17/SV

WP260rev.01

Artikel 29-arbetsgruppen

Riktlinjer om öppenhet enligt förordning (EU) 2016/679

Antagna den 29 november 2017

Senast granskade och antagna den 11 april 2018

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ

BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DESSA RIKTLINJER

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av dess arbetsordning.

Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet. Dess uppgifter beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

Gruppens sekretariat finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) på Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, kontor MO-59 02/013.

Webbplats: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Innehållsförteckning

Inledning

1. I dessa riktlinjer ger artikel 29-arbetsgruppen praktisk vägledning och hjälp med att tolka den nya öppenhetsskyldigheten vid behandling av personuppgifter i enlighet med den allmänna dataskyddsförordningen[1]. Öppenhet är en övergripande skyldighet enligt dataskyddsförordningen vilken tillämpas på tre centrala områden: 1) hur de registrerade får informeras om rättvis behandling, 2) hur de personuppgiftsansvariga kommunicerar med de registrerade i förhållande till deras rättigheter enligt dataskyddsförordningen och 3) hur de personuppgiftsansvariga underlättar de registrerades utövande av sina rättigheter[2]. I den mån som öppenhetsprincipen måste iakttas vid uppgiftsbehandling i enlighet med direktiv (EU) 2016/680[3], gäller dessa riktlinjer även för tolkningen av denna princip[4]. Riktlinjerna är, precis som alla riktlinjer från artikel 29-arbetsgruppen, avsedda att tillämpas generellt och vara relevanta för personuppgiftsansvariga oavsett sektor eller bransch eller vilka regler de omfattas av. Därför kan dessa riktlinjer inte omfatta alla de olika särdrag och situationer som kan uppstå när det gäller öppenhetskraven inom en specifik sektor eller bransch eller på ett specifikt lagstiftningsområde. Syftet med riktlinjerna är dock att de personuppgiftsansvariga ska få omfattande kunskap om artikel 29-arbetsgruppens tolkning av vad öppenhetskraven innebär i praktiken och hur de enligt artikel 29-arbetsgruppen bör gå till väga för att vara insynsvänliga och samtidigt garantera korrekthet och ansvarighet i sina öppenhetsåtgärder.

2. Öppenhet är något som sedan länge finns förankrat i EU-rätten[5]. Det handlar om att skapa tillit till processer som berör medborgarna genom att få dem att förstå och, om så krävs,

[1] 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.

[2] I dessa riktlinjer fastställs allmänna principer för de registrerades utövande av sina rättigheter snarare än särskilda villkor för de registrerades rättigheter enligt dataskyddsförordningen.

[3] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

[4] Öppenhet ingår inte bland principerna för behandling av personuppgifter i artikel 4 i direktiv (EU) 2016/680, men i skäl 26 anges det att varje behandling av personuppgifter måste vara ”laglig, korrekt och öppen” i förhållande till berörda fysiska personer.

[5] Enligt artikel 1 i EU-fördraget ska beslut fattas ”*så öppet som möjligt och så nära medborgarna som möjligt*” och enligt artikel 11.2 ska institutionerna ”*föra en öppen, tydlig och regelbunden dialog med de representativa sammanslutningarna och det civila samhället*”. I artikel 15 i EUF-fördraget anges det bland annat att unionsmedborgare ska ”*ha rätt till unionens institutioners, organs och byråers handlingar*” och att dessa institutioner, organ och byråer ska ”*säkerställa öppenhet i sitt arbete*”.

bestrida sådana processer. Det är också ett uttryck för den rättviseprincip vid behandling av personuppgifter som anges i artikel 8 i EU-stadgan om de grundläggande rättigheterna. Utöver kraven att uppgifterna måste behandlas på ett lagligt och öppet sätt enligt dataskyddsförordningen (artikel 5.1 a[6]) ingår öppenhet nu som en grundläggande aspekt av dessa principer[7]. Öppenhet har en direkt koppling till rättviseprincipen och den nya ansvarsprincipen i dataskyddsförordningen. Enligt artikel 5.2 måste den personuppgiftsansvarige alltid kunna visa att personuppgifterna behandlas på ett öppet sätt gentemot den registrerade.[8] I anslutning till detta kräver ansvarsprincipen att personuppgifter behandlas på ett öppet sätt, så att de registrerade kan visa att de fullgör sina skyldigheter enligt dataskyddsförordningen[9].

3. Enligt skäl 171 i dataskyddsförordningen bör en personuppgiftsansvarig, i de fall behandling redan pågår före den 25 maj 2018, se till att denna är förenlig med öppenhetskraven per den 25 maj 2018 (samt alla övriga skyldigheter i dataskyddsförordningen). Detta innebär att de personuppgiftsansvariga bör se över all information som lämnats till de registrerade i fråga om behandling av deras personuppgifter (t.ex. i integritetspolicyer/integritetsmeddelanden) för att säkerställa att de uppfyller de öppenhetskrav som behandlas i dessa riktlinjer. Om ändringar eller tillägg har gjorts i sådan information bör de personuppgiftsansvariga informera de registrerade om att förändringarna har gjorts med anledning av dataskyddsförordningen. Artikel 29-arbetsgruppen rekommenderar att de personuppgiftsansvariga informerar de registrerade om sådana ändringar eller tillägg, men att de som ett minimum offentliggör sådan information för allmänheten (t.ex. på sin webbplats). Om ändringarna eller tilläggen är relevanta eller väsentliga bör de dock, i linje med punkterna 29–32 nedan, aktivt informera de registrerade om dessa.

4. När de personuppgiftsansvariga respekterar öppenhetsprincipen kan de registrerade hålla personuppgiftsansvariga och personuppgiftsbiträden ansvariga och utöva kontroll över sina personuppgifter, genom att exempelvis ge eller återkalla informerat samtycke och utöva sina rättigheter som registrerade[10]. Begreppet öppenhet i dataskyddsförordningen är användarcentrerat snarare än formalistiskt och tar konkret form i praktiska krav på personuppgiftsansvariga och personuppgiftsbiträden i ett flertal artiklar. De praktiska kraven (informationskraven) anges i artiklarna 12–14 i dataskyddsförordningen.

---

[6] ”Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade […].”

[7] I direktiv 95/46/EG nämndes öppenhet endast i skäl 38 genom ett krav om att personuppgifter ska behandlas korrekt, men ingen uttrycklig hänvisning görs i motsvarande artikel 6.1 a.

[8] Enligt artikel 5.2 i dataskyddsförordningen måste en personuppgiftsansvarig visa att öppenhetsprincipen efterlevs (samt de övriga fem principer för behandling av personuppgifter som anges i artikel 5.1) i enlighet med ansvarsprincipen.

[9] I artikel 24.1 anges de personuppgiftsansvarigas skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandling sker i enlighet med dataskyddsförordningen.

[10] Se t.ex. förslag till avgörande av generaladvokat Pedro Cruz Villalón föredraget den 9 juli 2015 i mål C-201/14, Smaranda Bara m.fl., punkt 74: *”kravet på information till de registrerade vars personuppgifter behandlas, vilket säkerställer insyn i varje behandling, är av särskilt stor betydelse eftersom det utgör en förutsättning för att de berörda personerna ska kunna utöva sin rätt till tillgång till de behandlade uppgifterna, vilken avses i artikel 12 i direktiv 95/46, och deras rätt att göra invändningar mot behandlingen av dessa uppgifter, vilken fastställs i artikel 14 i direktivet.”*

Informationens kvalitet, åtkomlighet och begriplighet är dock lika viktigt som det faktiska innehållet i den klara och tydliga information som måste ges till de registrerade.

5. Öppenhetskraven i dataskyddsförordningen gäller oavsett rättslig grund för behandlingen och under hela behandlingens löptid. Detta framgår tydligt av artikel 12 där det anges att öppenhet ska iakttas vid följande skeden av uppgiftsbehandlingen:

- Innan eller när uppgiftsbehandlingen inleds, det vill säga när personuppgifterna inhämtas antingen från den registrerade eller från annat håll.
- Under hela behandlingen, dvs. vid kommunikation med registrerade om deras rättigheter.
- Vid särskilda tillfällen under pågående behandling, till exempel vid personuppgiftsincidenter eller vid väsentliga förändringar i behandlingen.

Öppenhetens innebörd

6. Öppenhet definieras inte i dataskyddsförordningen. Skäl 39 i dataskyddsförordningen är informativt beträffande öppenhetsprincipens innebörd och effekter för uppgiftsbehandling:

> *"Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas […]."*

Delar som rör öppenhet i dataskyddsförordningen

7. De viktigaste artiklarna i fråga om öppenhet i dataskyddsförordningen, eftersom de avser de registrerades rättigheter, finns i kapitel III ("Den registrerades rättigheter"). I artikel 12 anges de allmänna reglerna för tillhandahållande av information till registrerade (artiklarna 13 och 14), kommunikation med registrerade beträffande utövandet av deras rättigheter (artiklarna 15–22) och kommunikation vid personuppgiftsincidenter (artikel 34). Särskilt i artikel 12 krävs det att informationen eller kommunikationen måste uppfylla följande bestämmelser:

- Den måste vara i en koncis, klar och tydlig, begriplig och lätt tillgänglig form (artikel 12.1).
- Ett klart och tydligt språk måste användas (artikel 12.1).

- Kravet om ett klart och tydligt språk är särskilt viktigt för information som är riktad till barn (artikel 12.1).
- Informationen ska tillhandahållas skriftligt, "*eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form*" (artikel 12.1).
- Om den registrerade begär det får informationen tillhandahållas muntligt (artikel 12.1).
- Generellt sett ska den tillhandahållas kostnadsfritt (artikel 12.5).

