitionen fortfarande ”varje upplysning som avser en identifierad eller identifierbar fysisk person”. Bortsett från grundläggande personuppgifter som namn och adress, telefonnummer osv. kan en obegränsad, bred variation av uppgifter omfattas av denna definition, inklusive medicinska uppgifter, köphistorik, kreditvärdighetsindikatorer, kommunikationsinnehåll osv. Med tanke på den omfattande definitionen av personuppgifter skulle en restriktiv bedömning från den personuppgiftsansvarige av denna leda till en felaktig klassificering av personuppgifter[50] och i slutändan till en kränkning av rätten till tillgång.

95. I de förenade målen C-141/12 och C-372/12[51] slog EU-domstolen fast att rätten till tillgång omfattade personuppgifter i protokoll, nämligen ”namn, födelsedata, nationalitet, kön, etnicitet, religion och språk” och ”i förekommande fall, uppgifterna i den rättsliga analys som finns i ansökningsprotokollet”, men inte den rättsliga analysen i sig[52]. Den rättsliga analysen var i detta sammanhang inte föremål för den registrerades kontroll av dess riktighet eller en rättelse. Att ge tillgång till den rättsliga analysen uppfyller inte heller syftet att garantera integriteten, utan tillgång till administrativa handlingar.

96. I målet Nowak[53] gjorde EU-domstolen en bredare analys och kom fram till att skriftliga svar från en kandidat i en yrkesexamen och eventuella kommentarer från en examinator avseende dessa svar utgör personuppgifter som rör examinanden. Närmare bestämt är sådan subjektiv information personuppgifter ”i form av åsikter eller bedömningar, under förutsättning att upplysningarna ’avser’ den registrerade”[54] i motsats till examineringsfrågorna, som inte betraktas som personuppgifter[55]. En kontextuell bedömning bör därför belysa effekten eller resultatet som en information kan leda till för en enskild person och därmed omfattningen av rätten till tillgång.

Exempel 15: En person är på anställningsintervju hos ett företag. I samband med det överlämnar den arbetssökande en meritförteckning och ett ansökningsbrev. Under intervjun tar HR-tjänstemannen anteckningar på en dator som en dokumentation av intervjun. Efteråt begär den arbetssökande, i egenskap av registrerad, tillgång till personuppgifter om honom eller henne som företaget i egenskap av personuppgiftsansvarig samlat in under rekryteringsförfarandet.

Den personuppgiftsansvarige är skyldig att ge den registrerade personuppgifter som denne aktivt överfört i sin meritförteckning och sitt ansökningsbrev. Dessutom måste den personuppgiftsansvarige

[47] Artikel 29-arbetsgruppen är den oberoende europeiska arbetsgrupp som behandlade frågor som rör skydd av privatlivet och personuppgifter fram till och med den 25 maj 2018 (då dataskyddsförordningen trädde ikraft), föregångaren till EDPB.
[48] T.ex. WP251 rev01 Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, s. 19, artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 9.
[49] Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, s. 4.
[50] Som information som inte avser en identifierad eller identifierbar fysisk person.
[51] Domstolens dom av den 17 juli 2014 i förenade målen C-141/12 och C-372/12, YS/Minister voor Immigratie, Integratie en Asiel och Minister voor Immigratie, Integratie en Asiel/M och S.
[52] Domstolens dom i förenade målen C-141/12 och C-372/12, YS m.fl., punkterna 38 och 48.
[53] Domstolens dom av den 20 december 2017 i mål C-434/16, Peter Nowak/dataskyddskommissionären.
[54] Domstolens dom i mål C-434/16, Nowak, punkterna 34–35.
[55] Domstolens dom i mål C-434/16, Nowak, punkt 58.

ge den registrerade en sammanfattning av intervjun, inklusive subjektiva kommentarer om den registrerades beteende som HR-tjänstemannen skrev under anställningsintervjun, med förbehåll för eventuella undantag enligt nationell lagstiftning och i enlighet med artikel 23 i dataskyddsförordningen.

97. När en särskild begäran om tillgång bedöms ska bland annat följande typer av uppgifter tillhandahållas av personuppgiftsansvarige, med förbehåll för de specifika omständigheterna i fallet, utan att det påverkar tillämpningen av artikel 15.4 i dataskyddsförordningen:

- Särskilda kategorier av personuppgifter enligt artikel 9 i dataskyddsförordningen.
- Personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott enligt artikel 10 i dataskyddsförordningen.
- Uppgifter som den registrerade medvetet och aktivt tillhandahåller (t.ex. kontouppgifter som lämnas via formulär, svar på frågeformulär)[56].
- Observerade data eller rådata som tillhandahålls av den registrerade genom användning av tjänsten eller enheten (t.ex. uppgifter som behandlas av anslutna objekt, transaktionshistorik, aktivitetsloggar såsom åtkomstloggar, webbhistorik, sökaktiviteter, lokaliseringsuppgifter, klickaktivitet, unika aspekter av en persons beteende, t.ex. handstil, tangenttryckningar, särskilt sätt att gå eller tala)[57].
- Uppgifter som härletts från andra uppgifter, snarare än direkt från den registrerade (t.ex. kreditkvot, klassificering baserad på gemensamma attribut för registrerade, bosättningsland härlett från postnummer)[58].
- Data som härletts från andra uppgifter i stället för direkt från den registrerade (t.ex. för att genomgå en kreditkontroll eller följa reglerna för bekämpning av penningtvätt, algoritmiska resultat, resultat av en hälsokontroll eller ett individanpassat förfarande eller rekommendationsförfarande)[59].
- Pseudonymiserade uppgifter i motsats till anonymiserade uppgifter (se även avsnitt 3 i dessa riktlinjer).

Exempel 16: Uppgifter som har använts för att fatta beslut om t.ex. arbetstagarens befordran, löneökning eller nya arbetsuppgifter (t.ex. årlig prestationsöversyn, utbildningsönskemål, dokumenterade disciplinära åtgärder, prioriteringsordning, karriärpotential) är personuppgifter som rör den anställde. Således kan den registrerade på begäran få tillgång till sådana uppgifter med iakttagande av artikel 15.4 i dataskyddsförordningen i de fall personuppgifter till exempel även rör en annan person (t.ex. kan identiteten eller uppgifter som röjer identiteten hos en annan anställd, vars vittnesbörd om den yrkesmässiga prestationen ingår i en årlig prestationsöversyn, bli föremål för begränsningar enligt artikel 15.4 i dataskyddsförordningen och därför är det möjligt att de inte kan meddelas den registrerade för att skydda den andra anställdes rättigheter och friheter). Nationella arbetsrättsliga bestämmelser kan dock tillämpas t.ex. när det gäller anställdas tillgång till personalakter, eller andra nationella bestämmelser, t.ex. bestämmelser om tystnadsplikt. Under alla omständigheter måste sådana begränsningar av den registrerades rätt till tillgång (eller andra

[56] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 9.
[57] Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, s. 8.
[58] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 10–11.
[59] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 10–11. Artikel 29-arbetsgruppen, WP 251 rev.01, 6 februari 2018, Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 – godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 – godkända av EDPB*), s. 9–10.

rättigheter) enligt nationell lagstiftning uppfylla villkoren i artikel 23 i dataskyddsförordningen (se avsnitt 6.4).

98. Flera överväganden kan göras av den ovan nämnda icke uttömmande förteckningen över personuppgifter som kan lämnas till den registrerade i samband med en begäran om tillgång. Det framgår tydligt av ovanstående att den personuppgiftsansvarige inte får göra åtskillnad när det gäller att ge tillgång till personuppgifter mellan uppgifter som finns i pappersfiler och uppgifter som lagrats elektroniskt, så länge som de omfattas av dataskyddsförordningen. Personuppgifter som finns i pappersfiler som en del av ett register, eller är avsedda att ingå i ett register, omfattas med andra ord av rätten till tillgång på samma sätt som personuppgifter som lagras i ett datorminne med hjälp av t.ex. binär kod eller videoband.

99. I likhet med de flesta registrerades rättigheter omfattar dessutom rätten till tillgång härledda uppgifter, inklusive personuppgifter som skapats av en tjänsteleverantör, medan rätten till dataportabilitet endast omfattar uppgifter som tillhandahålls direkt av den registrerade[60]. I händelse av en begäran om tillgång, och till skillnad från en begäran om dataportabilitet, bör den registrerade därför inte bara förses med personuppgifter som lämnats till den personuppgiftsansvarige för att göra en efterföljande analys eller bedömning av dessa uppgifter, utan även med resultatet av en sådan efterföljande analys eller bedömning.

100. Det är också viktigt att komma ihåg att det finns information, såsom anonyma uppgifter[61], som är uppgifter som inte direkt eller indirekt avser en identifierbar person och som därför inte omfattas av dataskyddsförordningen. Exempelvis är platsen för den server där personuppgifterna för den registrerade behandlas inte personuppgifter. Det kan vara svårt att göra en åtskillnad och personuppgiftsansvariga kan fråga sig hur man drar en tydlig gräns mellan personuppgifter och icke-personuppgifter, särskilt när det gäller blandade dataset. I de fallen kan det vara lämpligt att skilja mellan blandade dataset där personuppgifter och icke-personuppgifter är oupplösligt förenade och sådana där så inte är fallet. Personuppgifter och icke-personuppgifter kan vara oupplösligt förenade i blandade dataset och falla inom ramen för rätten till tillgång för den registrerade som personuppgifterna avser[62]. I andra fall är det möjligt att personuppgifter och icke-personuppgifter i blandade dataset inte är oupplösligt förenade vilket innebär att endast personuppgifterna i setet görs tillgängliga för den registrerade. Ett företag kan till exempel behöva förse en registrerad med de enskilda it-incidentrapporter som har utlösts, men inte med företagets kunskapsdatabas med it-problem. De säkerhetsåtgärder som den personuppgiftsansvarige har infört ska i allmänhet inte förstås som personuppgifter, förutsatt att dessa inte är oupplösligt förenade med personuppgifter och därför inte omfattas av rätten till tillgång.

101. EDPB vill i detta sammanhang, innan avsnittet avslutas, erinra om att skyddet för fysiska personer med avseende på behandling av personuppgifter omfattar alla typer av personuppgifter som anges ovan och att en restriktiv tolkning av definitionen strider mot bestämmelserna i dataskyddsförordningen och i slutändan mot artikel 8 i stadgan om de grundläggande rättigheterna. Tillämpning av en annan ordning för utövande av en rättighet i samband med vissa typer av personuppgifter, som inte föreskrivs

[60] Såsom tidigare angetts i artikel 29-gruppens riktlinjer om rätten till dataportabilitet – som godkänts av EDPB, s. 10 och upprepats i artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 – godkända av EDPB, s. 17.

[61] Ytterligare förklaringar om begreppet anonymisering finns i artikel 29-arbetsgruppen, yttrande 05/2014 om anonymiseringsteknik, WP216, 10 april 2014, s. 5–19.

[62] Meddelande från kommissionen till Europaparlamentet och rådet, Vägledning om förordningen om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen, 29.5.2019, COM(2019) 250 final.

i dataskyddsförordningen, kan införas uteslutande genom lag, i enlighet med artikel 23 i dataskyddsförordningen (vilket förklaras närmare i avsnitt 6.4). De personuppgiftsansvariga kan därför inte begränsa utövandet av rätten till tillgång genom att otillbörligt begränsa omfattningen av personuppgifter.

4.2 De personuppgifter som rätten till tillgång avser

102. Enligt artikel 15.1 i dataskyddsförordningen ska ”den registrerade […] ha 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 följande information” (understrykning tillagd).

103. Flera element framgår av artikel 15.1 i dataskyddsförordningen. I stycket hänvisas uttryckligen till ”personuppgifter som rör honom eller henne” (4.2.1), som ”håller på att behandlas” (4.2.2) av den personuppgiftsansvarige:

4.2.1 ”personuppgifter som rör honom eller henne”

104. Rätten till tillgång kan utövas uteslutande med avseende på personuppgifter som rör den registrerade som begär tillgång eller, i tillämpliga fall, av en behörig person eller fullmaktsinnehavare (se avsnitt 3.4). Det finns också situationer där uppgifter inte har någon koppling till den person som utövar rätten till tillgång utan till en annan person. Den registrerade har dock endast rätt till personuppgifter som rör dem själva, vilket utesluter uppgifter som endast rör någon annan[63].

105. Klassificeringen av uppgifter som personuppgifter som rör den registrerade är dock inte beroende av huruvida dessa personuppgifter också avser någon annan[64]. Det är därför möjligt att personuppgifter samtidigt avser mer än en person. Detta innebär inte automatiskt att tillgången till personuppgifter som även rör någon annan bör beviljas, eftersom den personuppgiftsansvarige måste följa artikel 15.4 i dataskyddsförordningen.

106. Orden ”personuppgifter som rör honom eller henne” bör inte tolkas alltför restriktivt av personuppgiftsansvariga, vilket artikel 29-arbetsgruppen redan har påpekat i samband med rätten till dataportabilitet[65]. När det gäller rätten till tillgång anser EDPB till exempel att inspelningar av

[63] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 9: ”Endast personuppgifter omfattas av tillämpningsområdet för en begäran om dataportabilitet. Uppgifter som är avidentifierade 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.”

[64] Domstolens dom i mål C-434/16, Peter Nowak/dataskyddskommissionären, 2017, punkt 44.

[65] Artikel 29-gruppens riktlinjer om rätten till dataportabilitet – godkända av EDPB, s. 9: 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-telefon 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 parters rättigheter och friheter på ett ogynnsamt sätt (se det tredje villkoret nedan).

telefonsamtal (och utskrifter av dessa) mellan den registrerade som begär tillgång och den personuppgiftsansvarige kan omfattas av rätten till tillgång, förutsatt att de senare är personuppgifter[66]. Förutsatt att dataskyddsförordningen tillämpas och att behandlingen inte omfattas av hushållsundantaget enligt artikel 2.2 c i samma förordning, kommer den registrerade att bli personuppgiftsansvarig för behandlingen av personuppgifter som rör den andra person vars röst spelats in, om den registrerade använder inspelningen som omfattar motpartens personuppgifter för andra ändamål, till exempel genom att offentliggöra den. Även om detta inte kommer att undanta den personuppgiftsansvarige från dennes skyldigheter i fråga om dataskydd vid en vederbörlig analys av huruvida tillgång till hela inspelningen kan ges, uppmanas den personuppgiftsansvarige att informera registrerade om att de i ett sådant fall kan bli personuppgiftsansvariga. Detta påverkar inte ytterligare bedömningar enligt artikel 15.4 i dataskyddsförordningen som beskrivs i avsnitt 6. I samma stil kan meddelanden som registrerade har skickat till andra i form av ip-meddelanden och själva tagit bort från sin enhet, och som fortfarande är tillgängliga för tjänsteleverantören, omfattas av rätten till tillgång.