"En koncis, klar och tydlig, begriplig och lätt tillgänglig form"

8. Kravet att information som tillhandahålls eller kommuniceras till de registrerade ska vara i en "koncis, klar och tydlig" form innebär att de personuppgiftsansvariga bör presentera informationen/kommunicera på ett effektivt och kortfattat sätt för att undvika informationsutmattning. Informationen bör tydligt särskiljas från annan information som inte avser integritet, exempelvis avtalsbestämmelser eller allmänna användarvillkor. I internetsammanhang kan skiktade integritetspolicyer/integritetsmeddelanden göra det möjligt för de registrerade att direkt gå till en viss del av integritetspolicyn/integritetsmeddelandet som de vill läsa, i stället för att skrolla igenom stora mängder text för att hitta delen i fråga.

9. Kravet att informationen ska vara "begriplig" innebär att den bör kunna förstås av en genomsnittsmedlem av den avsedda målgruppen. Begriplighet har nära koppling till kravet om ett klart och tydligt språk. En personuppgiftsansvarig kommer att få kunskap om de personer som de samlar in uppgifter om och kan använda sig av denna för att avgöra vad som troligen skulle vara begripligt för målgruppen. En personuppgiftsansvarig som samlar in personuppgifter om yrkesutövare kan anta att hans eller hennes målgrupp förstår mer än vad barn gör. Om de personuppgiftsansvariga är osäkra på informationens begriplighet och öppenhet samt ändamålsenligheten i användargränssnitt/meddelanden/policyer och så vidare, kan de testa detta genom mekanismer som användargrupper, läsbarhetstester, formell och informell interaktion och dialog med branschföreträdare, konsumenträttsgrupper och tillsynsorgan och så vidare, där så är lämpligt.

10. En viktig aspekt av den öppenhetsprincip som beskrivs i dessa bestämmelser är att de registrerade på förhand bör kunna avgöra syftet med och konsekvenserna av behandlingen och att det inte bör komma som en överraskning för dem i ett senare skede hur deras personuppgifter har använts. Detta är även en viktig aspekt av rättviseprincipen enligt artikel 5.1 i dataskyddsförordningen, där det faktiskt finns en koppling till skäl 39 som anger att fysiska personer "*bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter*". När det gäller komplex, teknisk eller oväntad uppgiftsbehandling anser artikel 29-arbetsgruppen i synnerhet att de personuppgiftsansvariga inte bara bör tillhandahålla sådan information som anges i artiklarna 13 och 14 (vilken behandlas senare i dessa riktlinjer), utan att de även bör ange, i ett separat avsnitt och på ett otvetydigt språk, de mest betydande *konsekvenserna* av behandlingen, med andra ord hur den särskilda behandling som anges i en integritetspolicy/ett integritetsmeddelande faktiskt kommer att inverka på de registrerade.

I linje med ansvarsprincipen och skäl 39 bör de personuppgiftsansvariga bedöma huruvida särskilda risker föreligger för fysiska personer vars personuppgifter behandlas på ett sådant sätt, vilka de registrerade bör uppmärksammas på. På så sätt kan man få en översikt över de typer av behandlingar som skulle kunna få störst inverkan på de registrerades grundläggande rättigheter och friheter när det gäller skyddet av deras personuppgifter.

11. ”Lättillgänglig” innebär att de registrerade inte ska behöva leta reda på informationen; det bör vara direkt uppenbart för dem var och hur de kan få åtkomst till informationen, exempelvis genom att informationen ges direkt eller länkas till de registrerade, genom tydlig vägledning eller som ett svar på en fråga från en fysisk person (t.ex. i en integritetspolicy/ett integritetsmeddelande i flera skikt online, i ”Vanliga frågor”, via kontextuella popupmeddelanden som aktiveras när de registrerade fyller i ett onlineformulär eller i en interaktivt digitalt kontext via ett chatbotgränssnitt osv. Sådana mekanismer behandlas vidare nedan, bland annat i punkterna 33–40).

Exempel

Alla organisationer som har en webbplats bör offentliggöra en integritetspolicy/ett integritetsmeddelande på denna. På varje sida av webbplatsen bör det finnas en klart synlig direktlänk till integritetspolicyn/integritetsmeddelandet som ska ha försetts med en lämplig rubrik (t.ex. ”Integritet”, ”Integritetspolicy” eller ”Uppgiftsskyddsmeddelande”). Lättillgänglighet anses inte skapas genom positionerings- eller färgsystem som gör en text eller länk mindre synlig eller svår att hitta på en webbplats.

När det gäller appar bör nödvändig information även finnas att få från onlinebutikerna före nedladdning. Så snart appen har installerats måste informationen fortfarande finnas lättillgänglig inuti appen. Ett sätt att uppfylla detta krav är att se till att informationen aldrig är mer än ”två klick bort” (t.ex. genom att inkludera en flik om integritet eller uppgiftsskydd i appens menyfunktion). Dessutom bör integritetsinformationen enbart avse appen i fråga och inte bara bestå av den allmänna integritetsinformationen för det företag som äger eller erbjuder appen till allmänheten.

Artikel 29-arbetsgruppen rekommenderar en bästa praxis som innebär att en länk till integritetspolicyn/integritetsmeddelandet ges eller att sådan information ges på samma sida som personuppgifterna inhämtas från, när personuppgifter samlas in online.

”Klart och tydligt språk”

12. Vid skriftlig information (och där skriftlig information ges muntligen, eller via ljudfiler eller audiovisuellt, inbegripet för registrerade med synnedsättning) bör bästa klarspråkspraxis

följas[11]. Ett liknande språkkrav ("ett klart och begripligt språk") har tidigare använts av EU-lagstiftaren[12] och en uttrycklig hänvisning görs också till detta när det gäller samtycke i skäl 42 i dataskyddsförordningen[13]. Kravet om ett klart och tydligt språk innebär att informationen bör ges på ett så enkelt sätt som möjligt och att komplicerade meningar och språkstrukturer bör undvikas. Informationen bör vara konkret och exakt, och den bör inte vara abstrakt eller tvetydig eller kunna tolkas på olika sätt. Framför allt bör syftena med och de rättsliga grunderna för behandlingen av personuppgifterna vara tydliga.

Exempel på dålig praxis

Följande fraser är inte tillräckligt tydliga vad gäller syftena med behandlingen:

- *"Vi får använda dina personuppgifter för att utveckla nya tjänster"* (det är oklart vilka dessa "tjänster" är eller hur uppgifterna kommer att bidra till utvecklingen av dessa).

- *"Vi får använda dina personuppgifter för forskningsändamål"* (det är oklart vilken typ av forskning som avses).

- *"Vi får använda dina personuppgifter för att erbjuda personliga tjänster"* (det är oklart vad som avses med "personliga").

Exempel på god praxis[14]

- *"Vi kommer att spara din shoppinghistorik och använda uppgifter om de produkter som du tidigare har köpt för att föreslå andra produkter som vi tror att du också är intresserad av"* (det är tydligt vilka typer av uppgifter som kommer att behandlas, att den registrerade kommer att få ta emot riktad produktreklam och att personuppgifterna kommer att användas för detta ändamål).

- *"Vi kommer att spara och granska uppgifter om dina senaste besök på vår webbplats och om hur du navigerar mellan olika delar av denna för analysändamål, för att få kunskap om hur personer använder vår webbplats så att vi kan göra den mer intuitiv"* (det är tydligt vilka typer av uppgifter som kommer att behandlas och vilken sorts analys den personuppgiftsansvarige kommer att göra).

- *"Vi kommer att registrera de artiklar på vår webbplats som du har klickat på och*

[11] Se *Skriva klarspråk*, Europeiska kommissionen (2011): https://publications.europa.eu/sv/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1

[12] Artikel 5 i rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal.

[13] I skäl 42 anges att en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat bör tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäliga villkor.

[14] Insynskravet gäller fullt ut oberoende av kravet om att de personuppgiftsansvariga måste se till att det finns en lämplig rättslig grund för behandlingen enligt artikel 6.

använda denna information för att du ska få reklam på vår webbplats utifrån dina intressen, som vi har fastställt utifrån de artiklar som du har läst" (det är klart vad individanpassningen innebär och hur den registrerades intressen har fastställts).

13. Bestämningsord som "får", "kan", "viss", "ofta" och "eventuellt" bör också undvikas. Om de personuppgiftsansvariga väljer att använda ett svävande språk bör de, i överensstämmelse med ansvarsprincipen, kunna visa varför sådant språk inte har kunnat undvikas och att detta inte innebär att behandlingens korrekthet undergrävs. Punkter och meningar bör struktureras på ett bra sätt, och hierarkiska strukturer bör påvisas med hjälp av punkt- och strecksatser. Man bör skriva i aktiv form i stället för i passiv form och man bör undvika överdriven substantivering. Den information som ges till de registrerade bör inte innehålla ett språk eller en terminologi som är överdrivet formalistisk, teknisk eller specialiserad. Om informationen översätts till ett eller flera språk bör den personuppgiftsansvarige säkerställa att alla översättningar är riktiga och att språkbruket och syntaxen får rätt innebörd på det språket eller de andra språken, så att den översatta texten inte måste tydas eller tolkas på nytt. (En översättning till ett eller flera språk bör ges om den personuppgiftsansvarige riktar sig till[15] registrerade som talar dessa språk.)

Information till barn och andra utsatta personer

14. Om personuppgiftsansvariga riktar sig till barn[16] eller är, eller borde vara, medvetna om att deras tjänster särskilt används av barn (inklusive när de personuppgiftsansvariga åberopar barnens samtycke)[17], bör det säkerställas att vokabulären, tonen och stilen i det språk som används är lämpligt och anpassat för barn, så att de barn som får informationen förstår att meddelandet/informationen är riktat till dem[18]. Ett användbart exempel på ett barnvänligt språk som kan användas i stället för vanligt juridiskt språk finns i "Barnkonventionen – En lättläst skrift om konventionen om barnets rättigheter"[19].

15. Artikel 29-arbetsgruppen anser att öppenhet är en fristående rättighet som gäller lika mycket för barn som för vuxna. Artikel 29-arbetsgruppen betonar särskilt att barn, i egenskap av registrerade, inte förlorar sina rättigheter till öppenhet bara för att samtycke har getts/godkänts av den person som har föräldraansvar för barnet i en sådan situation

[15] Om den personuppgiftsansvarige har en webbplats på språket i fråga och/eller har landsspecifika erbjudanden och/eller underlättar betalning för varor och tjänster i en viss medlemsstats valuta, måste det framgå att översättningarna kommer från en personuppgiftsansvarig som riktar sig till registrerade i en viss medlemsstat.

[16] Ingen definition ges av begreppet "barn" i dataskyddsförordningen, men enligt artikel 29-arbetsgruppen är ett barn en person under 18 års ålder, i enlighet med barnkonventionen som ratificerats av alla EU-medlemsstater.

[17] Här avses barn som är 16 år eller mer (eller barn som uppnått den nationella samtyckesåldern i fall där medlemsstaterna i sin nationella rätt har fastställt samtyckesåldern till en viss ålder mellan 13 och 16 år för att barn ska få samtycka till ett erbjudande av informationssamhällestjänster).

[18] I skäl 38 anges följande: "Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter." I skäl 58 anges följande: "Eftersom barn förtjänar särskilt skydd, bör all information och kommunikation som riktar sig till barn utformas på ett tydligt och enkelt språk som barnet lätt kan förstå."

[19] https://www.barnombudsmannen.se/globalassets/systemimporter/publikationer2/barnkonv_lattlastweb-2014.pdf

som avses i artikel 8 i dataskyddsförordningen. Sådant samtycke ges eller godkänns i många fall en enda gång av den person som har föräldraansvaret, men ett barn har (precis som alla andra registrerade) fortfarande rätt till öppenhet under hela den period som avtalet med den personuppgiftsansvarige avser. Detta är i linje med artikel 13 i barnkonventionen där det anges att ett barn har rätt till yttrandefrihet, vilket innefattar frihet att "söka, ta emot och sprida information och tankar av alla slag"[20]. Det bör påpekas att det i artikel 8 anges att samtycke måste ges på ett barns vägnar när barnet är under en viss ålder,[21] men *inte* att öppenhetsrelaterade åtgärder måste riktas till den person som innehar föräldraansvar och ger samtycket. De personuppgiftsansvariga är därför skyldiga, enligt de särskilda öppenhetsåtgärder som ska vidtas när det gäller barn enligt artikel 12.1 (med stöd av skälen 38 och 58), att säkerställa att all information och kommunikation sker på ett klart och tydligt språk eller via ett medium som är lättbegripligt för barn, om de riktar sig till barn eller är medvetna om att deras varor eller tjänster särskilt används av barn i läs- och skrivkunnig ålder. För att undvika tvivel anser dock artikel 29-arbetsgruppen att öppenhetsåtgärderna också ska få riktas till personer som har föräldraansvar för barn som är mycket små eller inte är läs- och skrivkunniga, eftersom sådana barn i de flesta fall sannolikt inte kommer att kunna förstå ens de enklaste meddelanden om öppenhet som ges i skriftlig eller annan form.

16. På samma sätt gäller att om de personuppgiftsansvariga är medvetna om att deras varor/tjänster används av (eller riktas till) andra utsatta personer i samhället, inklusive personer med funktionsnedsättning eller personer som kan ha svårt att få åtkomst till information, bör de registrerade beakta sårbarheterna hos sådana registrerade när de bedömer hur de ska säkerställa respekt för öppenhetsskyldigheterna beträffande sådana registrerade[22]. Detta har att göra med att de personuppgiftsansvariga måste bedöma hur mycket målgruppen kan tänkas förstå, vilket behandlas i punkt 9 ovan.

"Skriftligt, eller i någon annan form"

17. Enligt artikel 12.1 är standardregeln för information till eller kommunikation med de registrerade att informationen tillhandahålls skriftligt[23]. (Enligt artikel 12.7 får information även tillhandahållas kombinerad med standardiserade symboler, och detta behandlas i avsnittet om visualiseringsverktyg i punkterna 49–53.) Enligt dataskyddsförordningen får dock även andra, ospecificerade "medel" användas, inbegripet elektroniska former. Artikel 29-arbetsgruppens ståndpunkt när det gäller skriftlig elektronisk form är att skiktade integritetspolicyer/integritetsmeddelanden bör användas om de personuppgiftsansvariga har en webbplats (eller helt eller delvis bedriver sin verksamhet via en sådan). Besökarna på

[20] I artikel 13 i barnkonventionen anges följande: "Barnet ska ha rätt till yttrandefrihet. Denna rätt innefattar frihet att oberoende av territoriella gränser söka, ta emot och sprida information och tankar av alla slag, i tal, skrift eller tryck, i konstnärlig form eller genom annat uttrycksmedel som barnet väljer."

[21] Se fotnot 17.

[22] Enligt konventionen om rättigheter för personer med funktionsnedsättning måste till exempel lämpliga former av hjälp och stöd ges till personer med funktionsnedsättning för att säkerställa deras tillgång till information.

[23] Artikel 12.1 handlar om "språk" och bland annat anges att informationen "ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form".

webbplatsen kan då navigera till särskilda delar av integritetspolicyn/integritetsmeddelandet som är av störst intresse för dem (läs mer om skiktade integritetspolicyer/integritetsmeddelanden i punkterna 35–37)[24]. All den information som riktas till de registrerade bör dock även finnas tillgänglig för dem på en och samma plats eller i ett fullständigt dokument (i digitalt format eller pappersformat), som de registrerade lätt kan få tillgång till om de vill läsa all den information som riktas till dem. Nog så viktigt är att skiktad information inte enbart handlar om skriftliga elektroniska medel för att ge information till de registrerade. Såsom behandlas i punkterna 35, 36 och 38 nedan kan skiktad information till de registrerade även användas tillsammans med andra *metoder* för att säkerställa öppenhet i behandlingen.

18. Självklart är inte digitala skiktade integritetspolicyer/integritetsmeddelanden de enda skriftliga elektroniska medel som de personuppgiftsansvariga kan använda. Annan elektronisk form är till exempel kontextuella popupmeddelanden i realtid, 3D Touch eller ”hover-meddelanden” och integritetsinfopaneler. Ej skriftlig elektronisk form som kan användas *utöver* skiktade integritetspolicyer/integritetsmeddelanden kan bland annat vara videor samt smartphone- och IoT-röstaviseringar[25]. ”Annan form”, som inte nödvändigtvis innefattar elektronisk form, kan till exempel vara tecknade serier, infografik eller flödesscheman. När den öppenhetsrelaterade informationen särskilt är riktad till barn bör de personuppgiftsansvariga fundera över vilka slags åtgärder som kan vara särskilt tillgängliga för barn (t.ex. serier, tecknade filmer, piktogram och animationer).

19. Det är ytterst viktigt att den metod eller de metoder som väljs för att ge informationen är lämpliga för situationen i fråga, det vill säga för hur den personuppgiftsansvarige och den registrerade interagerar eller hur den registrerades uppgifter inhämtas. Det kan till exempel vara olämpligt/opraktiskt att ge informationen i elektroniskt skriftligt format, till exempel i en integritetspolicy/ett integritetsmeddelande, om den utrustning som fångar upp uppgifterna saknar skärm (t.ex. IoT-utrustning/smart utrustning) för tillgång till webbplatsen/visning av den skriftliga informationen. I sådana fall bör *andra* alternativa sätt övervägas, till exempel att integritetspolicyn/integritetsmeddelandet ges i instruktionsmanualer i pappersform eller att webbadressen anges (dvs. adressen till den särskilda sidan på webbplatsen) där integritetspolicyn/integritetsmeddelandet online finns i pappersinstruktionerna eller i paketet. Information via ljudfiler (muntlig information) skulle också kunna ges om den skärmlösa utrustningen har ljudfilskapacitet. Artikel 29-arbetsgruppen har tidigare avgett rekommendationer om öppenhet och tillhandahållande av information till registrerade i sitt yttrande om den senaste utvecklingen av sakernas internet[26] (t.ex. användning av sakernas internet så att en skannad QR-kod visar den nödvändiga öppenhetsrelaterade informationen). Dessa rekommendationer är fortfarande gällande enligt dataskyddsförordningen.

[24] Artikel 29-arbetsgruppens erkännande av fördelarna med skiktade meddelanden noterades redan i yttrande 10/2004 om mer harmoniserade bestämmelser om informationsplikt och yttrande 2/2013 om appar på smarta enheter.

[25] Dessa exempel på elektroniska former ges endast i vägledande syfte och de personuppgiftsansvariga får ta fram nya innovativa metoder för att iaktta kraven i artikel 12.

[26] Artikel 29-arbetsgruppens yttrande 8/2014, antaget den 16 september 2014.