107. Dessutom finns det situationer där sambandet mellan uppgifterna och flera individer kan verka oklart för den personuppgiftsansvarige, till exempel vid identitetsstöld. Vid identitetsstöld agerar en person bedrägligt i en annan persons namn. I detta sammanhang är det viktigt att komma ihåg att brottsoffret bör få information om alla personuppgifter som den personuppgiftsansvarige lagrar i samband med dennes identitet, inbegripet sådana som har samlats in på grundval av bedragarens handlingar. Med andra ord utgörs den registrerades personuppgifter av personuppgifter som förknippas med eller har samband med brottsoffrets identitet, även sedan den personuppgiftsansvarige har fått kännedom om identitetsstölden.

Exempel 17: En person använder sig av någon annans identitet för att spela poker online. Gärningsmannen betalar onlinekasinot med det kreditkort han eller hon stulit från offret. När offret får vetskap om identitetsstölden ber denne leverantören av onlinekasinot att ge tillgång till offrets personuppgifter och mer specifikt till de onlinespel som spelats och information om det kreditkort som gärningsmannen använt.

Det finns ett samband mellan de insamlade uppgifterna och brottsoffret eftersom den senares identitet har använts. När bedrägeriet har upptäckts finns det fortfarande ett samband med de personuppgifter som nämns ovan på grund av deras innehåll (offrets kreditkort handlar tydligt om brottsoffret), syfte och verkan (informationen om de onlinespel som gärningsmannen spelat kan till exempel användas för att utfärda fakturor till brottsoffret). Därför ska onlinekasinot bevilja brottsoffret tillgång till ovannämnda personuppgifter.

108. Vid behov kan interna anslutningsloggar användas för att spara poster om tillgång till en fil och spåra vilka åtgärder som utförts i samband med tillgången till en post, t.ex. utskrift, kopiering eller borttagning av personuppgifter. Dessa loggar kan omfatta tidpunkten för loggningen, orsaken till tillgången till filen samt information som identifierar den person som har haft tillgång. Frågor i detta ämne är omstridda i ett mål som väntar på avgörande i EU-domstolen (C-579/21). Införandet samt övervakningen och revideringen av anslutningsloggar faller inom den personuppgiftsansvariges ansvarsområde och kan kontrolleras av tillsynsmyndigheterna. Den personuppgiftsansvarige bör därför se till att de personer som agerar under dess överinseende och har tillgång till personuppgifter inte behandlar personuppgifter utom på den personuppgiftsansvariges instruktioner, i enlighet med

[66] Se exempel 34 i avsnitt 6.2.

artikel 29 i dataskyddsförordningen. Om personen ändå behandlar personuppgifter i andra syften än för att följa den personuppgiftsansvariges instruktioner, kan den bli personuppgiftsansvarig för denna behandling och föremål för disciplinära eller straffrättsliga förfaranden eller administrativa sanktioner som utfärdats av tillsynsmyndigheter. EDPB noterar att det är arbetsgivarens ansvar enligt artikel 24 i dataskyddsförordningen att vidta lämpliga åtgärder, allt ifrån utbildning till disciplinära förfaranden, för att säkerställa att behandlingen är förenlig med dataskyddsförordningen och att ingen överträdelse sker.

4.2.2 Personuppgifter som ”håller på att behandlas”

109. I artikel 15.1 i dataskyddsförordningen hänvisas dessutom till personuppgifter som ”håller på att behandlas”. Referenspunkten i tid för att fastställa omfattningen av de personuppgifter som omfattas av begäran om tillgång har redan utvecklats i avsnitt 2.3.3. Ordalydelsen tyder dock också på att rätten till tillgång inte skiljer mellan syftena med behandlingen.

> **Exempel 18**: Ett företag har behandlat personuppgifter som rör en registrerad för att behandla dennes inköpsorder och ordna leverans till den registrerades hemadress. När de ursprungliga ändamålen för vilka personuppgifterna samlades in inte längre existerar sparar den personuppgiftsansvarige endast vissa av personuppgifterna för att uppfylla sina rättsliga skyldigheter i fråga om registerföring.
>
> Den registrerade begär tillgång till personuppgifter som rör denne. För att fullgöra sin skyldighet enligt artikel 15.1 i dataskyddsförordningen måste den personuppgiftsansvarige tillhandahålla de begärda personuppgifter till den registrerade som lagrats i enlighet med den personuppgiftsansvariges rättsliga skyldigheter.

110. Arkiverade personuppgifter måste särskiljas från säkerhetskopierade uppgifter som är personuppgifter som lagrats enbart i syfte att återställa uppgifterna i händelse av en dataförlust. När det gäller principerna om inbyggt dataskydd och dataminimering bör det påpekas att de säkerhetskopierade uppgifterna i princip är de samma som uppgifterna i livesystemet. Om det förekommer mindre skillnader mellan personuppgifter i backupen och liveproduktionssystemet kan dessa i allmänhet förklaras med insamlingen av ytterligare uppgifter efter den senaste säkerhetskopieringen. En minskning av data i livesystemet (t.ex. radering efter lagringsperioden för vissa data eller till följd av en begäran om radering) kommer i vissa fall endast skrivas över till säkerhetskopieringsdata vid tidpunkten för efterföljande backup. Om det finns en begäran om tillgång vid en tidpunkt då det finns fler personuppgifter om den registrerade i backupen än i livesystemet eller andra personuppgifter (t.ex. som syns i loggen över borttagningar i liveproduktionssystemet som genomförts i full överensstämmelse med principen om uppgiftsminimering), måste den personuppgiftsansvarige vara öppen om denna situation och, om det är tekniskt möjligt, ge den tillgång som den registrerade begär, även till personuppgifter som lagrats i backupen. För en öppenhet gentemot registrerade som utövar sin rätt kan en loggbok över borttagningar i liveproduktionssystemet göra det möjligt för den personuppgiftsansvarige att se att det finns uppgifter i backupen som inte längre finns i livesystemet eftersom de nyligen har tagits bort och ännu inte skrivits över i backupen.

4.2.3 Tillämpningsområdet för en ny begäran om tillgång

111. Vad som återstår att säga är att registrerade har rätt att få tillgång till alla behandlade uppgifter som rör dem, eller till delar av uppgifterna, beroende på omfattningen av begäran (se även 2.3.1 om informationens fullständighet och 3.1.1 för analys av innehållet i begäran). Om en personuppgiftsansvarig redan tidigare har fullföljt en begäran om tillgång, och under förutsättning att begäran inte är orimlig, kan den personuppgiftsansvarige därför inte begränsa omfattningen av denna

nya begäran. Detta innebär att den personuppgiftsansvarige i samband med varje ytterligare begäran om tillgång från samma registrerade inte bör informera den registrerade annat än om renodlade ändringar av de personuppgifter som behandlats eller behandlingen i sig sedan den senaste begäran, såvida inte den registrerade uttryckligen samtycker till detta. I annat fall skulle de registrerade vara tvungna att sammanställa de personuppgifter de fått för att få en fullständig uppsättning av den information de har fått om behandlingen och den registrerades rättigheter.

4.3 Information om behandlingen och om registrerades rättigheter

112. Utöver tillgången till personuppgifterna i sig måste den personuppgiftsansvarige tillhandahålla information om behandlingen och om registrerades rättigheter i enlighet med artikel 15.1 a–h och 15.2 i dataskyddsförordningen. Merparten av informationen om dessa specifika punkter har redan sammanställts, åtminstone rent allmänt, i den personuppgiftsansvariges register över behandling som avses i artikel 30 i dataskyddsförordningen och/eller i dess meddelande om integritetsskydd som utarbetats i enlighet med artiklarna 12–14 i dataskyddsförordningen. Därför kan det vara till hjälp att som ett första steg konsultera artikel 29-arbetsgruppens Guidelines on transparency under Regulation 2016/679[67] om innehållet i den information som ska lämnas enligt artiklarna 13 och 14 i dataskyddsförordningen.

113. För att uppfylla kraven i artikel 15.1 a–h och 15.2 får personuppgiftsansvariga noggrant använda textmoduler från sina meddelanden om integritetsskydd så länge de ser till att de är aktuella och exakta med hänsyn till den registrerades begäran. Innan eller i början av databehandlingen kan viss information, t.ex. identifiering av specifika mottagare eller uppgiftsbehandlingens specifika varaktighet, i regel inte tillhandahållas ännu. Viss information, t.ex. om rätten att inge klagomål till en tillsynsmyndighet (se artikel 15.1 f), ändras inte beroende på den person som gör begäran om tillgång. Därför kan den kommuniceras i allmänna ordalag så som den också görs i meddelandet om integritetsskydd. Andra typer av information, t.ex. information om mottagare, kategorier och källan till uppgifterna kan variera beroende på vem som gör begäran och vad begäran gäller. I samband med en begäran om tillgång enligt artikel 15 kan all den information om behandlingen som är tillgänglig för den personuppgiftsansvarige därför behöva uppdateras och skräddarsys för den behandling som rent faktiskt utförs med avseende på den registrerade som gör begäran. Att den personuppgiftsansvarige hänvisar till ordalydelsen i sin integritetspolicy skulle därför inte vara ett tillräckligt sätt att lämna den information som krävs enligt artikel 15.1 a–h och 15.2, om inte den skräddarsydda och uppdaterade informationen är densamma som den information som lämnades i början av behandlingen. När den personuppgiftsansvarige förklarar vilken information som rör den begärande personen, kan denne i förekommande fall hänvisa till vissa aktiviteter (t.ex. ”om du har använt denna tjänst …”, ”om du har betalat med faktura”) så länge det är uppenbart för de registrerade om de berörs. Nedan förklaras graden av specifikation som krävs i förhållande till de enskilda typerna av information.

114. Information om ändamålen enligt artikel 15.1 a måste vara specifik för det eller de exakta ändamål i det faktiska fallet med den begärande registrerade. Det skulle inte räcka att ange den personuppgiftsansvariges allmänna ändamål utan att klargöra vilket eller vilka ändamål den personuppgiftsansvarige eftersträvar i det aktuella fallet med den begärande registrerade. Om behandlingen utförs för flera olika ändamål måste den personuppgiftsansvarige klargöra vilka uppgifter eller vilka kategorier av uppgifter som behandlas för vilka ändamål. Till skillnad från artikel

[67] Artikel 29-arbetsgruppen, WP260 rev.01, 11 april 2018, Guidelines on transparency under Regulation 2016/679 – godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB*).

13.1 c och artikel 14.1 c i dataskyddsförordningen innehåller informationen om den behandling som avses i artikel 15.1 a inte information om den rättsliga grunden för behandlingen. Eftersom vissa av de registrerades rättigheter är beroende av den tillämpliga rättsliga grunden är denna information viktig för att de registrerade ska kunna kontrollera att behandlingen av deras uppgifter är laglig och avgöra vilka av den registrerades rättigheter som är tillämpliga i den specifika situationen. För att underlätta utövandet av registrerades rättigheter i enlighet med artikel 12.2 i dataskyddsförordningen rekommenderas därför den personuppgiftsansvarige att även informera de registrerade om den tillämpliga rättsliga grunden för varje behandling eller ange var de kan hitta den informationen. I vilket fall som helst förutsätter principen om öppen behandling att informationen om den rättsliga grunden för behandlingen görs tillgänglig för den registrerade på ett åtkomligt sätt (t.ex. i ett meddelande om integritetsskydd).

115. Information om kategorier av uppgifter (artikel 15.1 b) kan också behöva anpassas till den registrerades situation så att kategorier som visat sig inte vara relevanta för begäranden tas bort.

> **Exempel 19**: Inom ramen för den information som avses i artiklarna 13–14 i dataskyddsförordningen anger ett hotell att de behandlar ett antal kategorier av kunduppgifter (identifieringsuppgifter, kontaktuppgifter, bankuppgifter och antal kreditkort osv.). Om en begäran om tillgång görs på grundval av artikel 15 ska den registrerade som gör begäran, utöver tillgång till de faktiska uppgifter som behandlas (komponent 2), i enlighet med artikel 15.1 b också informeras om de specifika kategorier av uppgifter som behandlas i fallet (t.ex. som inte omfattar bankuppgifter eller kreditkortsuppgifter om betalningen gjorts kontant).

116. Information om ”mottagare eller kategorier av mottagare” (artikel 15.1 c) måste först och främst beakta den definition av mottagare som ges i artikel 4.9 i dataskyddsförordningen. Definitionen av mottagare bygger på att personuppgifter lämnas ut till fysiska eller juridiska personer, offentliga myndigheter, institutioner eller andra organ[68]. Av artikel 4.9 i dataskyddsförordningen följer att offentliga myndigheter som agerar inom ramen för ett särskilt uppdrag som omfattas av särskilda nationella bestämmelser inte ska betraktas som mottagare.

117. När det gäller frågan om den personuppgiftsansvarige fritt kan välja mellan information om mottagare eller kategorier av mottagare, bör det noteras att ”till skillnad från artiklarna 13 och 14 i dataskyddsförordningen, i vilka det föreskrivs en skyldighet för den personuppgiftsansvarige […] föreskrivs det i artikel 15 i dataskyddsförordningen en faktisk rätt för den registrerade att få tillgång till uppgifter. Detta innebär att den registrerade måste kunna välja att få antingen information om de specifika mottagare till vilka uppgifterna har lämnats ut eller ska lämnas ut, om detta är möjligt, eller information om kategorierna av mottagare[69].” Det måste också erinras om att information om mottagarna eller kategorierna av mottagare, såsom anges i de ovannämnda riktlinjerna om insyn[70], redan enligt artiklarna 13 och 14 i dataskyddsförordningen bör vara så konkret som möjligt när det gäller principerna om insyn och rättvisa. Om den registrerade inte har valt något annat är den

---

[68] Det bör vidare noteras att olika personuppgiftsansvariga enligt definitionen i artikel 4.7 i dataskyddsförordningen kan finnas inom samma företag. I en sådan konstellation är det möjligt att lämna ut uppgifter från en mottagare till en annan inom samma företag.

[69] Domstolens dom i mål C-154/21 (Österreichische Post AG), punkt 36.

[70] Artikel 29-arbetsgruppen, WP260 rev.01, 11 april 2018, Guidelines on transparency under Regulation 2016/679 – godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB*), s. 37 (bilaga).

personuppgiftsansvarige enligt artikel 15 skyldig att namnge de faktiska mottagarna, såvida det inte är omöjligt att identifiera dessa mottagare eller den personuppgiftsansvarige visar att den registrerades begäran om tillgång är uppenbart ogrundad eller orimlig i den mening som avses i artikel 12.5 i dataskyddsförordningen[71] [72]. EDPB erinrar i detta avseende om att lagring av information om de faktiska mottagarna är nödvändig, bland annat för att den personuppgiftsansvarige ska kunna uppfylla sina skyldigheter enligt artiklarna 5.2 och 19 i dataskyddsförordningen.