"… får informationen tillhandahållas muntligt"

20. I artikel 12.1 anges det uttryckligen att informationen får tillhandahållas muntligt på de registrerades begäran, förutsatt att deras identitet bevisats på andra sätt. Med andra ord bör man inte bara förlita sig på ett uttalande av personen i fråga om att han eller hon är en viss namngiven person, och den personuppgiftsansvarige bör kunna kontrollera en registrerad persons identitet med tillräcklig försäkran. Kravet om att den registrerades identitet måste kontrolleras innan muntlig information ges gäller endast information om en viss registrerad persons utövande av sina rättigheter enligt artiklarna 15–22 och artikel 34. Detta förhandsvillkor för tillhandahållande av muntlig information får inte tillämpas på tillhandahållande av allmän integritetsinformation såsom anges i artiklarna 13 och 14, eftersom sådan information som krävs enligt artiklarna 13 och 14 också måste göras tillgänglig för *framtida* användare/kunder (vars identitet en personuppgiftsansvarig inte skulle kunna kontrollera). Sådan information som avses i artiklarna 13 och 14 får således tillhandahållas muntligen utan att den personuppgiftsansvarige behöver kräva att den registrerade ska styrka sin identitet.

21. Muntligt tillhandahållande av sådan information som krävs enligt artiklarna 13 och 14 innebär inte nödvändigtvis muntlig information som ges från person till person (dvs. personligen eller via telefon). Automatiserad muntlig information får ges utöver skriftlig information. Så kan till exempel vara fallet när personer med synnedsättning interagerar med leverantörer av informationssamhällets tjänster eller skärmlös smart utrustning, i enlighet med punkt 19 ovan. Artikel 29-arbetsgruppen anser att de personuppgiftsansvariga bör ge de registrerade möjlighet att lyssna på de förinspelade meddelandena igen, om de personuppgiftsansvariga har valt att ge muntlig information till de registrerade eller om de registrerade begär muntlig information eller kommunikation. Detta är obligatoriskt om begäran om muntlig information avser registrerade med synnedsättning eller andra registrerade som kan ha svårt att få tillgång till eller förstå informationen i skriftligt format. De personuppgiftsansvariga bör också se till att de har ett register över och kan styrka följande (för iakttagandet av ansvarskravet): i) begäran om att få muntlig information, ii) den metod som använts för att kontrollera den registrerades identitet (i tillämpliga fall – se punkt 20 ovan) och iii) det faktum att informationen tillhandahållits den registrerade.

"Kostnadsfritt"

22. Enligt artikel 12.5[27] får de personuppgiftsansvariga generellt sett inte ta ut någon avgift för att tillhandahålla sådan information som avses i artiklarna 13 och 14 eller för kommunikationsändamål och åtgärder som vidtas enligt artiklarna 15–22 (om de registrerades rättigheter) samt artikel 34 (om information till den registrerade om en

[27] Här anges följande: "Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt."

personuppgiftsincident)[28]. Denna öppenhetsaspekt innebär också att all information som ges enligt öppenhetskraven inte får göras beroende av finansiella transaktioner, till exempel betalning för eller köp av tjänster eller varor[29].

Information som ska tillhandahållas den registrerade – artiklarna 13 och 14

Innehåll

23. I dataskyddsförordningen anges vilka kategorier av information som måste ges till de registrerade om behandlingen av deras personuppgifter, om personuppgifterna har erhållits från de registrerade (artikel 13) eller från en annan källa (artikel 14). I **tabellen i bilagan** till dessa riktlinjer sammanfattas de kategorier av information som måste tillhandahållas enligt artiklarna 13 och 14. Här beaktas även kravens art, omfattning och ändamål. Av tydlighetsskäl anser artikel 29-arbetsgruppen att det inte finns någon skillnad mellan statusen på sådan information som ska ges enligt punkterna 1 och 2 i artiklarna 13 respektive 14. All sådan information som anges i dessa punkter är lika viktig och måste ges till de registrerade.

"Lämpliga åtgärder"

24. Lika viktigt som innehållet i den information som krävs enligt artiklarna 13 och 14 är även hur den ska ges till de registrerade. Ett meddelande med sådan information kallas vanligen för uppgiftsskyddsmeddelande, integritetsmeddelande, integritetspolicy, sekretesspolicy eller meddelande om rättvis behandling av personuppgifter. I dataskyddsförordningen finns inga regler för i vilket format eller vilka regler som gäller för tillhandahållande av sådan information till de registrerade. Däremot klargörs att det är de personuppgiftsansvarigas ansvar att vidta "lämpliga åtgärder" för tillhandahållandet av den nödvändiga informationen av insynsskäl. Detta innebär att de personuppgiftsansvariga bör beakta alla omständigheter kring insamlingen och behandlingen av uppgifter när de beslutar om lämpliga villkor och format för tillhandahållandet. Framför allt måste de lämpliga åtgärderna bedömas mot bakgrund av produkt-/tjänsteanvändarens erfarenhet. Detta innebär att hänsyn ska tas till vilken utrustning som använts (i tillämpliga fall), typen av användargränssnitt/interaktion med den personuppgiftsansvarige (användarens "resa") och de begränsningar som dessa faktorer medför. Såsom anges ovan i punkt 17 rekommenderar

[28] Enligt artikel 12.5 får dock den personuppgiftsansvarige ta ut en rimlig avgift om till exempel en begäran från en registrerad med avseende på sådan information som avses i artiklarna 13 och 14 eller rättigheterna i artiklarna 15–22 eller artikel 34 är uppenbart ogrundad eller orimlig. (När det gäller rätten till tillgång enligt artikel 15.3 får en personuppgiftsansvarig ta ut en rimlig avgift på grundval av de administrativa kostnaderna för eventuella ytterligare kopior som den registrerade begär av personuppgifterna.)

[29] Om personuppgifter för en registrerad samlas in i samband med ett köp bör till exempel den information som krävs enligt artikel 13 tillhandahållas före betalning och när informationen samlas in, snarare än efter att transaktionen har avslutats. På samma sätt gäller dock att, när gratistjänster tillhandahålls den registrerade, måste sådan information som avses i artikel 13 ges före och inte efter att avtal ingås, eftersom artikel 13.1 innebär att informationen måste tillhandahållas "när personuppgifterna erhålls".

artikel 29-arbetsgruppen att en integritetspolicy/ett integritetsmeddelande i flera skikt online bör ges om den personuppgiftsansvarige finns på internet.

25. För att lättare finna det lämpligaste sättet att tillhandahålla informationen, innan att gå online, kan de personuppgiftsansvariga vilja pröva olika sätt genom användartester (t.ex. tester på olika målgrupper eller andra standardtester gällande läsbarhet eller tillgänglighet), för att få feedback på hur tillgänglig, begriplig och användarcentrerad den föreslagna åtgärden är för användarna. (Se även ytterligare kommentarer ovan om andra mekanismer för användartester i punkt 9.) Genom att dokumentera denna metod skulle det dessutom bli lättare för de personuppgiftsansvariga att visa på vilket sätt det verktyg/den metod som valts för att översända informationen är det lämpligaste verktyget under rådande förhållanden.

Tidpunkt för tillhandahållande av information

26. I artiklarna 13 och 14 anges vilken information som måste ges till de registrerade när behandlingen påbörjas[30]. Artikel 13 gäller scenariot då uppgifterna inhämtas från de registrerade. Detta innefattar följande slags uppgifter:

- Personuppgifter som en registrerad medvetet ger till en personuppgiftsansvarig (t.ex. genom att fylla i ett formulär på internet).
- Personuppgifter som en personuppgiftsansvarig inhämtar från en registrerad genom observation (t.ex. med användning av automatiserad datafångstutrustning eller datafångstprogramvara som kameror, nätverksutrustning, wi-fi-spårning, RFID eller andra slags sensorer).

Artikel 14 gäller scenariot då uppgifterna inte har inhämtats från de registrerade. Detta inbegriper personuppgifter som en personuppgiftsansvarig har erhållit från exempelvis följande källor:

- Personuppgiftsansvariga i egenskap av tredje part.
- Allmänt tillgängliga källor.
- Datamäklare.
- Andra registrerade.

27. När det gäller tidpunkten för tillhandahållandet av informationen är skyldigheten att tillhandahålla informationen snabbt och behandla uppgifter på ett rättvist sätt mycket viktiga delar i öppenhetsskyldigheten. I de fall där artikel 13 är tillämplig måste informationen ges "*när personuppgifterna erhålls*", enligt artikel 13.1. När det gäller

[30] Enligt principerna om rättvisa och ändamålsbegränsning bör den organisation som samlar in de registrerades personuppgifter alltid ange ändamålen med behandlingen vid den tidpunkt då uppgifterna samlas in. Om ändamålet inbegriper avledda personuppgifter måste de registrerade alltid informeras om det avsedda syftet med att skapa och ytterligare behandla sådana avledda personuppgifter samt om de kategorier av avledda uppgifter som behandlas, vid tidpunkten för insamlingen eller innan ytterligare behandling för ett nytt ändamål i enlighet med artiklarna 13.3 eller 14.4.

personuppgifter som har erhållits indirekt enligt artikel 14 anges de tidsramar inom vilka den begärda informationen måste ges till de registrerade i artikel 14.3 a–c:

- Generellt sett måste informationen ges inom en ”rimlig tid” efter det att personuppgifterna har erhållits och senast inom en månad ”*med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas*” (artikel 14.3 a).

- Den allmänna tidsgränsen på en månad i artikel 14.3 a kan minskas ytterligare enligt artikel 14.3 b[31], som handlar om en situation där uppgifterna används för kommunikation med den registrerade. I ett sådant fall måste informationen lämnas senast vid tidpunkten för den första kommunikationen med den registrerade. Om den första kommunikationen sker inom en månad efter det att personuppgifterna har erhållits, måste informationen lämnas *senast* vid tidpunkten för den första kommunikationen med den registrerade även om det inte har gått en månad sedan uppgifterna erhölls. Om den första kommunikationen med den registrerade sker mer än en månad efter det att personuppgifterna har erhållits är artikel 14.3 a fortfarande tillämplig. Detta innebär att sådan information som avses i artikel 14 måste lämnas till den registrerade senast en månad efter erhållandet.