Exempel 20: I ett meddelande om integritetsskydd informerar arbetsgivaren om vilka kategorier av uppgifter som vidarebefordras till resebyråer eller hotell i samband med affärsresor, i enlighet med artikel 13.1 e och artikel 14.1 e i dataskyddsförordningen. Om en arbetstagare begär tillgång till personuppgifterna efter affärsresor bör arbetsgivaren, när det gäller mottagarna av personuppgifterna enligt artikel 15.1 c, i sitt svar ange vilka resebyråer och hotell som mottagit uppgifterna. Arbetsgivaren hänvisade visserligen legitimt till kategorier av mottagare i sitt meddelande om integritetsskydd i enlighet med artiklarna 13 och 14, eftersom det i detta skede ännu inte var möjligt att namnge mottagarna, men bör, om inte den anställde har valt något annat, lämna information om de specifika mottagarna (namn på resebyråer, hotell osv.) när den anställde gör en begäran om tillgång.

Om de personuppgiftsansvariga, med hänsyn till ovannämnda villkor, endast kan ange mottagarkategorierna bör informationen vara så specifik som möjligt och innehålla uppgift om typen av mottagare (dvs. med hänvisning till den verksamhet som denne bedriver), bransch, sektor, undersektor och mottagarnas fysiska belägenhet[73].

118. Enligt artikel 15.1 d ska information om möjligt lämnas om den planerade period för vilken personuppgifterna kommer att lagras. I annat fall måste de kriterier som används för att fastställa denna period anges. Den information som den personuppgiftsansvarige lämnar måste vara tillräckligt exakt för att den registrerade ska veta hur länge uppgifterna om den registrerade kommer att fortsätta lagras. Om det inte är möjligt att ange den exakta tidpunkten för borttagandet ska lagringstidens längd och början på denna period eller den utlösande händelsen anges (t.ex. uppsägning av ett avtal, upphörande av en garantiperiod osv.). Enbart en hänvisning till t.ex. ”borttagning efter utgången av de föreskrivna lagringsperioderna” är inte nog. Uppgifter om lagringsperioder ska särskilt avse uppgifter som rör den registrerade. Om den registrerades personuppgifter omfattas av olika borttagningsperioder (t.ex. på grund av att alla uppgifter inte omfattas av lagstadgad lagring) ska borttagningsperioderna anges i förhållande till respektive behandling och kategorier av uppgifter.

119. Information om rätten att lämna in ett klagomål till en tillsynsmyndighet (artikel 15.1 f) beror inte på de särskilda omständigheterna, men de registrerades rättigheter som nämns i artikel 15.1 e varierar beroende på den rättsliga grund som ligger till grund för behandlingen. När det gäller den personuppgiftsansvariges skyldighet att underlätta utövandet av registrerades rättigheter enligt artikel 12.2 i dataskyddsförordningen ska den personuppgiftsansvariges respons på dessa rättigheter skräddarsys i den registrerades fall och hänföras till den berörda behandlingen. Information om rättigheter som inte är tillämpliga för den registrerade i den specifika situationen bör undvikas.

[71] Domstolens dom i mål C-154/21 (Österreichische Post AG).
[72] Enbart det faktum att uppgifterna har lämnats ut till ett stort antal mottagare skulle i sig inte göra begäran orimlig, se avsnitt 6, punkt 188.
[73] Artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB, s. 37 (bilaga)

120. Enligt artikel 15.1 g ska ”all tillgänglig information” om källan till uppgifterna lämnas, om personuppgifterna inte samlats in från den registrerade. Graden av tillgänglig information kan ändras med tiden.

Exempel 21: I integritetspolicyn för ett stort företag anges följande:

”Kreditkontroller hjälper oss att förhindra problem med betalningstransaktioner. De garanterar att vårt företag skyddas mot ekonomiska risker, vilket också kan påverka försäljningspriserna på medellång till lång sikt. En kreditkontroll måste utföras när vi ska frakta varor utan att samtidigt erhålla inköpspriset i fråga, t.ex. vid köp på konto. Utan att kreditkontrollen utförs är det endast möjligt att göra en förskottsbetalning (omedelbar banköverföring, betalleverantör online, kreditkort).

För en kreditkontroll kommer vi att skicka ditt namn, din adress och ditt födelsedatum till följande tjänsteleverantörer, bland annat: 1) Financial Information Agency X 2) Business Information Provider Y, 3) Commercial Credit Reference Agency Z.

Uppgifterna vidarebefordras till ovannämnda kreditinstitut endast inom ramen för det som är tillåtet enligt lag och enbart för en analys av ditt tidigare betalningsbeteende samt för en bedömning av risken för fallissemang på grundval av matematiska statistiska förfaranden med hjälp av adressuppgifter samt för en verifiering av din adress (leveranskontroll). Beroende på resultatet av kreditkontrollen kanske vi inte längre kan erbjuda dig individuella betalningsmetoder, som inköp av fakturor.”

Meddelandet om integritetsskydd innehåller därför allmän information om möjligheten att få information från de angivna ekonomiska informationskontoren i enlighet med artiklarna 13 och 14 i dataskyddsförordningen. Om det inte är tydligt på förhand vilka av företagen som kommer att delta i behandlingen räcker det att i integritetspolicyn nämna namnen på de alternativa företagen. I samband med en begäran som grundar sig på artikel 15 skulle det, utöver information om att en kreditupplysning har erhållits, (i efterhand) vara nödvändigt att lämna ut exakt vilka av de nämnda företagen som har varit inbegripna. Det uttrycks tydligt i artikel 15.1 g att information om behandlingen av uppgifterna består av ”all tillgänglig information om varifrån dessa uppgifter kommer”, om personuppgifterna inte samlats in från den registrerade.

121. I artikel 15.1 h föreskrivs att varje registrerad ska ha rätt att på ett ändamålsenligt sätt informeras, bland annat om förekomsten av och den underliggande logiken bakom ett automatiserat beslutsfattande, inbegripet om profilering av den registrerade, och om betydelsen och de förutsedda följderna av en sådan behandling[74]. Om möjligt måste information enligt artikel 15.1 h vara mer specifik i förhållande till det resonemang som leder till särskilda beslut som rör den registrerade som begärde tillgång.

122. Information om planerade överföringar av uppgifter till ett tredjeland eller en internationell organisation, inbegripet förekomsten av ett kommissionsbeslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder, måste lämnas enligt artiklarna 13.1 f och 14.1 f i dataskyddsförordningen. I samband med en begäran om tillgång enligt artikel 15.2 kräver artikel 15.2 information om lämpliga skyddsåtgärder enligt artikel 46 i dataskyddsförordningen endast i de fall där en överföring till ett tredjeland eller en internationell organisation faktiskt äger rum.

[74] Se för detta ändamål artikel 29-gruppens riktlinjer: Guidelines on transparency under Regulation 2016/679 (WP 260), punkt 41, med hänvisning till riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 (WP 251).

5 HUR KAN EN PERSONUPPGIFTSANSVARIG GE TILLGÅNG?

123. Dataskyddsförordningen är inte särskilt normativ i fråga om hur den personuppgiftsansvarige ska ge tillgång. Rätten till tillgång kan vara lätt och enkel att tillämpa i vissa situationer, till exempel när en mindre organisation har begränsad information om den registrerade. I andra situationer är rätten till tillgång mer komplicerad eftersom uppgiftsbehandlingen är mer komplex: när det gäller antalet registrerade, kategorier av behandlade uppgifter samt flödet av uppgifter inom och mellan olika organisationer. Med tanke på skillnaderna i behandling av personuppgifter kan det lämpliga sättet att ge tillgång variera i motsvarande grad.

124. Syftet med detta avsnitt är att ge viss vägledning och praktiska exempel på olika sätt för personuppgiftsansvariga att tillmötesgå en begäran om tillgång samt om vad som avses i artikel 12.1 i dataskyddsförordningen i fråga om rätten till tillgång. Detta avsnitt kommer också att ge viss vägledning om vad som anses vara ett elektroniskt format som är allmänt använt samt tidpunkten för att ge tillgång enligt artikel 12.3 i dataskyddsförordningen.

5.1 Hur kan den personuppgiftsansvarige hämta de begärda uppgifterna?

125. De registrerade bör få tillgång till all information som den personuppgiftsansvarige behandlar avseende dem. Detta innebär till exempel att den personuppgiftsansvarige är skyldig att söka efter personuppgifter i sina it-system och andra register än it-system. Vid en sådan sökning bör den personuppgiftsansvarige använda tillgänglig information i organisationen om den registrerade som sannolikt kommer att resultera i matchningar i systemen beroende på hur informationen är strukturerad[75]. Om informationen till exempel sorteras i filer utifrån namn eller referensnummer kan sökningen begränsas till dessa faktorer. Men om uppgifternas struktur är beroende av andra faktorer, t.ex. familjeförhållanden eller yrkestitlar eller någon form av direkta eller indirekta identifierare (t.ex. kundnummer, användarnamn eller IP-adresser), ska sökningen utvidgas till att omfatta även dessa, förutsatt att den personuppgiftsansvarige har sådan information om den registrerade, eller får denna information av den registrerade. Detsamma gäller när uppgifter om tredje man sannolikt kommer att innehålla personuppgifter om den registrerade. Den personuppgiftsansvarige får dock inte kräva att den registrerade tillhandahåller mer information än vad som är nödvändigt för att identifiera den registrerade. Om en personuppgiftsansvarig använder ett personuppgiftsbiträde för sin uppgiftsbehandling måste sökningen utvidgas till att även omfatta personuppgifter som behandlas av personuppgiftsbiträdet.

126. I linje med artikel 25 i dataskyddsförordningen om inbyggt dataskydd och dataskydd som standard bör den personuppgiftsansvarige (och alla personuppgiftsbiträden den använder) redan innan ha infört funktioner som gör det möjligt att efterleva de registrerades rättigheter. Det innebär i detta sammanhang att det bör finnas lämpliga sätt att hitta och hämta information om en registrerad vid hanteringen av en begäran. Det bör dock noteras att en orimlig tolkning i detta avseende skulle kunna leda till funktioner för att hitta och hämta information som i sig utgör en risk för de registrerades integritet. Det är därför viktigt att komma ihåg att förfarandet med att hämta uppgifter också bör utformas på ett dataskyddsvänligt sätt, så att det inte äventyrar andras integritet, till exempel den personuppgiftsansvariges anställda.

[75] En sådan sökning bör naturligtvis även omfatta information som innehas av ett personuppgiftsbiträde, se artikel 28.3 e i dataskyddsförordningen.

5.2 Lämpliga åtgärder för att ge tillgång

5.2.1 Vidta lämpliga åtgärder

127. Artikel 12 i dataskyddsförordningen fastställer kraven för att ge tillgång, dvs. på att tillhandahålla bekräftelse, personuppgifter och ytterligare information enligt artikel 15, och anger även form, sätt och tidsfrist när det gäller rätten till tillgång. Artikel 29-arbetsgruppens riktlinjer: Guidelines on transparency under Regulation 2016/679[76] ger ytterligare vägledning när det gäller artikel 12, och främst när det gäller artiklarna 13 och 14 i dataskyddsförordningen, men även när det gäller artikel 15 och om insyn i allmänhet. Det som definieras i dessa riktlinjer kan därför ofta också tillämpas när det gäller att ge tillgång enligt artikel 15.

128. I artikel 12.1 i dataskyddsförordningen anges att den personuppgiftsansvarige ska vidta lämpliga åtgärder för att tillhandahålla all kommunikation enligt artikel 15 om behandling av den registrerade i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. I artikel 12.2 föreskrivs att den personuppgiftsansvarige ska underlätta den registrerades utövande av sin rätt till tillgång. De mer exakta kraven i detta avseende får bedömas från fall till fall. När de personuppgiftsansvariga beslutar vilka åtgärder som är lämpliga måste de ta hänsyn till alla relevanta omständigheter, inbegripet, men inte begränsat till, den mängd uppgifter som behandlas, komplexiteten i deras uppgiftsbehandling och den kunskap de har om sina registrerade, till exempel om majoriteten av de registrerade är barn, äldre eller personer med funktionsnedsättning. I situationer där den personuppgiftsansvarige får kännedom om eventuella särskilda behov hos den registrerade som lämnar in begäran, till exempel genom ytterligare information i den begäran som görs, måste den personuppgiftsansvarige dessutom beakta dessa omständigheter. Till följd av detta kommer de lämpliga åtgärderna att variera.

129. Det är viktigt att vid en bedömning komma ihåg att begreppet ”lämplig” aldrig bör tolkas som ett sätt att begränsa omfattningen av de uppgifter som omfattas av rätten till tillgång. Begreppet ”lämplig” innebär inte att ansträngningen för att tillhandahålla informationen till exempel kan vägas mot den registrerades intresse av att erhålla personuppgifterna. I stället bör bedömningen syfta till att välja den lämpligaste metoden för att tillhandahålla all information som omfattas av denna rättighet, beroende på de särskilda omständigheterna i det enskilda fallet. Således måste en personuppgiftsansvarig som behandlar en större mängd data i stor skala finna sig i att ägna stora ansträngningar åt att säkerställa rätten till tillgång för de registrerade i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

130. Det måste undvikas att den registrerade hänvisas till olika källor som svar på en begäran om tillgång till uppgifter. Såsom tidigare angetts i artikel 29-gruppens riktlinjer om insyn (med avseende på begreppet ”tillhandahålla” i artiklarna 13 och 14 i dataskyddsförordningen) innebär begreppet ”tillhandahålla” att den registrerade inte aktivt ska behöva söka efter information som omfattas av dessa artiklar bland annan information, t.ex. användningsvillkoren för en webbplats eller app[77]. Därför, och i enlighet med principen om insyn, måste de registrerade av den personuppgiftsansvarige få den information och de personuppgifter som krävs enligt artikel 15.1, 15.2 och 15.3 på ett sätt som möjliggör fullständig tillgång till den begärda informationen. Under särskilda omständigheter skulle det

[76] Artikel 29-arbetsgruppen, WP260 rev.01, 11 april 2018, Guidelines on transparency under Regulation 2016/679 – godkända av EDPB (nedan kallade *artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB*).

[77] Artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB, punkt 33.

vara olämpligt eller till och med olagligt att dela den personuppgiftsansvariges information, till exempel på grund av informationens känsliga karaktär (t.ex. information om visselblåsning). I dessa fall kan det vara lämpligt att dela upp informationen i flera svar som respons på de registrerades begäran om tillgång. Den metod som den personuppgiftsansvarige väljer måste rent faktiskt förse den registrerade med de begärda uppgifterna och den begärda informationen. Därför skulle det inte vara lämpligt att enbart hänvisa den registrerade till att kontrollera de begärda uppgifterna som finns lagrade på deras egen enhet, t.ex. att de ska kontrollera klickningshistorik och IP-adresser på sin egen mobiltelefon.

131. I enlighet med principen om ansvarsskyldighet måste en personuppgiftsansvarig dokumentera sin strategi för att kunna visa hur de metoder som valts för att tillhandahålla nödvändig information enligt artikel 15 är lämpliga under de aktuella omständigheterna.