    - Den allmänna tidsgränsen på en månad i artikel 14.3 a kan också minskas ytterligare enligt artikel 14.3 c[32] som handlar om en situation där uppgifterna utlämnas till andra mottagare (oavsett om de är tredje parter eller inte)[33]. I ett sådant fall måste informationen lämnas senast vid tidpunkten för det första utlämnandet. I ett sådant scenario gäller att om det första utlämnandet sker inom en månad, måste informationen lämnas *senast* vid tidpunkten för det första utlämnandet, även om det inte har gått en månad sedan uppgifterna erhölls. I likhet med regeln gällande artikel 14.3 b gäller att om något utlämnande av personuppgifterna görs mer än en månad efter det att personuppgifterna har erhållits är artikel 14.3 a återigen fortsatt tillämplig. Detta innebär att sådan information som avses i artikel 14 måste lämnas till den registrerade senast en månad efter erhållandet.

28. Den längsta tidsfristen för tillhandahållande av sådan information som avses i artikel 14 till den registrerade är därför en månad. Rättvise- och ansvarsprincipen enligt dataskyddsförordningen innebär dock att de personuppgiftsansvariga alltid måste beakta de registrerades rimliga förväntningar, den effekt som behandlingen kan få för dem och deras möjlighet att utöva sina rättigheter med avseende på behandlingen, när de beslutar om när sådan information som avses i artikel 14 ska ges. Ansvarsprincipen innebär att de

[31] Användningen av orden ”*om personuppgifterna ska användas för …*” i artikel 14.3 b innebär en specificering av den allmänna regeln när det gäller den högsta tidsgränsen i artikel 14.3 a men inte att denna ersätts.

[32] Användningen av orden ”*om ett utlämnande till en annan mottagare förutses …*” i artikel 14.3 c innebär en specificering av den allmänna regeln när det gäller den högsta tidsgränsen i artikel 14.3 a, men inte att denna ersätts.

[33] Artikel 4.9 innehåller en definition av begreppet ”mottagare” och ett förtydligande av att en mottagare till vilken personuppgifter utlämnas inte måste vara en tredje part. Mottagare kan därför vara personuppgiftsansvariga, gemensamt personuppgiftsansvariga eller personuppgiftsbiträden.

personuppgiftsansvariga ska ange den logiska grunden till sitt beslut och motivera varför informationen gavs vid en viss tidpunkt. I praktiken kan det vara svårt att uppfylla dessa krav när information ges i "sista stund". I detta avseende anges bland annat i skäl 39 att fysiska personer bör "*göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen*". I skäl 60 hänvisas också till kravet om att de registrerade måste informeras om att behandling sker och syftet med den, enligt principerna om rättvis och öppen behandling. Av alla dessa skäl anser artikel 29-arbetsgruppen att de personuppgiftsansvariga, närhelst så är möjligt, bör ge informationen till de registrerade i god tid före de angivna tidsfristerna, i enlighet med rättviseprincipen. I punkterna 30, 31 och 48 ges ytterligare kommentarer om den lämpliga tidsramen mellan det att de registrerade informeras om behandlingen och behandlingens faktiska inledande.

Ändringar av sådan information som avses i artiklarna 13 och 14

29. Att vara ansvarig gällande öppenhet gäller inte bara vid insamling av personuppgifter utan under hela behandlingen, oavsett vilken information eller kommunikation det rör sig om. Så är till exempel fallet när innehållet i befintliga integritetspolicyer/integritetsmeddelanden ändras. De personuppgiftsansvariga bör följa samma principer när de delger såväl de befintliga integritetspolicyerna/integritetsmeddelandena och alla efterföljande relevanta eller väsentliga ändringar av dessa. Faktorer som de personuppgiftsansvariga bör beakta vid sin bedömning av vad som är en relevant eller väsentlig ändring är bland annat påverkan på de registrerade (inklusive deras möjlighet att utöva sina rättigheter) och hur oväntad/överraskande ändringen skulle bli för de registrerade. Ändringar av integritetspolicyer/integritetsmeddelanden som alltid bör delges de registrerade är bland annat en ändring av behandlingens syfte, en ändring av den personuppgiftsansvariges identitet eller en ändring av hur de registrerade kan utöva sina rättigheter beträffande behandlingen. Artikel 29-arbetsgruppen anser däremot inte att ändringar av integritetspolicyer/integritetsmeddelanden är relevanta eller väsentliga om det handlar om rättelser av felstavningar eller stilistiska/grammatiska brister. Eftersom merparten befintliga kunder eller användare bara kommer att ögna igenom meddelanden om ändringar i integritetspolicyer/integritetsmeddelanden, bör de personuppgiftsansvariga vidta alla åtgärder som krävs för att se till att ändringarna delges på ett sådant sätt att de flesta mottagare faktiskt kommer att uppmärksamma dem. Detta innebär till exempel att meddelanden om ändringar alltid bör delges på lämpligt sätt (t.ex. via e-post, i pappersform, genom ett popupmeddelande på en webbplats eller på något annat sätt som effektivt uppmärksammar de registrerade på ändringarna) och separat (t.ex. inte tillsammans med direktmarknadsföring). Meddelandet bör uppfylla kraven i artikel 12 och vara koncist, klart och tydligt, begripligt och lättillgängligt samt innehålla ett klart och tydligt språk. Hänvisningar i integritetspolicyn/integritetsmeddelandet om att de registrerade regelbundet bör kontrollera om eventuella ändringar eller uppdateringar har gjorts anses vara otillräckliga men också oskäliga inom ramen för artikel 5.1 a. Ytterligare vägledning om tidpunkten för att delge de registrerade ändringar behandlas nedan i punkterna 30–31.

Tidpunkt för information om ändringar av sådan information som avses i artiklarna 13 och 14

30. I dataskyddsförordningen sägs ingenting om de krav gällande tidpunkt (och inte heller metoder) för att underrätta om ändringar i information som tidigare har getts till de registrerade enligt artiklarna 13 eller 14 (bortsett för ett avsett framtida behandlingsändamål, i vilket fall information om det framtida ändamålet måste ges innan denna behandling inleds i enlighet med artiklarna 13.3 och 14.4 – se punkt 45 nedan). Såsom anges ovan när det gäller tidpunkten för att tillhandahålla sådan information som avses i artikel 14, måste den personuppgiftsansvarige återigen beakta rättvise- och ansvarsprinciperna i fråga om den registrerades rimliga förväntningar eller hur ändringarna eventuellt påverkar den registrerade. Om ändringen av informationen tyder på en grundläggande förändring av själva behandlingen (t.ex. fler kategorier av mottagare eller vidarebefordran till ett tredjeland) eller en förändring som kanske inte är grundläggande i fråga om behandlingsåtgärden men som är relevant för och påverkar den registrerade, måste informationen ges till den registrerade i god tid innan ändringen faktiskt träder i kraft. Vidare bör den metod som används för att uppmärksamma den registrerade på ändringen vara tydlig och ändamålsenlig. Skälet till detta är att man ska säkerställa att de registrerade inte "missar" ändringen och att de får rimlig tid på sig för att a) överväga ändringens art och påverkan och b) utöva sina rättigheter enligt dataskyddsförordningen när det gäller ändringen (t.ex. att ta tillbaka sitt samtycke eller invända mot behandlingen).

31. De personuppgiftsansvariga bör noggrant överväga omständigheterna och bakgrunden till varje situation som föranleder en uppdatering av öppenhetsinformationen, inklusive ändringarnas eventuella påverkan på de registrerade och den metod som används för att kommunicera ändringarna. Dessutom bör de kunna visa på vilket sätt tidsfristen mellan det att ändringarna delges och ändringen träder i kraft överensstämmer med principen om rättvisa gentemot de registrerade. Artikel 29-arbetsgruppen anser vidare att de personuppgiftsansvariga, när de informerar de registrerade om sådana ändringar, även bör förklara hur ändringarna sannolikt kommer att påverka dem, i linje med rättviseprincipen. Förenlighet med öppenhetskraven är dock ingen ursäkt för en situation där ändringarna i behandlingen är så omfattande att behandlingen blir av ett helt annat slag jämfört med tidigare. Artikel 29-arbetsgruppen betonar att alla övriga bestämmelser i dataskyddsförordningen, inbegripet de om oförenlig ytterligare behandling, fortsätter att gälla oavsett om öppenhetsskyldigheterna fullgörs eller inte.

32. Dessutom är det troligt, även när öppenhetsinformation (t.ex. i en integritetspolicy/ett integritetsmeddelande) inte ändras väsentligt, att de registrerade som har använt en tjänst under en betydande tid inte kommer att komma ihåg den information som de fick från början enligt artiklarna 13 och/eller 14. Artikel 29-arbetsgruppen rekommenderar att de personuppgiftsansvariga ska underlätta de registrerades tillgång till information, så att de återigen kan sätta sig in i uppgiftsbehandlingens syfte. I linje med ansvarsprincipen bör de personuppgiftsansvariga även överväga huruvida och med vilka intervaller de bör ge de registrerade tydliga påminnelser om integritetspolicyn/integritetsmeddelandet och var dessa finns.