5.2.2 Olika sätt att ge tillgång

132. Som redan förklarats i avsnitt 2.2.2 ovan har de registrerade, när de gör en begäran om tillgång, rätt att få en kopia av sina uppgifter som håller på att behandlas i enlighet med artikel 15.3 tillsammans med ytterligare information, vilket anses vara den huvudsakliga metoden för att ge tillgång till personuppgifterna.

133. Under vissa omständigheter kan det dock vara lämpligt att den personuppgiftsansvarige ger tillgång på andra sätt än genom att tillhandahålla en kopia. Sådana icke varaktiga sätt att få tillgång till uppgifterna kan till exempel vara muntlig information, granskning av filer, tillgång på plats eller fjärrtillgång utan möjlighet till nedladdning. Dessa metoder kan vara lämpliga sätt att bevilja tillgång, t.ex. i fall där det ligger i den registrerades intresse eller den registrerade ber om det. Tillgång på plats kan också vara lämplig, som en inledande åtgärd, när en personuppgiftsansvarig hanterar en stor mängd icke-digitaliserade uppgifter, för att den registrerade ska få kännedom om vilka personuppgifter som håller på att behandlas och för att denne ska kunna fatta ett välgrundat beslut om vilka personuppgifter han eller hon vill få tillgång till i form av en kopia. Icke varaktiga sätt att få tillgång kan vara tillräckliga och lämpliga i vissa situationer. De kan till exempel tillgodose de registrerades behov av att kontrollera att de uppgifter som behandlas av den personuppgiftsansvarige är korrekta genom att de registrerade får möjlighet att se de ursprungliga uppgifterna. En personuppgiftsansvarig är inte skyldig att tillhandahålla informationen på andra sätt än genom en kopia men bör vidta rimliga åtgärder när denne tar ställning till en sådan begäran. Att ge tillgång på andra sätt än genom att tillhandahålla en kopia utesluter inte de registrerades rätt att även få en kopia, såvida de inte väljer att avstå.

134. Den personuppgiftsansvarige kan, beroende på den aktuella situationen, välja att tillhandahålla en kopia av de uppgifter som håller på att behandlas tillsammans med ytterligare information på olika sätt, t.ex. via e-post, fysisk post eller med hjälp av ett självbetjäningsverktyg. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt i enlighet med artikel 15.3, om inte den registrerade begär något annat. Under alla omständigheter måste den personuppgiftsansvarige överväga lämpliga tekniska och organisatoriska åtgärder, inklusive lämplig kryptering när information tillhandahålls via e-post eller självbetjäningsverktyg online.

135. I en situation där den personuppgiftsansvarige endast behandlar personuppgifter om den person som gör begäran i mindre skala kan och bör kopian av personuppgifterna och ytterligare information tillhandahållas genom ett enkelt förfarande.

Exempel 22: En lokal bokhandel för register över namn och adresser till de kunder som har beställt hemleveranser. En kund besöker bokhandeln och gör en begäran om tillgång. I denna situation skulle det vara tillräckligt att skriva ut personuppgifterna om kunden direkt från affärssystemet, samtidigt som man ger ytterligare information enligt artikel 15.1 och 15.2.

Exempel 23: En månadsgivare till en välgörenhetsorganisation gör en begäran om tillgång via e-post. Välgörenhetsorganisationen har information om de bidrag som getts under de senaste tolv månaderna samt namn och e-postadresser till givarna. Den personuppgiftsansvarige kan tillhandahålla en kopia av personuppgifterna och ytterligare information genom att svara på e-postmeddelandet, förutsatt att alla nödvändiga skyddsåtgärder tillämpas, med beaktande av exempelvis uppgifternas art.

136. Till och med personuppgiftsansvariga som behandlar en stor mängd data kan välja att förlita sig på manuella rutiner för att hantera begäranden om tillgång. Om den personuppgiftsansvarige behandlar uppgifter på flera olika avdelningar ska den personuppgiftsansvarige samla in personuppgifterna från varje avdelning för att kunna svara på den registrerades begäran.

Exempel 24: En administratör utses av den personuppgiftsansvarige till att hantera de praktiska frågorna med begäranden om tillgång. När administratören tar emot en begäran skickar den en förfrågan via e-post till organisationens olika avdelningar och ber dem att samla in personuppgifter om den registrerade. Företrädare för varje avdelning ger administratören de personuppgifter som behandlats av respektive avdelning. Administratören skickar sedan alla personuppgifter till den registrerade tillsammans med nödvändig ytterligare information, i förekommande fall till exempel via e-post.

137. Även om manuella processer för hantering av begäranden om tillgång kan anses vara lämpliga, får vissa personuppgiftsansvariga dra nytta av automatiserade processer för att hantera begäranden från registrerade. Detta kan till exempel vara fallet för personuppgiftsansvariga som tar emot ett stort antal begäranden. Ett sätt att tillhandahålla informationen enligt artikel 15 är att förse den registrerade med självbetjäningsverktyg. Dessa kan underlätta en effektiv och snabb hantering av registrerades begäranden om tillgång och gör det också möjligt för den personuppgiftsansvarige att inkludera kontrollmekanismen i självbetjäningsverktyget.

Exempel 25: En social medietjänst har en automatiserad process för hantering av begäranden om tillgång som gör det möjligt för den registrerade att få tillgång till sina personuppgifter från sitt användarkonto. För att hämta personuppgifter kan användare av tjänsten välja alternativet ”Hämta dina personuppgifter” när de är inloggade på sitt användarkonto. Med det självbetjäningsverktyget kan användarna hämta en fil som innehåller deras personuppgifter direkt från användarkontot till sin egen dator.

138. Användningen av självbetjäningsverktyg bör aldrig begränsa omfattningen av de personuppgifter som tillhandahålls. Om det inte är möjligt att lämna all information enligt artikel 15 genom självbetjäningsverktyget måste resterande information tillhandahållas på annat sätt. Den personuppgiftsansvarige kan uppmuntra den registrerade att använda ett självbetjäningsverktyg som den personuppgiftsansvarige har inrättat för att hantera begäranden om tillgång. Det bör dock noteras att den personuppgiftsansvarige också måste hantera begäranden om tillgång som inte skickas via den etablerade kommunikationskanalen[78].

[78] Se avsnitt 3.1.2.

5.2.3 Ge tillgång i en ”koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk”

139. I artikel 12.1 i dataskyddsförordningen anges att den personuppgiftsansvarige ska vidta lämpliga åtgärder för att ge tillgång enligt artikel 15, i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

140. Kravet på att den registrerade ska ges tillgång i en koncis, klar och tydlig form betyder att personuppgiftsansvariga ska presentera informationen på ett effektivt och kortfattat sätt så att den registrerade lätt kan förstå den, särskilt om det är ett barn. Den personuppgiftsansvarige måste ta hänsyn till uppgifternas kvantitet och komplexitet när denne väljer sätt att ge tillgång enligt artikel 15.

> **Exempel 26:** En leverantör av sociala medier behandlar en stor mängd information om en registrerad. En stor del av dessa personuppgifter är information som finns i loggfiler på hundratals sidor där den registrerades verksamhet på webbplatsen finns registrerad. Om registrerade begär tillgång till sina personuppgifter omfattas personuppgifterna i dessa loggfiler av rätten till tillgång. Rätten till tillgång kan därför uppfyllas formellt om dessa hundratals sidor med loggfiler ges till den registrerade. Utan åtgärder för att underlätta förståelsen av informationen i loggfilerna är det möjligt att den registrerades rätt till tillgång inte uppfylls i praktiken, eftersom det inte är enkelt att hämta kunskap från loggfilerna. Därmed uppfylls inte kravet i artikel 12.1 i dataskyddsförordningen. Den personuppgiftsansvarige måste därför vara omsorgsfull och noggrann när denne väljer hur informationen och personuppgifterna ska presenteras för den registrerade.

141. Under omständigheterna i exemplet ovan kan användningen av en skiktad strategi, liknande den skiktade strategi som förespråkas i riktlinjerna om insyn i fråga om meddelanden om integritetsskydd[79], vara en lämplig åtgärd för att uppfylla båda kraven i artiklarna 15 och 12.1 i dataskyddsförordningen. Detta kommer att vidareutvecklas i avsnitt 5.2.4 nedan. Kravet på att informationen är ”begriplig” innebär att den bör kunna förstås av den avsedda mottagaren[80], samtidigt som hänsyn tas till eventuella särskilda behov som den registrerade kan ha och som den personuppgiftsansvarige känner till[81]. Eftersom rätten till tillgång ofta gör det möjligt att utöva andra rättigheter för den registrerade är det avgörande att den information som lämnas är begriplig och tydlig. Detta beror på att registrerade endast kommer att kunna överväga om de ska åberopa sin rätt till exempelvis rättelse enligt artikel 16 i dataskyddsförordningen när de har fått veta vilka personuppgifter som behandlas, i vilka syften osv. Därför kan den personuppgiftsansvarige behöva förse den registrerade med ytterligare information som förklarar de uppgifter som lämnas. Det bör poängteras att uppgiftsbehandlingens komplexitet tvingar den personuppgiftsansvarige att tillhandahålla medel för att göra uppgifterna begripliga och inte kan användas som ett argument för att begränsa tillgången till samtliga uppgifter. På samma sätt kan den personuppgiftsansvariges skyldighet att tillhandahålla uppgifter i en koncis form inte användas som argument för att begränsa tillgången till samtliga uppgifter.

---

[79] Artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB, punkt 35.

[80] Begripligheten är nära kopplad till kravet på att använda ett klart och tydligt språk (artikel 29-gruppens riktlinjer: Guidelines on transparency - godkända av EDPB, punkt 9). Vad som sägs om ett enkelt och tydligt språk i punkterna 12–16 när det gäller den information som avses i artiklarna 13 och 14 i dataskyddsförordningen gäller även för kommunikation enligt artikel 15.

[81] Se punkt 128.

Exempel 27: En webbplats för e-handel samlar in uppgifter om artiklar som visas eller köps på webbplatsen i marknadsföringssyfte. En del av dessa uppgifter består av uppgifter i råformat[82] som inte har analyserats och kanske inte är direkt ändamålsenliga för läsaren (koder, aktivitetshistorik osv.). Sådana uppgifter om de registrerades verksamhet omfattas också av rätten till tillgång och bör därför tillhandahållas till den registrerade som svar på en begäran om tillgång. När uppgifter tillhandahålls i råformat är det viktigt att den personuppgiftsansvarige vidtar nödvändiga åtgärder för att säkerställa att den registrerade förstår uppgifterna, till exempel genom ett förklarande dokument som omvandlar råformatet till ett användarvänligt format. Ett sådant dokument kan också förklara att förkortningar och andra akronymer, till exempel A, innebär att köpet har avbrutits och B att köpet har gått igenom.

142. Elementet ”lätt tillgänglig” innebär att informationen enligt artikel 15 bör presenteras på ett sätt som är enkelt för den registrerade att få tillgång till. Detta gäller till exempel layout, lämpliga rubriker och styckesindelning. Informationen ska alltid tillhandahållas på ett klart och tydligt språk. En personuppgiftsansvarig som erbjuder en tjänst i ett land bör också erbjuda svar på det språk som de registrerade i det landet förstår. Användning av standardiserade ikoner uppmuntras också när det underlättar informationens begriplighet och tillgänglighet. När begäran om information rör registrerade som är synskadade eller andra registrerade som kan ha svårt att få tillgång till eller förstå information förväntas den personuppgiftsansvarige vidta åtgärder för att underlätta förståelsen av den information som tillhandahålls, inklusive muntlig information, när så är lämpligt[83]. Den personuppgiftsansvarige bör särskilt se till att äldre personer, barn, synskadade eller personer med kognitiva eller andra funktionsnedsättningar kan utöva sina rättigheter, till exempel genom att proaktivt tillhandahålla lättillgängliga delar som underlättar utövandet av dessa rättigheter.

5.2.4 En stor mängd information ställer särskilda krav på hur informationen tillhandahålls

143. Oavsett vilka medel som används för att ge tillgång kan det finnas en spänning mellan den mängd information som den personuppgiftsansvarige måste tillhandahålla till de registrerade och kravet på att den ska vara koncis. Ett sätt att uppnå båda, och ett exempel på en lämplig åtgärd för vissa personuppgiftsansvariga när en stor mängd uppgifter ska tillhandahållas, är att använda en skiktad strategi. Den strategin kan göra det lättare för de registrerade att förstå uppgifterna. Det bör dock betonas att denna strategi endast kan användas under vissa omständigheter och måste utövas på ett sätt som inte begränsar rätten till tillgång, såsom förklaras nedan. Dessutom bör användningen av en skiktad strategi inte utgöra en extra belastning för den registrerade. Den skulle därför vara bäst lämpad när tillgång ges i ett online-sammanhang. En skiktad strategi är endast ett sätt att presentera informationen enligt artikel 15 på ett sätt som också är förenligt med kraven i artikel 12.1 i dataskyddsförordningen och bör inte förväxlas med de personuppgiftsansvarigas möjlighet att begära att den registrerade närmare anger vilken information eller behandling som begäran avser, såsom föreskrivs i skäl 63 i dataskyddsförordningen[84].

144. En skiktad strategi när det gäller rätten till tillgång innebär att en personuppgiftsansvarig under vissa omständigheter kan tillhandahålla personuppgifterna och den ytterligare information som krävs enligt artikel 15 i olika skikt. Det första skiktet bör innehålla information om behandlingen och den

[82] Råformatet i exemplet ska förstås som oanalyserade data som ligger till grund för en behandling, och inte den lägsta nivån av rådata som endast kan vara maskinläsbara (t.ex. ”bitar”).
[83] Se artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB, punkt 21.
[84] Se även avsnitt 2.3.1.

registrerades rättigheter enligt artikel 15.1 a–h och 15.2 samt en första del av de behandlade personuppgifterna. I ett andra skikt bör fler personuppgifter tillhandahållas.

145. När den personuppgiftsansvarige fattar beslut om vilken information som bör lämnas i de olika skikten bör denne överväga vilken information som den registrerade i allmänhet anser vara mest relevant. I enlighet med rättviseprincipen bör det första skiktet också innehålla information om den behandling som har störst inverkan på den registrerade[85]. De personuppgiftsansvariga måste kunna visa ansvarsskyldighet kring sitt resonemang om ovanstående.

Exempel 28: En personuppgiftsansvarig analyserar stora datamängder för att placera kunder i olika segment utifrån deras onlinebeteende. I denna situation kan man anta att den information som är viktigast för de registrerade är information om vilket segment de har placerats i. Det innebär att den informationen bör ingå i första skiktet. Data i råformat[86] som ännu inte har analyserats eller behandlats ytterligare, såsom användaraktivitet på en webbplats, är också personuppgifter som omfattas av rätten till tillgång, men det kan i vissa fall vara tillräckligt att tillhandahålla den informationen i ett annat skikt.