Förfaranden – format för tillhandahållande av information

33. I både artikel 13 och artikel 14 hänvisas till den personuppgiftsansvariges skyldighet att "*till den registrerade lämna information om följande …*". Det avgörande ordet här är "lämna". Detta innebär att den personuppgiftsansvarige måste vidta aktiva åtgärder för att ge informationen i fråga till den registrerade eller aktivt ledsaga den registrerade till den plats där informationen finns (t.ex. via en direktlänk, användning av QR-kod osv.). Den registrerade måste inte aktivt söka efter sådan information som omfattas av dessa artiklar bland annan information, såsom användarvillkor för en webbplats eller app. Detta illustreras i exemplet i punkt 11. Såsom anges i punkt 17 ovan rekommenderar artikel 29-arbetsgruppen att all den information som riktas till de registrerade också bör finnas tillgänglig på en enda plats eller i ett enda dokument (t.ex. i digital form på en webbplats eller i pappersformat) som de registrerade enkelt kan få tillgång till om de vill läsa hela informationen.

34. I dataskyddsförordningen finns en inneboende spänning mellan kraven att ge de registrerade omfattande information å ena sidan och att informationen ska ges i en koncis, klar och tydlig, begriplig och lätt tillgänglig form å andra sidan. Med tanke på de viktiga ansvars- och rättviseprinciperna måste de registrerade därför själva analysera arten, omständigheterna, omfattningen och sammanhanget gällande behandlingen av den behandling av personuppgifter som de gör och besluta, inom ramen för de rättsliga kraven i dataskyddsförordningen och med hänsyn tagen till rekommendationerna i dessa riktlinjer, framför allt punkt 36 nedan, hur man ska prioritera information som måste ges till de registrerade och vilka detaljnivåer och metoder som är lämpliga för att förmedla informationen.

En skiktad metod i den digitala miljön och skiktade integritetspolicyer/integritetsmeddelanden

35. I digitala sammanhang kan de personuppgiftsansvariga, med tanke på den omfattande information som ska ges till de registrerade, tillämpa en skiktad metod där de väljer att använda en kombination av metoder för att säkerställa öppenhet. Artikel 29-arbetsgruppen rekommenderar framför allt att skiktade integritetspolicyer/integritetsmeddelanden bör användas för att länka till de olika kategorier av information som måste ges till de registrerade, i stället för att visa all sådan information i ett och samma meddelande på skärmen. Syftet med detta är att undvika informationsutmattning. Skiktade integritetspolicyer/integritetsmeddelanden kan lösa konflikten mellan fullständighet och förståelse, framför allt genom att användarna direkt kan gå till det avsnitt i policyn/meddelandet som de vill läsa. Det bör noteras att skiktade integritetspolicyer/integritetsmeddelanden inte bara är en sammanställning av sidor där man måste klicka flera gånger för att få fram rätt information. Utformningen av och layouten på integritetspolicyns/integritetsmeddelandets första skikt bör vara sådan att de registrerade får en tydlig översikt över den information som finns om behandlingen av deras personuppgifter och var/hur de kan finna denna utförliga information bland

policyns/meddelandets olika skikt. Det är också viktigt att den information som ges i de olika skikten i ett skiktat meddelande är konsekvent och att inte motstridig information ges.

36. När det gäller innehållet i en personuppgiftsansvarigs första tillvägagångssätt för att informera registrerade inom ramen för en skiktad metod (dvs. den personuppgiftsansvariges första relation med den registrerade) eller innehållet i det första skiktet i skiktade integritetspolicyer/integritetsmeddelanden, rekommenderar artikel 29-arbetsgruppen att det första skiktet/förfarandet inkluderar uppgifter om behandlingens ändamål, den personuppgiftsansvariges identitet och en beskrivning av den registrerades rättigheter. (Vidare bör den registrerade direkt uppmärksammas på sådan information vid den tidpunkt då personuppgifterna samlas in, exempelvis genom att informationen visas när den registrerade fyller i ett onlineformulär.) Vikten av att ge denna information på förhand härrör särskilt från skäl 39[34]. De personuppgiftsansvariga måste kunna påvisa ansvarighet i fråga om vilken ytterligare information de beslutar att prioritera. Artikel 29-arbetsgruppen anser därför att även det första skiktet/förfarandet, utöver den information som anges ovan i denna punkt, bör innehålla information om den behandling som mest påverkar den registrerade och sådan behandling som skulle kunna komma som en överraskning för dem, i linje med rättviseprincipen. De registrerade bör därför kunna förstå av informationen i det första skiktet/förfarandet vilka konsekvenser behandlingen kommer att få för dem (se även punkt 10 ovan).

37. I ett digitalt sammanhang kan de personuppgiftsansvariga, bortsett från att ge skiktade integritetspolicyer/integritetsmeddelanden online, även välja att använda *ytterligare* öppenhetsverktyg (se fler exempel nedan) som ger skräddarsydd information till den registrerade vilken särskilt utformats för den registrerades position och de varor/tjänster som den registrerade använder. Det bör dock noteras att artikel 29-arbetsgruppen rekommenderar att skiktade integritetspolicyer/integritetsmeddelanden används, men att dock andra innovativa metoder får utvecklas och användas för att uppfylla öppenhetskraven.

Skiktad metod i en icke-digital miljö

38. En skiktad metod för att ge de registrerade öppenhetsinformation kan också användas i offline-/icke-digitala sammanhang (dvs. i den verkliga världen som vid direktkontakt och via telefon), där de personuppgiftsansvariga kan använda flera olika förfaranden för att förenkla tillhandahållandet av information. (Se även punkterna 33–37 och 39–40 i fråga om olika förfaranden för tillhandahållande av information.) Denna metod bör inte förväxlas med skiktade integritetspolicyer/integritetsmeddelanden. Oavsett vilka format som används i den skiktade metoden rekommenderar artikel 29-arbetsgruppen att den

[34] I skäl 39 anges följande i fråga om öppenhetsprincipen: "Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas."

viktigaste informationen (se punkt 36 ovan) generellt sett bör ges i det första skiktet (dvs. den personuppgiftsansvariges första relation med den registrerade). Denna information innefattar uppgifter om behandlingens ändamål, den personuppgiftsansvariges identitet och den registrerades rättigheter samt information om de största konsekvenserna av behandlingen eller behandling som skulle kunna komma som en överraskning för den registrerade. Om den första kontakten med en registrerad sker via telefon skulle sådan information exempelvis kunna ges under telefonsamtalet med den registrerade. En sammanfattning av den information som krävs enligt artiklarna 13 eller 14 skulle dessutom kunna ges på andra sätt, genom att en kopia av integritetspolicyn skickas per e-post och/eller att den registrerade får en länk till den personuppgiftsansvariges skiktade integritetspolicy/integritetsmeddelande online.

Push- och pullmeddelanden

39. Öppenhetsinformation kan också ges via push- och pullmeddelanden. I push-meddelanden ges öppenhetsinformation i realtid, medan pull-meddelanden innebär att tillgång till information ges på begäran, via Privacy Dashboards och "lär dig mer"-system. Dessa möjliggör en mer användarcentrerad öppenhetsrelaterad upplevelse för de registrerade.

- Via en sekretesspanel kan de registrerade ta del av "integritetsinformation" och ange sina integritetsrelaterade önskemål genom att tillåta eller förhindra att deras personuppgifter används på vissa sätt av tjänsten i fråga. Detta är särskilt användbart när de registrerade använder samma tjänst på flera olika utrustningar, eftersom det ger dem tillgång till och kontroll över sina personuppgifter oavsett hur de använder tjänsten. Genom att ge de registrerade möjlighet att anpassa sina sekretessinställningar via en sekretesspanel kan man lättare individanpassa integritetspolicyer/integritetsmeddelanden genom att endast ange de behandlingstyper som är relevanta för den registrerade. En sekretesspanel som integreras i en tjänsts befintliga struktur (t.ex. genom att samma utformning och benämningar används som i resten av tjänsten) är att föredra, eftersom tillgången och användningen av tjänsten då säkert blir intuitiv och användarna kan uppmuntras att ta del av informationen på samma sätt som andra delar av tjänsten. Detta kan vara ett effektivt sätt att visa att sekretessinformation är en nödvändig och integrerad del av en tjänst snarare än en lång lista med juridisk jargong.

- Ett realtidsmeddelande används för att ge särskild sekretessinformation på ad hoc-basis, när det är som viktigast att den registrerade läser informationen. Denna metod är användbar för att ge information vid flera olika tillfällen under insamlingen av personuppgifter; den gör det lättare att dela upp informationen i delar som de registrerade lätt kan tillgodogöra sig och innebär att man i mindre grad åberopar enskilda integritetspolicyer/integritetsmeddelanden som innehåller svårbegriplig information utan kontext. Om en registrerad köper en produkt online kan till exempel kortfattad information ges i popupmeddelanden i anslutning till relevanta textfält. I den information som ges bredvid ett fält där den registrerade

ska ange sitt telefonnummer skulle det exempelvis kunna förklaras att uppgifterna endast samlas in i kontaktsyfte gällande köpet och att de endast kommer att lämnas ut till leveranstjänsten.