146. För att en skiktad strategi ska kunna betraktas som en lämplig åtgärd är det nödvändigt att den registrerade informeras från början om att informationen enligt artikel 15 är strukturerad i olika skikt samt får en beskrivning av vilka personuppgifter och vilken information som kommer att ingå i de olika skikten. På så sätt blir det lättare för de registrerade att avgöra vilka skikt de vill få tillgång till. Beskrivningen bör objektivt återspegla alla kategorier av personuppgifter som faktiskt behandlas av den personuppgiftsansvarige. Det måste också klargöras hur den registrerade kan få tillgång till de olika skikten. Tillgången till de olika skikten ska inte kräva en oproportionell ansträngning från den registrerades sida och inte vara beroende av att en ny begäran från den registrerade formuleras. Detta innebär att de registrerade ska ha möjlighet att välja om de vill få tillgång till alla skikt samtidigt eller om de nöjer sig med att få tillgång till ett eller två av skikten.

Exempel 29: En registrerad gör en begäran om tillgång till en videostreamingtjänst. Begäran görs genom ett alternativ som är tillgängligt när den registrerade har loggat in på sitt konto. Två alternativ visas för den registrerade som knappar på webbsidan. Alternativ ett är att hämta del 1 av personuppgifterna och ytterligare information. Den innehåller till exempel senaste strömningshistorik, kontoinformation och betalinformation. Alternativ två är att hämta del 2 av de personuppgifter som innehåller tekniska loggfiler om den registrerades aktiviteter och historisk information på kontot. I detta fall har den personuppgiftsansvarige gjort det möjligt för registrerade att utöva sin rätt på ett sätt som inte ställer extra krav på den registrerade.

Variation 1: I fall där den registrerade endast väljer knappen för att hämta del 1 av personuppgifterna är den personuppgiftsansvarige bara skyldig att tillhandahålla del 1 av uppgifterna.

Variation 2: Om den registrerade väljer knapparna för både del 1 och del 2 av uppgifterna kan den personuppgiftsansvarige inte bara kommunicera del 1 av uppgifterna och sedan begära en ny bekräftelse innan del 2 av uppgifterna överförs. I stället måste båda delarna av uppgifterna lämnas till den registrerade, vilket framgår av den begäran som gjorts.

147. Användningen av en skiktad strategi kommer inte att anses lämplig för alla personuppgiftsansvariga eller i alla situationer. Den bör endast användas när det skulle vara svårt för den registrerade att förstå

[85] Se artikel 29-gruppens riktlinjer: Guidelines on transparency – godkända av EDPB, punkt 36.
[86] Se fotnot 82.

informationen om den lämnades i sin helhet. Med andra ord måste den personuppgiftsansvarige kunna visa att användningen av en skiktad strategi ger den registrerade ett mervärde och hjälper dem att förstå den information som tillhandahålls. En skiktad strategi skulle därför endast anses lämplig när en personuppgiftsansvarig behandlar en stor mängd personuppgifter om den registrerade som gör en begäran och där det skulle finnas uppenbara svårigheter för den registrerade att greppa eller förstå informationen om den tillhandahölls i sin helhet. Att det skulle krävas stora insatser och resurser från den personuppgiftsansvarige för att tillhandahålla informationen enligt artikel 15 är i sig inte ett argument för att använda en skiktad strategi.

5.2.5 Format

148. Enligt artikel 12.1 i dataskyddsförordningen ska information enligt artikel 15 tillhandahållas skriftligt eller i någon annan form, inbegripet, när så är lämpligt i elektronisk form. När det gäller tillgång till personuppgifter som är under behandling anges i artikel 15.3 att om den registrerade gör begäran i elektronisk form, och om inte den registrerade begär något annat, ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt. I dataskyddsförordningen anges inte vad ett elektroniskt format som är allmänt använt är. Det finns därför flera tänkbara format som kan användas. Det som anses vara ett elektroniskt format som är allmänt använt kommer också att variera över tid.

149. Vad som kan betraktas som ett elektroniskt format som är allmänt använt bör baseras på en objektiv bedömning och inte på vilket format den personuppgiftsansvarige använder i sin dagliga verksamhet. För att fastställa vilket format som ska betraktas som ett allmänt använt format i den aktuella situationen måste den personuppgiftsansvarige bedöma om det finns särskilda format som används allmänt inom den personuppgiftsansvariges verksamhetsområde eller i det givna sammanhanget. Om det inte finns några sådana format som används allmänt bör öppna format som anges i en internationell standard, t.ex. ISO, i allmänhet betraktas som allmänt använda elektroniska format. EDPB utesluter dock inte att andra format också kan anses vara allmänt använda i den mening som avses i artikel 15.3. Vid bedömningen av om ett format är ett allmänt använt elektroniskt format anser EDPB att det är viktigt hur enkelt den enskilde kan få tillgång till den information som tillhandahålls i det aktuella formatet. I detta avseende bör noteras vilken information som den personuppgiftsansvarige har lämnat till den registrerade om hur denne får tillgång till en fil som har tillhandahållits i ett visst format, t.ex. vilka program eller vilken programvara som kan användas för att göra formatet mer tillgängligt för den registrerade. Den registrerade bör dock inte vara tvungen att köpa en viss programvara för att få tillgång till informationen.

150. När den personuppgiftsansvarige beslutar i vilket format kopian av personuppgifterna och informationen enligt artikel 15 ska tillhandahållas måste denne komma ihåg att formatet ska göra det möjligt att framställa informationen på ett sätt som är både begripligt och lätt tillgängligt. Det är viktigt att den registrerade får information i en fast, beständig form (text, elektronisk form). Eftersom informationen bör finnas kvar över tid är skriftlig information, även på elektronisk väg, i princip att föredra framför andra former. Kopian av personuppgifterna kan, när så är lämpligt, lagras på en elektronisk lagringsenhet som en cd eller ett usb-minne.

151. Det bör noteras att det inte räcker att de registrerade har fått tillgång till sina personuppgifter för att en personuppgiftsansvarig ska kunna anse att de registrerade har fått en kopia av sina personuppgifter. För att kravet på att tillhandahålla en kopia av personuppgifter ska vara uppfyllt, och i de fall där uppgifterna tillhandahålls elektroniskt/digitalt, måste de registrerade kunna hämta sina uppgifter i ett elektroniskt format som är allmänt använt.

152. Det är den personuppgiftsansvariges ansvar att besluta i vilken form personuppgifterna ska lämnas. Den personuppgiftsansvarige kan, men är inte nödvändigtvis skyldig att, tillhandahålla de handlingar som innehåller personuppgifter om den registrerade som gör begäran, i sin ursprungliga form. Den personuppgiftsansvarige kan till exempel från fall till fall ge tillgång till en kopia av mediet som sådant, med tanke på behovet av insyn (t.ex. för att kontrollera att de uppgifter som den personuppgiftsansvarige har är korrekta vid en begäran om tillgång till en läkarjournal eller en ljudinspelning vars utskrift ifrågasätts). I sin tolkning av rätten till tillgång enligt direktiv 95/46/EG konstaterade EU-domstolen: ”För att denna [*rätt till tillgång*] ska anses vara säkerställd, är det tillräckligt att sökanden ges tillgång till en fullständig sammanställning av dessa uppgifter i begriplig form, det vill säga en form som gör det möjligt för sökanden att få kännedom om dessa uppgifter och kontrollera att de är korrekta och att de behandlas på ett sätt som är förenligt med detta direktiv, i syfte att sökanden, i förekommande fall, ska kunna utöva sina rättigheter enligt nämnda direktiv”[87]. Till skillnad från det direktivet innehåller dataskyddsförordningen uttryckligen en skyldighet att förse den registrerade med en kopia av de personuppgifter som behandlas. Detta innebär dock inte att den registrerade alltid har rätt att få en kopia av de handlingar som innehåller personuppgifterna, utan en oförändrad kopia av de personuppgifter som behandlas i dessa handlingar. [88] En sådan kopia av personuppgifterna kan tillhandahållas genom en sammanställning över alla personuppgifter som omfattas av rätten till tillgång så länge som den sammanställningen gör att den registrerade kan vara medveten om och kontrollera att behandlingen är laglig. Det finns därför ingen motsägelse mellan ordalydelsen i dataskyddsförordningen och EU-domstolens avgörande i det avseendet. Ordet ”sammanställning” i domstolens avgörande bör inte misstolkas så att sammanställningen inte ska omfatta alla uppgifter som rätten till tillgång gäller, utan är bara ett sätt att presentera alla dessa uppgifter utan att ge tillgång till de underliggande handlingar som innehåller personuppgifterna. Då sammanställningen måste innehålla en kopia av personuppgifterna bör det betonas att den inte kan göras på ett sätt som på något sätt modifierar eller ändrar innehållet i uppgifterna.

Exempel 30: En registrerad har varit försäkrad hos ett försäkringsbolag i många år. Flera försäkrade händelser har inträffat. I varje enskilt fall har en skriftlig korrespondens ägt rum via e-post mellan den registrerade och försäkringsbolaget. Eftersom den registrerade fick lämna information om de särskilda omständigheterna kring varje händelse innehåller korrespondensen en mängd personuppgifter om den registrerade (hobbyer, lägenhetskamrater, dagliga vanor osv.). I vissa av fallen uppstod oenighet om försäkringsbolagets skyldighet att kompensera den registrerade, vilket orsakade en livlig korrespondens fram och tillbaka. All denna korrespondens finns lagrad hos försäkringsbolaget. Den registrerade gör en begäran om tillgång. I den situationen behöver den personuppgiftsansvarige inte nödvändigtvis tillhandahålla e-postmeddelanden i sin ursprungliga form genom att vidarebefordra dem till den registrerade. I stället kan den personuppgiftsansvarige välja att sammanställa den e-postkorrespondens som innehåller den registrerades personuppgifter i en fil som den registrerade får.

153. Oberoende av den form i vilken den personuppgiftsansvarige lämnar personuppgifterna, t.ex. genom att tillhandahålla de faktiska handlingar som innehåller personuppgifterna eller en sammanställning av personuppgifterna, ska informationen uppfylla kraven på insyn i artikel 12 i dataskyddsförordningen. Att sammanställa och/eller extrahera uppgifterna på ett sätt som gör informationen lätt att förstå kan i vissa fall vara ett sätt att uppfylla dessa krav. I andra fall kan informationen förstås bättre genom att en kopia av det faktiska dokument som innehåller personuppgifterna tillhandahålls. Vilken form som är lämpligast måste därför avgöras från fall till fall.

[87] Domstolens dom i de förenade målen C-141/12 och C-372/12, YS m.fl., punkt 60.

[88] Frågor i detta ämne är omstridda i mål som väntar på avgörande i EU-domstolen (C-487/21 och C-307/21).

154. I detta sammanhang är det viktigt att komma ihåg att det finns en skillnad mellan rätten till tillgång enligt artikel 15 i dataskyddsförordningen och rätten att få en kopia av administrativa handlingar som regleras i nationell lagstiftning, eftersom den senare är en rätt att få en kopia av den faktiska handlingen. Detta innebär inte att rätten till tillgång enligt artikel 15 i dataskyddsförordningen utesluter möjligheten att få en kopia av de handlingar/de medier i vilka personuppgifterna förekommer.

155. I vissa fall fastställer personuppgifterna i sig kraven på det format i vilket personuppgifterna ska tillhandahållas. Om personuppgifterna till exempel utgörs av handskriven information från den registrerade kan den registrerade behöva få en fotokopia av den handskrivna informationen, eftersom handskriften i sig är personuppgifter. Detta kan särskilt vara fallet när handstilen är något som har betydelse för behandlingen, t.ex. en skriftanalys. Detsamma gäller i allmänhet för ljudinspelningar eftersom den registrerades röst är personuppgifter. I vissa fall kan dock tillgång ges genom att en utskrift av samtalet tillhandahålls, t.ex. om den registrerade och den personuppgiftsansvarige kommer överens om detta.

156. Det bör noteras att bestämmelserna om krav på format skiljer sig åt när det gäller rätten till tillgång och rätten till dataportabilitet. Rätten till dataportabilitet enligt artikel 20 i dataskyddsförordningen kräver att informationen tillhandahålls i ett maskinläsbart format, men det gör inte rätten till information enligt artikel 15. Därför kan format som anses olämpliga när de uppfyller en begäran om dataportabilitet, t.ex. pdf-filer, fortfarande vara lämpliga när de uppfyller en begäran om tillgång.

5.3 Tidpunkt för att ge tillgång

157. Enligt artikel 12.3 i dataskyddsförordningen ska den personuppgiftsansvarige utan onödigt dröjsmål, och under alla omständigheter inom en månad från mottagandet av begäran, till den registrerade tillhandahålla information om åtgärder som vidtagits med anledning av en begäran enligt artikel 15. Tidsfristen får förlängas med högst två månader beroende på hur komplicerad begäran är och antalet begäranden, förutsatt att den registrerade har informerats om skälen till denna försening inom en månad efter mottagandet av begäran. Denna skyldighet att informera den registrerade om förlängningen och skälen till den ska inte förväxlas med den information som måste lämnas utan dröjsmål och senast inom en månad när den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, i enlighet med artikel 12.4 i dataskyddsförordningen.

158. Den personuppgiftsansvarige ska utan onödigt dröjsmål ge respons och i regel tillhandahålla den information som avses i artikel 15, vilket innebär att informationen bör lämnas så snart som möjligt. Detta innebär att den personuppgiftsansvarige bör lämna den begärda informationen på kortare tid än en månad, om det är möjligt. EDPB anser också att tidpunkten för att besvara begäran i vissa situationer måste anpassas till lagringsperioden för att tillgång ska kunna ges[89].

159. Tidsfristen börjar när den personuppgiftsansvarige har mottagit en begäran enligt artikel 15, det vill säga när begäran når den personuppgiftsansvarige genom en av dess officiella kanaler[90]. Det är inte nödvändigt att den personuppgiftsansvarige faktiskt har kännedom om begäran. När den personuppgiftsansvarige behöver kommunicera med den registrerade på grund av osäkerhet kring

[89] Se avsnitt 2.3.3.

[90] I vissa medlemsstater finns det nationell lagstiftning som fastställer när ett meddelande ska anses vara mottaget, under beaktande av helger och nationella helgdagar.

identiteten hos den person som gör begäran kan det göras en vilandeförklaring tills den personuppgiftsansvarige har fått den nödvändiga informationen från den registrerade, förutsatt att den personuppgiftsansvarige har begärt ytterligare information utan onödigt dröjsmål. Detsamma gäller när en personuppgiftsansvarig har begärt att en registrerad ska ange närmare vilken behandling som begäran avser, när villkoren i skäl 63 är uppfyllda[91].

Exempel 31: Efter mottagandet av en begäran reagerar en personuppgiftsansvarig omedelbart och begär den information som denne behöver för att bekräfta identiteten hos den person som gör begäran. Den senare svarar inte förrän flera dagar senare och den information som den registrerade skickar för att verifiera sin identitet tycks inte vara tillräcklig, vilket gör att den personuppgiftsansvarige får begära förtydliganden. I denna situation kommer det att göras en vilandeförklaring tills dess att den personuppgiftsansvarige har fått tillräckligt med information för att kunna kontrollera den registrerades identitet.