Andra slags "lämpliga åtgärder"

40. Med tanke på den mycket stora tillgången till internet i EU och det faktum att de registrerade kan gå ut på nätet när som helst, från flera olika platser och med olika utrustning, såsom anges ovan, anser artikel 29-arbetsgruppen att elektroniska integritetspolicyer/integritetsmeddelanden är en "lämplig åtgärd" för att tillhandahålla öppenhetsinformation om de personuppgiftsansvariga digitalt/online. Baserat på omständigheterna kring insamlingen och behandlingen av uppgifterna kan dock en personuppgiftsansvarig även (eller alternativt där den personuppgiftsansvarige inte finns digitalt/online) använda andra förfaranden och format för att tillhandahålla informationen. Andra sätt för att ge information till de registrerade utifrån de olika personuppgiftsmiljöerna kan inkludera följande sätt som är tillämpliga på relevant miljö enligt nedan. Såsom tidigare nämnts kan de personuppgiftsansvariga tillämpa en skiktad metod om de väljer att använda en kombination av sådana metoder och samtidigt se till att den allra viktigaste informationen (se punkterna 36 och 38) alltid ges i det första förfarandet för att kommunicera med de registrerade.

a. Papperskopia/i pappersformat, till exempel när avtal ingås per post: skriftliga förklaringar, broschyrer, avtalsinformation, tecknade filmer, infografik eller flödesschema.
b. Telefon: muntliga förklaringar av en fysisk person för att möjliggöra interaktion och svar på frågor eller automatisk eller förinspelad information med alternativ att höra mer utförlig information.
c. Skärmlös smart teknik/IoT, till exempel wi-fI-spårningsanalys: symboler, QR-koder, röstaviseringar, skriftliga uppgifter i installationsanvisningar i pappersformat, videor i digitala installationsanvisningar, skriftlig information om smart utrustning, meddelanden per sms eller e-post, synliga paneler med information, allmän skyltning eller allmänna informationskampanjer.
d. Direktkontakt, till exempel svar på opinionsundersökningar, personlig registrering till en tjänst: muntliga förklaringar eller skriftliga förklaringar som ges i papperskopia eller i en skärmbild.
e. Realtid med CCTV-/drönarinspelning: synliga paneler med information, allmän skyltning, allmänna informationskampanjer eller tidnings-/medieannonser.

Information om profilering och automatiserat beslutsfattande

41. Information om förekomsten av automatiserat beslutsfattande, inbegripet profilering, enligt artikel 22.1 och 22.4, samt meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av behandlingen för den registrerade, utgör en del av den obligatoriska information som måste lämnas till den registrerade enligt artiklarna 13.2 f och 14.2 g. Artikel 29-arbetsgruppen har tagit fram riktlinjer om automatiserat

individuellt beslutsfattande och profilering[35] vilka det bör hänvisas till för ytterligare vägledning om hur öppenhet bör tillämpas just i fråga om profilering. Förutom de särskilda öppenhetskrav som tillämpas på automatiserat beslutsfattande enligt artiklarna 13.2 f och 14.2 g, bör det noteras att kommentarerna i dessa riktlinjer om vikten av att informera de registrerade om följderna av behandlingen av deras personuppgifter, och den allmänna principen att de registrerade inte bör bli överraskade av att deras personuppgifter behandlas, även är tillämpliga på profilering i allmänhet (inte bara på sådan profilering som avses i artikel 22[36]) som behandlingstyp[37].

Övriga frågor – risker, bestämmelser och skyddsåtgärder

42. I skäl 39 i dataskyddsförordningen hänvisas också till tillhandahållande av viss information som inte uttryckligen omfattas av artiklarna 13 och 14 (se utdrag från skälet i punkt 28 ovan). Hänvisningen i detta skäl om att de registrerade ska göras medvetna om risker, bestämmelser och skyddsåtgärder vad beträffar behandlingen av personuppgifter har koppling till en rad andra frågor. Bland dessa finns konsekvensbedömningar avseende dataskydd. Såsom artikel 29-arbetsgruppen anger i sina riktlinjer om konsekvensbedömning avseende dataskydd[38] får de personuppgiftsansvariga överväga att offentliggöra konsekvensbedömningen (eller delar av denna), för att skapa tillit till behandlingsåtgärderna och visa öppenhet och ansvarighet. De måste dock inte offentliggöra den. Vidare kan anslutning till en uppförandekod (såsom anges i artikel 40) användas för att visa öppenhet, eftersom uppförandekoder kan upprättas för att ange att dataskyddsförordningen tillämpas när det gäller rättvis och öppen behandling, information till allmänheten och de registrerade, information till och skydd av barn och så vidare.

43. En annan viktig fråga när det gäller öppenhet är inbyggt dataskydd och dataskydd som standard (enligt kraven i artikel 25). Dessa principer innebär att de personuppgiftsansvariga ska ta med uppgiftsskyddshänsyn i sina behandlingsåtgärder och system från grunden, snarare än att beakta uppgiftsskydd i sista stund för att följa kraven. I skäl 78 hänvisas till personuppgiftsansvariga som vidtar åtgärder som uppfyller kraven om inbyggt dataskydd och dataskydd som standard, inbegripet åtgärder som handlar om öppenhet om personuppgifternas syfte och behandling.

44. Frågan om gemensamt personuppgiftsansvariga handlar också om att göra de registrerade medvetna om risker, bestämmelser och skyddsåtgärder. Enligt artikel 26.1 måste gemensamt personuppgiftsansvariga fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen på ett öppet sätt, särskilt vad gäller den registrerades utövande av sina rättigheter och skyldigheterna att tillhandahålla den

[35] Riktlinjer om automatiserat beslutsfattande och profilering enligt förordning (EU) 2016/679).

[36] Detta är tillämpligt på beslutsfattande som enbart baseras på automatiserad behandling, inbegripet profilering, vilket har rättsverkan på den registrerade eller på ett liknande sätt påverkar honom eller henne väsentligt.

[37] I skäl 60, som är relevant i detta avseende, anges följande: ”Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering.”

[38] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av om behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning (EU) 2016/679,WP248 rev.1.

information som avses i artiklarna 13 och 14. Enligt artikel 26.2 ska det väsentliga innehållet i arrangemanget mellan de personuppgiftsansvariga göras tillgängligt för den registrerade. Med andra ord måste det vara fullständigt klart för den registrerade vilken personuppgiftsansvarig som han eller hon kan kontakta om han eller hon avser att utöva en eller flera av sina rättigheter enligt dataskyddsförordningen[39].

Information om ytterligare behandling

45. Både artikel 13 och artikel 14 innehåller en bestämmelse[40] om att en personuppgiftsansvarig måste informera den registrerade om den avser att behandla personuppgifterna för andra ändamål än det för vilket uppgifterna samlades in. I sådana fall ska den personuppgiftsansvarige "*före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2*". Genom dessa bestämmelser verkställs framför allt principen i artikel 5.1 b om att personuppgifter ska samlas in "för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är *oförenligt* med dessa ändamål"[41]. Enligt den andra delen av artikel 5.1 b ska ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 inte anses vara oförenlig med de ursprungliga ändamålen. Om personuppgifter behandlas ytterligare för ändamål som är *förenliga* med de ursprungliga ändamålen (se artikel 6.4[42]) är artiklarna 13.3 och 14.4 tillämpliga. Kraven i dessa artiklar om att en registrerad måste informeras om ytterligare behandling stöder ståndpunkten i dataskyddsförordningen att en registrerad rimligen kan förvänta sig vid tidpunkten för inhämtandet av personuppgifter och i samband med detta att en uppgiftsbehandling för detta ändamål kan komma att ske[43]. Med andra ord bör en registrerad inte bli överraskad över det ändamål för vilket personuppgifterna behandlas.

46. I den mån som artiklarna 13.3 och 14.4 avser tillhandahållande av "*ytterligare relevant information enligt punkt 2*" kan de vid första anblicken tolkas så att de ger ett visst utrymme för den personuppgiftsansvarige att bedöma i vilken utsträckning och vilken särskild kategori av information i den relevanta punkten 2 (dvs. artiklarna 13.2 eller 14.2 enligt vad som är tillämpligt) som bör tillhandahållas den registrerade. (I skäl 61 betecknas detta som "*annan nödvändig information*".) Standardregeln är dock att all sådan information som

[39] I artikel 26.3 anges det att den registrerade får utöva sina rättigheter enligt dataskyddsförordningen med avseende på och emot var och en av de personuppgiftsansvariga, oavsett formerna för det arrangemang som avses i punkt 26.1.

[40] I artiklarna 13.3 och 14.4, som är identiska.

[41] Se t.ex. skälen 47, 50, 61, 156 och 158 samt artiklarna 6.4 och 89.

[42] I artikel 6.4 anges, på ett icke-uttömmande sätt, de faktorer som ska beaktas för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in, nämligen kopplingen mellan ändamålen, det sammanhang inom vilket personuppgifterna har samlats in, personuppgifternas art (särskilt huruvida särskilda kategorier av personuppgifter eller personuppgifter om fällande domar i brottmål och överträdelser behandlas), eventuella konsekvenser för de registrerade när det gäller den planerade ytterligare behandlingen och förekomsten av lämpliga skyddsåtgärder.

[43] Skälen 47 och 50.

anges i nämnda delpunkt bör ges till den registrerade förutom om en eller flera kategorier av informationen inte finns eller inte är tillämpliga.

47. Artikel 29-arbetsgruppen rekommenderar att de personuppgiftsansvariga, för att säkerställa öppenhet, rättvisa och ansvar, bör överväga att i sina integritetspolicyer/integritetsmeddelanden informera de registrerade om den förenlighetsanalys som görs enligt artikel 6.4[44], i fall där en annan rättslig grund än samtycke eller nationell rätt/EU-rätt åberopas för det nya ändamålet med behandlingen. (Det vill säga en förklaring av hur behandlingen för det eller de andra ändamålen är förenlig med det ursprungliga ändamålet.) Skälet till detta är att de registrerade ska få möjlighet att bedöma förenligheten av den ytterligare behandlingen och de skyddsåtgärder som vidtas samt besluta huruvida de ska utöva sina rättigheter, till exempel rätten till begränsning av behandlingen eller rätten att invända mot behandling[45]. I fall där de personuppgiftsansvariga väljer att inte ta med sådan information i sina integritetspolicyer/integritetsmeddelanden, rekommenderar artikel 29-arbetsgruppen att de klargör för de registrerade att de kan erhålla informationen på begäran.