160. Tidsfristen för att besvara en begäran om tillgång måste beräknas i enlighet med förordning nr 1182/71[92].

Exempel 32: En organisation tar emot en begäran den 5 mars. Tidsfristen börjar löpa samma dag. Detta ger organisationen fram till senast den 5 april att tillmötesgå begäran.

Exempel 33: Om organisationen mottar en begäran den 31 augusti finns det inget motsvarande datum följande månad eftersom den är kortare, och då är det senaste svarsdatumet sista dagen i följande månad, dvs. den 30 september.

161. Om den sista dagen i denna tidsperiod infaller på en helg eller en helgdag har den personuppgiftsansvarige på sig till nästa arbetsdag att svara.

162. Under vissa omständigheter kan den personuppgiftsansvarige förlänga tiden för att svara på en begäran om tillgång med ytterligare två månader om så krävs, med beaktande av komplexiteten och antalet begäranden. Det bör poängteras att denna möjlighet är ett undantag från den allmänna regeln som inte bör överutnyttjas. Om personuppgiftsansvariga ofta blir tvungna att förlänga tidsfristen kan det vara en indikation på ett behov av att de vidareutvecklar sina allmänna förfaranden för att hantera begäranden.

163. Vad som utgör en komplicerad begäran varierar beroende på de särskilda omständigheterna i varje enskilt fall. Några av de faktorer som kan anses vara relevanta är till exempel följande:

- Mängden uppgifter som behandlas av den personuppgiftsansvarige.
- Hur informationen är lagrad, särskilt när det är svårt att hämta informationen, t.ex. när uppgifter behandlas av olika enheter inom en organisation.
- Behovet av att redigera information när ett undantag gäller, till exempel information som rör andra registrerade eller som utgör affärshemligheter.
- När informationen kräver ytterligare arbete för att bli begriplig.

[91] Se även avsnitt 2.3.1.

[92] Rådets förordning (EEG, Euratom) nr 1182/71 av den 3 juni 1971 om regler för bestämning av perioder, datum och frister.

164. Enbart det faktum att det skulle kräva stora ansträngningar att tillmötesgå en begäran gör inte begäran komplicerad. På samma sätt skulle det faktum att ett stort företag tar emot ett stort antal begäranden inte automatiskt leda till en förlängning av tidsfristen. När en personuppgiftsansvarig tillfälligt tar emot en stor mängd begäranden, till exempel på grund av en osedvanlig publicitet kring sin verksamhet, kan detta dock betraktas som ett legitimt skäl till att förlänga svarstiden. En personuppgiftsansvarig, särskilt en som hanterar en stor mängd uppgifter, bör dock ha infört mekanismer och förfaranden för att kunna hantera begäranden inom tidsfristen under normala omständigheter.

6 BEGRÄNSNINGAR OCH RESTRIKTIONER AV RÄTTEN TILL TILLGÅNG

6.1 Allmänna anmärkningar

165. Rätten till tillgång omfattas av de begränsningar som följer av artikel 15.4 i dataskyddsförordningen (andras rättigheter och friheter) och artikel 12.5 i dataskyddsförordningen (uppenbart ogrundade eller orimliga begäranden). Dessutom kan unionsrätten eller medlemsstaternas nationella rätt begränsa rätten till tillgång i enlighet med artikel 23 i dataskyddsförordningen. Undantag avseende behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål kan baseras på artikel 89.2 och 89.3 i dataskyddsförordningen och undantag för behandling som utförs för journalistiska ändamål eller akademiskt, konstnärligt eller litterärt skapande kan baseras på artikel 85.2 i dataskyddsförordningen.

166. Det är viktigt att notera att dataskyddsförordningen, utöver ovannämnda gränser, undantag och eventuella begränsningar, inte tillåter ytterligare undantag eller avvikelser från rätten till tillgång. Detta innebär bland annat att rätten till tillgång inte är någon allmän reservation mot proportionalitet i fråga om de insatser som den personuppgiftsansvarige måste göra för att tillmötesgå de registrerades begäran enligt artikel 15 i dataskyddsförordningen[93]. Dessutom är det inte tillåtet att begränsa eller inskränka rätten till tillgång i ett avtal mellan den personuppgiftsansvarige och den registrerade.

167. Enligt skäl 63 beviljas de registrerade rätten till tillgång för att de ska vara medvetna om och kontrollera att behandlingen är laglig. Rätten till tillgång gör det bland annat möjligt för den registrerade att, beroende på omständigheterna, erhålla rättelse, radering eller blockering av personuppgifter[94]. De registrerade är dock inte skyldiga att ange skäl till eller motivera sin begäran. Så länge kraven i artikel 15 i dataskyddsförordningen är uppfyllda bör syftet med begäran betraktas som irrelevant[95].

6.2 Artikel 15.4 i dataskyddsförordningen

168. Enligt artikel 15.4 i dataskyddsförordningen ska rätten att erhålla en kopia inte inverka menligt på andras rättigheter och friheter. Förklaringar om denna begränsning ges i den femte och sjätte meningen i skäl 63. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran.

---

[93] Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, så som framgår av skäl 63 i dataskyddsförordningen, får den personuppgiftsansvarige begära att den registrerade närmare anger vilken information eller behandling begäran avser. Se även avsnitt 2.3.1.

[94] Domstolens dom i förenade målen C-141/12 och C-372/12, YS m.fl.

[95] Detta påverkar inte tillämplig nationell lagstiftning som uppfyller kraven i artikel 23 i dataskyddsförordningen, se kapitel 6.4.

Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Vid tolkningen av artikel 15.4 i dataskyddsförordningen bör man vara särskilt försiktig så att man inte på ett oacceptabelt sätt vidgar de begränsningar som fastställs i artikel 23 i dataskyddsförordningen, vilka endast är tillåtna på strikta villkor.

169. Artikel 15.4 i dataskyddsförordningen är tillämplig på rätten att erhålla en kopia av uppgifterna, vilket är den huvudsakliga metoden för att ge tillgång till de behandlade uppgifterna (andra komponenten i rätten till tillgång). Det är också tillämpligt om tillgången till personuppgifter undantagsvis beviljas på annat sätt än genom en kopia, och andras rättigheter och friheter ska också beaktas. Det finns till exempel ingen godtagbar anledning till att affärshemligheter skulle påverkas genom att en kopia tillhandahålls eller genom att den registrerade får tillgång till uppgifterna på plats. Artikel 15.4 i dataskyddsförordningen är inte tillämplig på den ytterligare information om behandlingen som anges i artikel 15.1 a–h i dataskyddsförordningen.

170. Enligt skäl 63 inbegriper motstridiga rättigheter och friheter affärshemligheter och immateriella rättigheter och särskilt upphovsrätten som skyddar programvaran. Dessa rättigheter och friheter som uttryckligen nämns, bör endast betraktas som exempel, eftersom varje rättighet eller frihet som grundar sig på unionsrätten eller medlemsstaternas nationella rätt i princip kan anses åberopa begränsningen i artikel 15.4 i dataskyddsförordningen[96]. Rätten till skydd av personuppgifter (artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna) kan därför också betraktas som en rättighet som berörs i enlighet med artikel 15.4 i dataskyddsförordningen. När det gäller rätten att få en kopia är rätten till dataskydd för andra ett typiskt fall där begränsningen måste bedömas. Dessutom måste rätten till konfidentiell korrespondens beaktas, till exempel när det gäller privat e-postkorrespondens i anställningssammanhang[97]. Det är viktigt att notera att inte alla intressen är lika med ”rättigheter och friheter” i enlighet med artikel 15.4 i dataskyddsförordningen. Ett företags ekonomiska intresse av att inte lämna ut personuppgifter når t.ex. inte upp till tröskelvärdet för att utnyttja undantaget i artikel 15.4 så länge det inte rör sig om affärshemligheter, immateriella rättigheter eller andra skyddade rättigheter som påverkas.

171. Med ”andra” avses varje annan person eller enhet än den registrerade som utövar sin rätt till tillgång. Den personuppgiftsansvariges eller personuppgiftsbiträdets rättigheter och friheter (t.ex. när det gäller att hålla affärshemligheter och immateriella rättigheter konfidentiella) kan därför övervägas. Om EU:s lagstiftare hade velat utesluta personuppgiftsansvariga eller personuppgiftsbiträdenas rättigheter och friheter skulle de ha använt begreppet ”tredje part”, som definieras i artikel 4.10 i dataskyddsförordningen.

172. Den allmänna oron över att andras rättigheter och friheter kan påverkas av att begäran om tillgång tillmötesgås räcker inte för att stödja sig på artikel 15.4 i dataskyddsförordningen. Den personuppgiftsansvarige måste kunna visa att andras rättigheter eller friheter faktiskt skulle påverkas i den konkreta situationen.

Exempel 34: En person som nu är vuxen togs om hand inom ramen för socialtjänsten under ett antal år tidigare. Akterna i ärendet kan eventuellt innehålla känslig information om andra personer (föräldrar, socialarbetare, andra minderåriga). En begäran om information från den registrerade kan dock i allmänhet inte avslås av detta skäl med hänvisning till artikel 15.4 i dataskyddsförordningen.

[96] Vikten eller prioriteringen av motstridiga rättigheter och friheter är inte en fråga om definitionen av begreppen ”rättigheter och friheter”. En avvägning av sådana intressen är dock en del av ett andra steg i bedömningen, oavsett om artikel 15.4 är tillämplig eller ej. Se punkt 173 nedan.

[97] Europadomstolens dom i målet Barbulescu/Rumänien, nr 61496/08, punkt 80, 5 september 2017.

Snarare måste andras rättigheter och friheter undersökas i detalj och påvisas av socialtjänsten i egenskap av personuppgiftsansvarig. Beroende av intressena i fråga och deras relativa betydelse kan tillhandahållandet av sådana specifika uppgifter avvisas (t.ex. genom att namnen ändras).

173. När det gäller skäl 4 i dataskyddsförordningen och den logiska grunden till artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna är rätten till skydd av personuppgifter inte en absolut rättighet[98]. Därför måste utövandet av rätten till tillgång också vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. När bedömningen enligt artikel 15.4 i dataskyddsförordningen visar att det skulle ha ogynnsamma (negativa) effekter på andra delaktigas rättigheter och friheter (steg 1) att tillmötesgå begäran måste alla delaktigas intressen vägas mot bakgrund av de särskilda omständigheterna i fallet, särskilt sannolikheten för och allvaret i de risker som finns med överföringen av uppgifterna. Den personuppgiftsansvarige bör försöka sammanjämka de motstridiga rättigheterna (steg 2), till exempel genom att vidta lämpliga åtgärder för att minska risken för andras rättigheter och friheter. Såsom betonas i skäl 63 bör skyddet av andras rättigheter och friheter i kraft av artikel 15.4 i dataskyddsförordningen inte leda till att den registrerade vägras all information. Detta innebär till exempel, när begränsningen gäller, att information om andra måste göras oläslig i så stor utsträckning som möjligt i stället för att man vägrar tillhandahålla en kopia av personuppgifterna. Om det emellertid är omöjligt att hitta en lösning för att sammanjämka de relevanta rättigheterna måste den personuppgiftsansvarige i nästa steg besluta vilka av de motstridiga rättigheterna och friheterna som ska gälla (steg 3).

Exempel 35: En återförsäljare erbjuder sina kunder möjligheten att beställa produkter via en direktlinje som sköts av dess kundtjänst. För att kunna bevisa affärstransaktionen lagrar återförsäljaren en inspelning av samtalet, i enlighet med de strikta kraven i tillämplig lagstiftning. En kund vill ha en kopia av det samtal han hade med en kundtjänstmedarbetare. I ett första steg analyserar återförsäljaren begäran och inser att inspelningen innehåller personuppgifter som också rör någon annan, nämligen kundtjänstmedarbetaren. För att bedöma om tillhandahållandet av kopian skulle påverka andras rättigheter och friheter måste återförsäljaren i ett andra steg balansera de motstridiga intressena, och särskilt beakta sannolikheten för och allvaret i de eventuella risker för kundtjänstmedarbetarens rättigheter och friheter som är förenade med att inspelningen kommuniceras till kunden. Återförsäljaren drar slutsatsen att det finns mycket begränsade personuppgifter som rör kundtjänstmedarbetaren i inspelningen, nämligen bara hans röst. Återförsäljaren/personuppgiftsansvarige kommer fram till att medarbetaren inte är lätt att identifiera. Dessutom är diskussionens innehåll av yrkesmässig karaktär och den registrerade var samtalspartnern. På grundval av ovannämnda omständigheter drar den personuppgiftsansvarige den objektiva slutsatsen att rätten till tillgång inte ogynnsamt påverkar rättigheterna och friheterna för kundtjänstmedarbetaren, så den personuppgiftsansvarige kan förse den registrerade med hela röstinspelningen, inklusive de delar som härrör sig från kundtjänstmedarbetaren.

Exempel 36: En kund på ett apotek vill ha tillgång till mätresultaten för sina ben på grundval av artikel 15 i dataskyddsförordningen. Apoteket hade mätt den registrerades ben för att tillverka individuellt anpassade medicinska kompressionsstrumpor. Apoteket hade tydligen mycket erfarenhet och hade infört en speciell teknik för korrekt mätning. Efter mätningen på apoteket vill kunden använda mätresultaten för att köpa billigare strumpor någon annanstans (beställa dem i en onlinebutik). Apoteket vägrar delvis tillgång till uppgifterna på grundval av artikel 15.4 i

[98] Se t.ex. även domstolens dom i de förenade målen C-92/09 och C-93/09, Volker und Markus Schecke GbR och Hartmut Eifert/Land Hessen (GC), 9 november 2010, punkt 48.

dataskyddsförordningen och hävdar att resultaten till följd av deras särskilda, korrekta mättekniker skyddas som affärshemligheter. Om och i den mån den personuppgiftsansvarige kan bevisa att

- det inte är möjligt att ge den registrerade information om mätresultaten utan att avslöja hur mätningarna gjordes samt
- information om hur mätningarna gjordes, inklusive i förekommande fall den exakta bestämningen av mätpunkterna, och att det är affärshemligheter

får de tillämpa artikel 15.4 i dataskyddsförordningen.

Den personuppgiftsansvarige skulle fortfarande behöva lämna så mycket information som möjligt om de mätresultat som inte skulle avslöja affärshemligheter, även om det skulle kräva ansträngningar att revidera och redigera resultaten.

Exempel 37: SPELARE X är registrerad användare på spelplattformen i PLATTFORM Y. En dag underrättas SPELARE X om att hans onlinekonto har begränsats. Eftersom han inte längre kan logga in ber SPELARE X den personuppgiftsansvarige om tillgång till alla personuppgifter som rör honom. Dessutom kräver SPELARE X tillgång till skälen för kontobegränsningen. PLATTFORM Y, den personuppgiftsansvarige för onlinespelplattformen till vilken begäran har lämnats in, informerar användarna i sina allmänna villkor på webbplatsen om att varje form av fusk (främst genom användning av programvara från tredje part) kommer att medföra en tillfällig eller varaktig avstängning från plattformen. PLATTFORM Y informerar också användarna i sin integritetspolicy om behandlingen av personuppgifter i syfte att upptäcka spelfusk, i enlighet med kraven i artikel 13 i dataskyddsförordningen.

Efter mottagandet av SPELARE X:s begäran om tillgång ska PLATTFORM Y förse SPELARE X med en kopia av de personuppgifter som behandlats om SPELARE X. När det gäller skälet till kontobegränsningen bör PLATTFORM Y bekräfta till SPELARE X att den beslutat att begränsa SPELARE X:s åtkomst till onlinespel på grund av spelfusk vid ett eller flera tillfällen vilket strider mot de allmänna användarvillkoren. Utöver den information som lämnas om behandlingen för att upptäcka spelfusk bör PLATTFORM Y ge SPELARE X tillgång till den information den har lagrat om SPELARE X:s spelfusk och som lett till begränsningen. I synnerhet ska PLATTFORM Y förse SPELARE X med den information som lett till begränsningen av kontot (t.ex. loggöversikt, datum och tid för fusk, upptäckt av programvara från tredje part osv.) så att den registrerade (dvs. SPELARE X) kan kontrollera att databehandlingen har varit korrekt.

Enligt artikel 15.4 i dataskyddsförordningen och skäl 63 i dataskyddsförordningen är PLATTFORM Y inte skyldig att avslöja någon del av den tekniska funktionen av programvaran mot fusk, även om denna information rör SPELARE X, så länge som denna kan betraktas som affärshemligheter. Den nödvändiga balanseringen av intressen enligt artikel 15.4 i dataskyddsförordningen kommer att utesluta att dessa personuppgifter utlämnas, till följd av affärshemligheterna i PLATTFORM Y, eftersom kunskap om den tekniska funktionen hos programvaran mot fusk också skulle kunna göra det möjligt för användaren att undgå framtida upptäckt av fusk eller bedrägerier[99].

[99] Omfattningen av den information som lämnas till enskilda personer kommer att vara starkt beroende av sammanhanget, med beaktande av den personuppgiftsansvariges art och typen av överträdelse av tjänstevillkoren. I vissa fall kan det endast vara möjligt för den personuppgiftsansvarige att lämna grundläggande information som svar på en begäran om tillgång som omfattas av artikel 15.4.

174. Om den personuppgiftsansvarige vägrar att tillmötesgå en begäran om rätt till tillgång, helt eller delvis, enligt artikel 15.4 i dataskyddsförordningen, måste denne informera den registrerade om skälen utan dröjsmål och senast inom en månad (artikel 12.4 i dataskyddsförordningen). Motiveringen måste hänvisa till de konkreta omständigheterna för att den registrerade ska kunna bedöma om denne vill vidta åtgärder mot vägran. Den ska innehålla information om möjligheten att lämna in ett klagomål till en tillsynsmyndighet (artikel 77 i dataskyddsförordningen) och att begära rättslig prövning (artikel 79 i dataskyddsförordningen).

6.3 Artikel 12.5 i dataskyddsförordningen

175. Artikel 12.5 i dataskyddsförordningen gör det möjligt för personuppgiftsansvariga att vägra tillmötesgå begäranden om rätt till tillgång som är uppenbart ogrundade eller orimliga. Dessa begrepp måste tolkas snävt, eftersom principerna om insyn och kostnadsfria rättigheter för den registrerade inte får undergrävas.

176. De registeransvariga måste kunna visa för den enskilde varför de anser att begäran är uppenbart ogrundad eller orimlig och, vid förfrågan, förklara skälen för den behöriga tillsynsmyndigheten. Begäranden bör bedömas från fall till fall i det sammanhang där de görs för att avgöra om de är uppenbart ogrundade eller orimliga.

6.3.1 Vad betyder uppenbart ogrundat?

177. En begäran om rätt till tillgång är uppenbart ogrundad när det klart och tydligt framgår att kraven i artikel 15 i dataskyddsförordningen inte uppfylls vid tillämpning av ett objektivt tillvägagångssätt. Såsom förklaras särskilt i avsnitt 3 ovan finns det endast ett fåtal förutsättningar för begäranden om rätt till tillgång. Därför poängterar EDPB att det endast finns ett mycket begränsat utrymme för att stödja sig på det ”uppenbart ogrundade” alternativet i artikel 12.5 i dataskyddsförordningen när det gäller begäranden om rätt till tillgång.

178. Dessutom är det viktigt att komma ihåg att de personuppgiftsansvariga, innan de åberopar begränsningen, noggrant måste analysera begärans innehåll och omfattning. En begäran bör till exempel inte anses vara uppenbart ogrundad om den rör behandling av personuppgifter som inte omfattas av dataskyddsförordningen (i detta fall bör begäran inte behandlas som en artikel 15-begäran över huvud taget).

179. Andra fall där tillämpligheten av artikel 12.5 i dataskyddsförordningen kan ifrågasättas är begäranden som rör information eller behandling som klart och tydligt inte omfattas av den personuppgiftsansvariges behandling.

Exempel 38: En registrerad riktar en begäran till en kommunal myndighet om uppgifter som behandlas av en statlig myndighet. I stället för att hävda att denna begäran är uppenbart ogrundad skulle det vara lämpligare och enklare att den myndighet som begäran riktades till konstaterade att dessa uppgifter inte behandlas av myndigheten i fråga (första beståndsdelen av artikel 15 i dataskyddsförordningen: ”huruvida” personuppgifter behandlas)[100].

[100] En annan fråga är huruvida den myndighet som begäran om tillgång riktades till har rätt att översända begäran till den behöriga statliga myndigheten.

180. En personuppgiftsansvarig bör inte förutsätta att en begäran är uppenbart ogrundad för att den registrerade tidigare har lämnat in begäranden som har varit uppenbart ogrundade eller orimliga eller om den innehåller ett osakligt eller oanständigt språk.

6.3.2 Vad betyder orimlig?

181. Det finns ingen definition av begreppet ”orimlig” i dataskyddsförordningen. Å ena sidan gör ordalydelsen ”särskilt på grund av deras repetitiva art” i artikel 12.5 i dataskyddsförordningen det möjligt att dra slutsatsen att huvudscenariot för tillämpningen av detta led med avseende på artikel 15 i dataskyddsförordningen är kopplat till mängden begäranden från en registrerad om rätten till tillgång. Å andra sidan visar ovannämnda formulering att andra skäl som kan ge upphov till orimligheter inte utesluts på förhand.

182. När det gäller rätten att erhålla en kopia enligt artikel 15.3 i dataskyddsförordningen kan den registrerade förvisso lämna in mer än en begäran till en personuppgiftsansvarig[101]. Vid begäranden som potentiellt kan anses orimliga beror bedömningen av ”orimligheten” på den personuppgiftsansvariges analys och de närmare detaljerna i den sektor där denne är verksam.

183. Vid efterföljande begäranden ska bedömas om tröskelvärdet för rimliga intervall (se skäl 63) har överskridits eller inte. De registeransvariga måste noggrant beakta de särskilda omständigheterna i varje enskilt fall.

184. När det till exempel gäller sociala nätverk förväntas en ändring av datamängden ske med kortare intervall än när det gäller fastighetsregister eller centrala bolagsregister. När det gäller affärspartners bör kontaktfrekvensen med kunden beaktas. Därför varierar också de ”rimliga intervall” inom vilka registrerade kan utöva sin rätt till tillgång igen. Ju oftare ändringar görs i den personuppgiftsansvariges databas, desto oftare kan registrerade tillåtas begära tillgång till sina personuppgifter utan att det är orimligt. Å andra sidan kan en andra begäran från samma registrerade under vissa omständigheter anses vara repetitiv.

185. För att kunna avgöra om ett rimligt intervall har förflutit bör personuppgiftsansvariga beakta följande, mot bakgrund av den registrerades rimliga förväntningar:

- Hur ofta ändras uppgifterna – är det osannolikt att informationen har ändrats mellan begärandena? Om en datapool uppenbarligen inte är föremål för någon annan behandling än lagring och den registrerade är medveten om detta, t.ex. till följd av en tidigare begäran om rätt till tillgång, kan det vara en indikation på en orimlig begäran.
- Uppgifternas art – detta kan inbegripa huruvida de är särskilt känsliga.
- Syftet med behandlingen – detta kan inbegripa huruvida behandlingen sannolikt kommer att åsamka den sökande lidande (skada) om den röjs.
- Huruvida de efterföljande begärandena avser samma eller olika typ av information eller behandling[102].

[101] Enligt artikel 15.3 andra meningen får den personuppgiftsansvarige ta ut en rimlig avgift för ytterligare begärda kopior.

[102] Om den efterföljande begäran avser samma typ av information i fråga om omfattning OCH tid är detta inte en fråga om orimlighet utan en fråga om begäran om ytterligare en kopia, se avsnitt 2.2.2.2.

Exempel 39 (snickare): En registrerad lämnar in en begäran om tillgång **varannan månad** till snickaren som har tillverkat ett bord åt denne. Snickaren besvarar den första begäran i sin helhet. När man avgör om ett rimligt intervall har förflutit bör man beakta att snickaren endast ibland (första punktsatsen ovan) och inte som en del av sin kärnverksamhet samlar in och behandlar personuppgifter. Det är ännu mindre sannolikt att snickaren ofta tillhandahåller tjänster till samma registrerade. I det här fallet hade snickaren inte tillhandahållit mer än en tjänst till den registrerade, vilket gjorde det osannolikt att förändringar inträffat i datasetet för den registrerade. Med tanke på de behandlade personuppgifternas art och omfattning kan riskerna i samband med behandlingen anses vara låga (andra punktsatsen ovan), och syftet med behandlingen (faktureringsändamål och efterlevnad av skyldigheten att föra register) är sannolikt inte till skada för den registrerade (tredje punktsatsen ovan). Begäran gäller dessutom samma information som den senaste begäran (fjärde punktsatsen ovan). Sådana begäranden kan därför anses vara orimliga eftersom de är repetitiva.

Exempel 40 (plattform för sociala medier): En plattform för sociala medier vars kärnverksamhet är insamling och/eller behandling av de registrerades personuppgifter utövar en storskalig komplex och kontinuerlig behandling. En registrerad som använder plattformens tjänster lämnar in en begäran om tillgång **var tredje månad**. I detta fall är det högst sannolikt att personuppgifterna som rör den registrerade ändras ofta (första punktsatsen ovan), och det breda spektrumet av insamlade uppgifter omfattar härledda känsliga personuppgifter (andra punktsatsen ovan) som behandlas i syfte att visa relevant innehåll och nätverksmedlemmar för den registrerade (tredje punktsatsen). En begäran om tillgång var tredje månad kan – under dessa omständigheter – i princip inte betraktas som orimlig på grund av sin repetitiva art.

Exempel 41 (kreditinstitut): Det kan liksom i fråga om sociala nätverk inte uteslutas att ändringar av relevanta uppgifter som innehas av kreditinstitut kommer att ske med mycket kortare intervall än inom andra områden (första punktsatsen ovan). Detta beror på flera faktorer som den registrerade, som utomstående, vanligtvis inte känner till på grund av affärsmodellens komplexitet. Svaret på frågan om vilken typ av uppgifter som samlats in av den personuppgiftsansvarige för en beräkning av poängvärdet och vilka uppgifter som för närvarande ingår i beräkningen kan därför endast ges av kreditinstitutet självt. Dessutom kan databehandling genom kreditinstitut och det resulterande poängvärdet få långtgående konsekvenser för den registrerade när det gäller planerade rättsliga transaktioner, såsom ingående av köpe-, hyres- eller leasingavtal (tredje punktsatsen ovan).

Det är inte möjligt att generellt fastställa ett visst intervall inom vilket inlämningen av ytterligare en begäran om tillgång skulle kunna anses vara orimlig enligt artikel 12.5 andra meningen i dataskyddsförordningen. Snarare är en övergripande bedömning av omständigheterna i det enskilda fallet nödvändig. Med tanke på hur viktig uppgiftsbehandlingen är för den registrerades realitet i vardagen kan det dock förmodas att ett **ettårsintervall** mellan de gånger som information tillhandahålls kostnadsfritt under alla omständigheter är för stort för att begäran ska anses vara orimlig. Om en begäran lämnas in inom ett mycket kort tidsintervall bör den avgörande faktorn vara huruvida den registrerade har skäl att anta att informationen eller behandlingen har ändrats sedan den senaste begäran. Om den registrerade till exempel har genomfört en finansiell transaktion, som att ta ett lån, bör den registrerade ha rätt att begära tillgång till kreditinformationen även om en sådan begäran lämnades in och besvarades strax före.

186. När det är möjligt att enkelt tillhandahålla informationen på elektronisk väg eller genom fjärråtkomst till ett säkert system, vilket innebär att tillmötesgåendet av begärandena inte belastar den personuppgiftsansvarige, är det osannolikt att efterföljande begäranden kan betraktas som orimliga.

187. Om en begäran överlappar en tidigare begäran kan den överlappande begäran i allmänhet anses vara orimlig om och i den utsträckning den omfattar exakt samma information eller behandling som den föregående begäran och denna ännu inte har fullföljts av den personuppgiftsansvarige utan att ha fått statusen ”onödigt dröjsmål” (se artikel 12.3 i dataskyddsförordningen). I praktiken skulle båda begärandena till följd av detta kunna kombineras.

188. Det faktum att det skulle kräva mycket tid och ansträngningar av den personuppgiftsansvarige att tillhandahålla informationen eller kopian till den registrerade kan inte i sig göra en begäran orimlig[103]. Ett stort antal behandlingsaktiviteter kräver i regel större ansträngningar när det gäller att tillmötesgå begäranden om tillgång. Såsom anges ovan kan dock begäranden under vissa omständigheter betraktas som orimliga av andra skäl än sin repetitiva karaktär. Enligt EDPB omfattar detta särskilt fall av missbruk av rätten att stödja sig på artikel 15 i dataskyddsförordningen, vilket innebär fall där registrerade utnyttjar rätten till tillgång i orimlig utsträckning enbart i syfte att orsaka skada eller men för den personuppgiftsansvarige.

189. Mot bakgrund av detta bör en begäran inte anses vara orimlig av följande skäl:

- Den registrerade lämnar inga skäl för begäran eller den personuppgiftsansvarige anser att begäran är meningslös.
- Den registrerade använder ett olämpligt eller oförskämt språk.
- Den registrerade har för avsikt att använda uppgifterna för att ställa ytterligare anspråk till den personuppgiftsansvarige[104].

190. Å andra sidan kan en begäran anses vara orimlig, t.ex. om

- en enskild person gör en begäran, men samtidigt erbjuder sig att dra tillbaka den i utbyte mot någon form av förmåner från den personuppgiftsansvarige eller
- begäran är uppsåtlig och används för att trakassera den personuppgiftsansvarige eller dess anställda i det enda syftet att orsaka störningar, till exempel utifrån det faktum att
    - personen i fråga i sin begäran eller i andra meddelanden uttryckligen har angett att den avser att orsaka störningar och ingenting annat eller
    - den enskilde systematiskt skickar olika begäranden till en personuppgiftsansvarig som en del av en kampanj, t.ex. en gång i veckan, med avsikten och effekten att orsaka störningar[105].

[103] Inget proportionalitetstest, se punkt 166.
[104] Detta påverkar inte tillämplig nationell lagstiftning som uppfyller kraven i artikel 23 i dataskyddsförordningen, se kapitel 6.4.
[105] Att systematiskt skicka som en del av en kampanj innebär att begäranden som lätt skulle kunna kombineras i en och samma begäran på ett onaturligt sätt delas upp, inte bara i ett fåtal utan i många olika delar av den registrerade med den uppenbara avsikten att orsaka störningar.

6.3.3 Konsekvenser

191. Vid en uppenbart ogrundad eller orimlig begäran om rätt till tillgång får personuppgiftsansvarig enligt artikel 12.5 i dataskyddsförordningen antingen ta ut en rimlig avgift (med beaktande av de administrativa kostnaderna för att tillhandahålla information eller kommunicera eller vidta den begärda åtgärden) eller vägra att tillmötesgå begäran.

192. EDPB påpekar att personuppgiftsansvariga å ena sidan inte är skyldiga rent generellt att ta ut en rimlig avgift innan de vägrar att tillmötesgå en begäran. Å andra sidan är de inte helt fria att välja mellan de båda alternativen heller. De personuppgiftsansvariga måste i själva verket fatta ett lämpligt beslut beroende på de särskilda omständigheterna i fallet. Även om det är svårt att föreställa sig att en lämplig åtgärd vid uppenbart ogrundade begäranden är att ta ut en rimlig avgift, kommer det i enlighet med principen om insyn vara lämpligare att vid orimliga begäranden ta ut en avgift som kompensation för de administrativa kostnader som repetitiva begäranden ger upphov till.

193. Personuppgiftsansvariga måste kunna visa att en begäran är uppenbart ogrundad eller orimlig (artikel 12.5 tredje meningen i dataskyddsförordningen). Det rekommenderas därför att man säkerställer en riktig dokumentation av de underliggande omständigheterna. I enlighet med artikel 12.4 i dataskyddsförordningen måste personuppgiftsansvariga, om de helt eller delvis vägrar att följa en begäran om tillgång, utan dröjsmål och senast inom en månad efter mottagandet av begäran informera den registrerade om

- skälet till detta,
- rätten att lämna in ett klagomål till en tillsynsmyndighet,
- möjligheten att ansöka om rättslig prövning.

194. Innan personuppgiftsansvariga tar ut en rimlig avgift på grundval av artikel 12.5 i dataskyddsförordningen bör de ge en indikation om att de planerar detta till de registrerade. De senare måste kunna avgöra om de ska dra tillbaka sin begäran för att undvika att bli debiterade.

195. Omotiverade avslag på begäranden om rätt till tillgång kan betraktas som en överträdelse av registrerades rättigheter enligt artiklarna 12–22 i dataskyddsförordningen och kan därför bli föremål för behöriga tillsynsmyndigheters utövande av korrigerande befogenheter, inbegripet administrativa sanktionsavgifter på grundval av artikel 83.5 b i dataskyddsförordningen. Om registrerade anser att deras rättigheter kränks har de rätt att lämna in klagomål på grundval av artikel 77 i dataskyddsförordningen.

6.4 Möjliga begränsningar och undantag i unionsrätten eller medlemsstaternas lagstiftning på grundval av artikel 23 i dataskyddsförordningen

196. Tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artikel 15 i dataskyddsförordningen kan begränsas genom lagstiftningsåtgärder i unionsrätten eller medlemsstaternas lagstiftning[106].

197. Personuppgiftsansvariga, som har för avsikt att stödja sig på en begränsning som grundar sig på nationell lagstiftning, måste noggrant undersöka bestämmelsens krav i respektive nationell

[106] Se t.ex. avsnitten 32–37 i den tyska federala dataskyddslagen (BDSG), avsnitten 16 och 17 i den norska lagen om personuppgifter och kapitel 5 i den svenska dataskyddslagen.

lagstiftning. Det är dessutom viktigt att notera att begränsningar av rätten till tillgång i medlemsstaternas (eller unions) lagstiftning som grundar sig på artikel 23 i dataskyddsförordningen strikt måste uppfylla villkoren i denna bestämmelse. EDPB har utfärdat riktlinjer 10/2020 om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen med ytterligare förklaringar kring detta. När det gäller rätten till tillgång påminner EDPB om att personuppgiftsansvariga bör upphäva begränsningarna så snart de omständigheter som motiverar dessa inte längre föreligger[107].

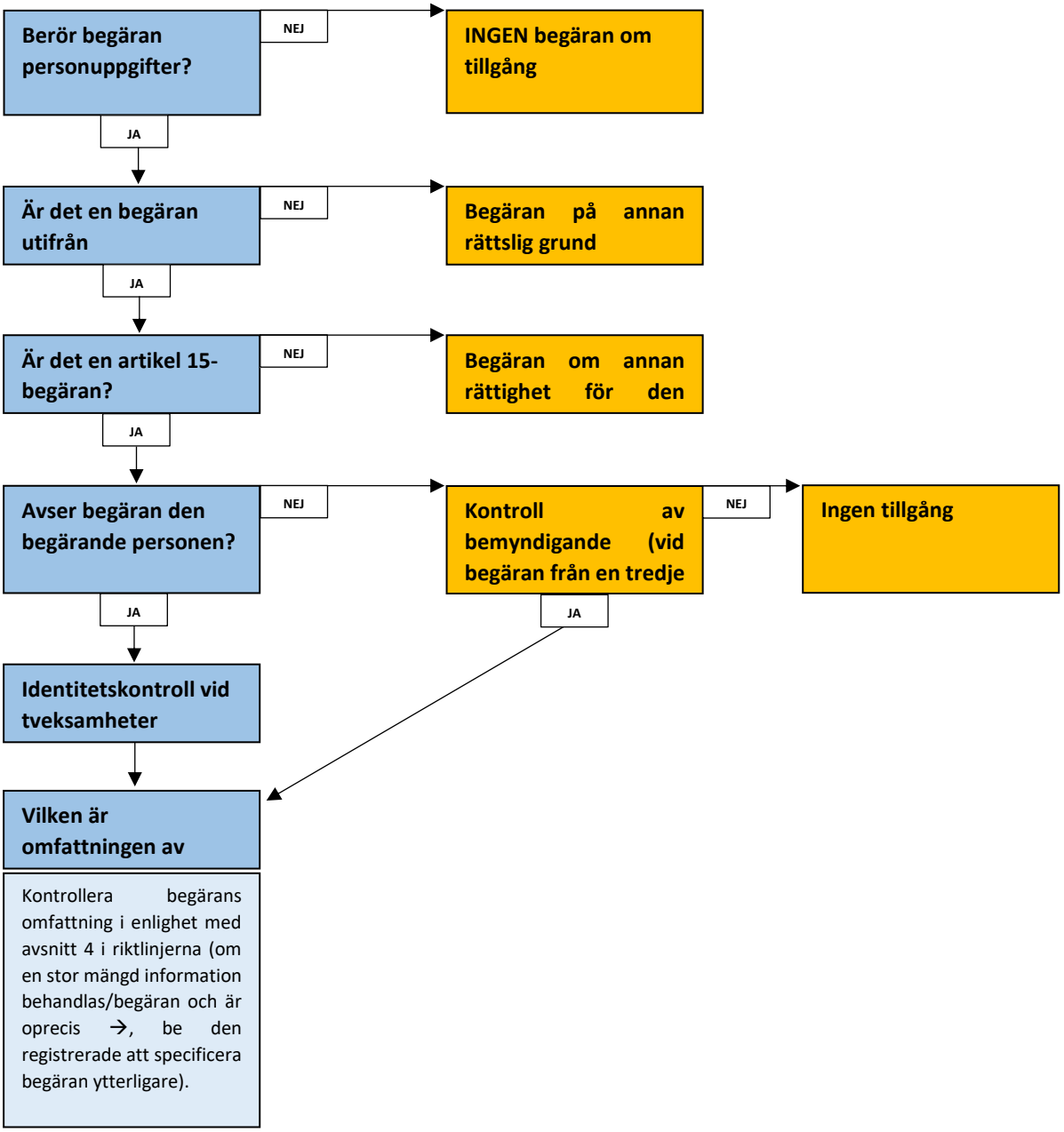
198. De lagstiftningsåtgärder som medför begränsningar enligt artikel 23 i dataskyddsförordningen får också föreskriva att utövandet av en rättighet skjuts upp, att en rättighet delvis utövas eller avgränsas till vissa kategorier av uppgifter eller att en rättighet kan utövas indirekt genom en oberoende tillsynsmyndighet[108].

[107] Punkt 76 i riktlinjerna om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen, version 2.0, som antogs den 13 oktober 2021.

[108] Punkt 12 i riktlinjerna om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen, version 2.0, som antogs den 13 oktober 2021. I avsnitt 34.3 i den tyska federala dataskyddslagen anges till exempel att om en offentlig myndighet inte tillhandahåller information till en registrerad, för att tillmötesgå en begäran om tillgång på grund av vissa begränsningar, ska sådan information lämnas till den federala tillsynsmyndigheten på begäran av den registrerade, såvida inte den ansvariga högsta federala myndigheten (till den myndighet som var föremål för begäran) i det enskilda fallet fastställer att detta skulle äventyra förbundsstatens eller en delstats säkerhet. Den italienska DPCode ger (genom myndigheten) indirekt tillgång i de fall tillgången skulle kunna påverka flera olika intressen negativt (t.ex. intresset av att motverka penningtvätt), se artikel 2-L i den italienska DPCode.

BILAGA – FLÖDESSCHEMA

Steg 1: Hur begäran ska tolkas och bedömas?



Steg 2: Hur besvaras begäran (1)?

3 huvudkomponenter i rätten till tillgång (struktur enligt artikel 15)		
Bekräftelse på huruvida personuppgifter håller på att	Tillgång till personuppgifterna	Ytterligare information om ändamål, mottagare osv. (artikel 15.1 a–h)

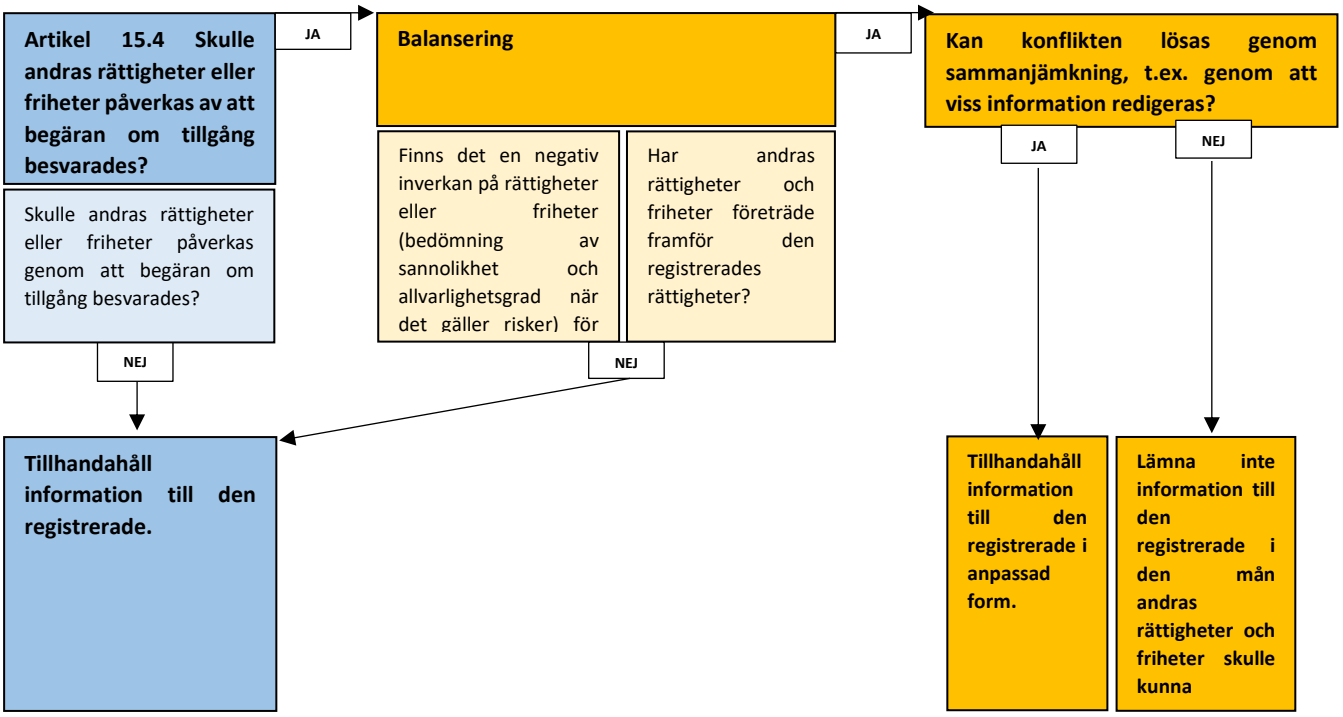
Steg 2: Hur besvaras begäran (2)?

Vidta lämpliga åtgärder			
Artikel 12.1: en koncis, klar och tydlig, begriplig och lätt tillgänglig form.	Artikel 12.2: underlätta utövandet av rätten till tillgång.		
Välj mellan olika metoder.	Tillhandahåll en kopia, om inte annat överenskommits (artikel 15.3).	Använd en skiktad strategi vid behov (mest relevant i onlinesammanhang).	Tidpunkt – utan onödigt dröjsmål, under alla omständigheter inom en månad (förlängning med ytterligare två månader i undantagsfall) (artikel 12.3).

Steg 2: Hur besvaras begäran (3)?

Hur kan den personuppgiftsansvarige hämta alla uppgifter om den registrerade?			
Definiera sökkriterier – baserat på vad den registrerade har tillhandahållit, annan information som den personuppgiftsansvarige har om den registrerade och de faktorer som uppgifterna är strukturerade utifrån (t.ex. kundnummer, IP-adresser, yrkestitel, familjerelationer osv.).	Identifiera vilka tekniska funktioner som kan vara tillgängliga för att hämta uppgifter.	Sök igenom alla relevanta it- eller icke-it-register.	Sammanställ, extrahera eller samla på annat sätt in uppgifter som rör den registrerade på ett sätt som fullständigt återspeglar behandlingen, dvs. som omfattar alla personuppgifter som rör den registrerade och gör det möjligt för den registrerade att vara medveten om och kontrollera att behandlingen är laglig. Informationen kan hämtas från fall till fall eller, i förekommande fall, med hjälp av ett verktyg för inbyggt

Steg 3: Kontrollera gränser och begränsningar (1)



Steg 3: Kontrollera gränser och begränsningar (2)