48. Frågan om tidpunkt är kopplad till den registrerades utövande av sina rättigheter. Såsom betonas ovan är tillhandahållande av information i god tid en viktig del i öppenhetskraven enligt artiklarna 13 och 14 och har nära anknytning till begreppet rättvis behandling. Information som rör *ytterligare behandling* måste ges ”före denna ytterligare behandling”. Artikel 29-arbetsgruppen anser att en rimlig tid bör gå mellan underrättelsen och behandlingens början i stället för att behandlingen inleds direkt efter att den registrerade underrättats. På så sätt kan de registrerade utnyttja de praktiska fördelarna med öppenhetsprincipen, genom att de får en verklig möjlighet att överväga (och eventuellt utöva sina rättigheter med avseende på) den ytterligare behandlingen. Vad som är en rimlig tid kommer att bero på omständigheterna i det särskilda fallet. Rättviseprincipen innebär att ju mer inkräktande (eller mindre väntad) den ytterligare behandlingen är, ju längre bör perioden vara. På samma sätt innebär ansvarsprincipen att de personuppgiftsansvariga bör kunna visa på vilket sätt deras val av tidpunkt för tillhandahållandet av denna information är motiverad sett till omständigheterna och på vilket sätt tidpunkten på det hela taget är rättvis för de registrerade. (Se även tidigare kommentarer i fråga om fastställande av rimliga tidsramar i punkterna 30–32 ovan.)

<u>Visualiseringsverktyg</u>

49. Vad som är viktigt är att öppenhetsprincipen i dataskyddsförordningen inte enbart ska verkställas genom språklig kommunikation (oavsett muntlig eller skriftlig). Enligt dataskyddsförordningen ska visualiseringsverktyg användas där så är lämpligt (framför allt symboler, certifieringsmekanismer samt sigill och märkningar för dataskydd). Enligt skäl

[44] Se även skäl 50.

[45] Såsom anges i skäl 63 kommer en registrerad på så sätt att kunna utöva rätten till tillgång, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig.

58[46] är det särskilt viktigt att sådan information som riktar sig till allmänheten eller till de registrerade finns att tillgå online[47].

Symboler

50. Enligt skäl 60 får information tillhandahållas till de registrerade "kombinerad" med standardiserade symboler, vilket därmed möjliggör en flerskiktsstrategi. Symboler bör dock inte rent av ersätta sådan information som är nödvändig för de registrerades utövande av sina rättigheter, och de bör inte heller användas som ett substitut för att den personuppgiftsansvarige ska fullgöra sina skyldigheter enligt artiklarna 13 och 14. Enligt artikel 12.7 får sådana symboler användas på följande sätt:

> *"Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara."*

51. Det som anges i artikel 12.7, nämligen "*Om sådana symboler visas elektroniskt ska de vara maskinläsbara*", innebär att det kan finnas situationer då symboler inte avser elektronisk visning[48], till exempel symboler för fysiskt pappersarbete, IoT-utrustning eller IoT-produktförpackning, meddelanden på offentliga platser om wi-fi-spårning, QR-koder och meddelanden via CCTV.

52. Det framgår tydligt att syftet med symboler är att öka öppenheten gentemot de registrerade genom att eventuellt minska behovet av stora mängder skriftlig information till dem. Användbarheten av symboler för att delge de registrerade sådan information som avses i artiklarna 13 och 14 på ett ändamålsenligt sätt är dock beroende av att det finns standardiserade symboler/bilder som används överallt och erkänns i hela EU som stenografi för sådan information. I detta avseende ger dataskyddsförordningen kommissionen ansvaret att ta fram en kod för symboler, men i slutändan är det Europeiska dataskyddsstyrelsen som, antingen på kommissionens begäran eller självmant, får avge ett

---

[46] "Denna information kan ges elektroniskt, exempelvis på en webbplats, när den riktas till allmänheten. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet."

[47] De personuppgiftsansvariga bör i detta avseende ta hänsyn till registrerade med synnedsättning (t.ex. personer med röd-grön färgblindhet).

[48] I dataskyddsförordningen ges ingen definition av "maskinläsbara" men i skäl 21 i direktiv 2013/37/EU definieras "maskinläsbart format" på följande sätt:

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

yttrande om sådana symboler till kommissionen[49]. Artikel 29-arbetsgruppen anser att en kod för symboler bör tas fram utifrån en evidensbaserad strategi i linje med skäl 166 och att omfattande forskning måste göras, före sådan standardisering, i samarbete med industrin och allmänheten i fråga om ändamålsenligheten med symboler i detta avseende.

Certifieringsmekanismer, sigill och märkningar

53. Förutom standardiserade symboler föreskrivs i dataskyddsförordningen (artikel 42) även användning av certifieringsmekanismer för dataskydd samt sigill och märkningar för dataskydd som syftar till att visa att de personuppgiftsansvarigas eller personuppgiftsbiträdenas behandling är förenlig med dataskyddsförordningen och öka insynen för de registrerade[50]. Artikel 29-arbetsgruppen kommer att utfärda riktlinjer om certifieringsmekanismer i sinom tid.

Utövande av de registrerades rättigheter

54. Öppenhet innebär tre skyldigheter för de registrerade vad beträffar de registrerades rättigheter enligt dataskyddsförordningen[51]:

- Att informera de registrerade om deras rättigheter[52] (enligt kraven i artiklarna 13.2 b och 14.2 c).
- Att iaktta öppenhetsprincipen (dvs. i fråga om kommunikationens kvalitet enligt artikel 12.1) vid kommunikation med de registrerade om deras rättigheter enligt artiklarna 15–22 och artikel 34.
- Att underlätta utövandet av de registrerades rättigheter i enlighet med artiklarna 15–22.

55. Kraven i dataskyddsförordningen när det gäller utövandet av dessa rättigheter och den typ av information som krävs syftar till att de registrerade ska få *en väsentlig möjlighet* att hävda sina rättigheter och ställa de personuppgiftsansvariga till svars för behandlingen av deras personuppgifter. I skäl 59 betonas att förfaranden bör fastställas "*som gör det lättare för registrerade att utöva sina rättigheter*" och att den personuppgiftsansvarige även bör

[49] Enligt artikel 12.8 ska kommissionen ges befogenhet "att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler". Skäl 166 (som handlar om delegerade akter från kommissionen i allmänhet) ges i upplysningssyfte och anger att kommissionen måste genomföra lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. Europeiska dataskyddsstyrelsen har dock också en viktig rådgivande roll när det gäller standardisering av symboler, eftersom det i artikel 70.1 r anges att den ska avge ett yttrande till kommissionen om symboler, på eget initiativ eller på kommissionens begäran i förekommande fall.

[50] Se hänvisningen i skäl 100.

[51] Enligt avsnittet "Insyn och villkor" i dataskyddsförordningen om kapitlet "Den registrerades rättigheter" (kapitel III, avsnitt 1, artikel 12).

[52] Rätt till tillgång, rättelse, radering och begränsning av behandling, rätt att invända mot behandling och rätt till dataportabilitet.

"*tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt*". Det förfarande som en personuppgiftsansvarig fastställer för att de registrerade ska kunna utöva sina rättigheter bör vara lämpligt sett till omfattningen och typen av det förhållande och den interaktion som finns mellan den personuppgiftsansvarige och den registrerade. En personuppgiftsansvarig kan därför vilja fastställa ett eller flera olika förfaranden för utövandet av rättigheter vilka återspeglar de olika sätt på vilka de registrerade interagerar med den personuppgiftsansvarige.

Exempel

En vårdleverantör använder sig av ett elektroniskt formulär på sin webbplats och pappersformulär i vårdklinikernas receptioner, för att underlätta åtkomstförfrågningar rörande personuppgifter såväl online som personligen. Vårdleverantören erbjuder dessa förfaranden men godtar fortfarande förfrågningar som ingetts på annat sätt (t.ex. per brev och via e-post) och tillhandahåller en särskild kontaktpunkt (som man kan få åtkomst till via e-post och telefon) för att de registrerade ska kunna utöva sina rättigheter.

<u>Undantag från skyldigheten att lämna information</u>

Undantag till artikel 13

56. Undantag till den personuppgiftsansvariges skyldigheter enligt artikel 13 kan endast göras i fall där personuppgifterna har inhämtats direkt från den registrerade "*om och i den mån den registrerade redan förfogar över informationen*"[53]. Ansvarsprincipen innebär att de personuppgiftsansvariga måste visa (och dokumentera) vilken information de registrerade redan har, hur och när de fick den samt att inga ändringar har gjorts i informationen vilka skulle göra den inaktuell. Användningen av frasen "i den mån" i artikel 13.4 klargör att den personuppgiftsansvarige, även om den registrerade redan har fått vissa kategorier av den information som anges i artikel 13, fortfarande är skyldig att komplettera informationen för att säkerställa att den registrerade nu har all den information som avses i artikel 13.1 och 13.2. Nedan följer ett exempel på bästa praxis när det gäller den begränsade tolkning som bör göras av undantaget i artikel 13.4.

Exempel

En privatperson tecknar sig för en e-posttjänst och får all den information som krävs i artikel 13.1 och 13.2 vid tecknandet. Sex månader senare aktiverar den registrerade en snabbmeddelandefunktion som är kopplad till tjänsten via e-postleverantören och anger sitt telefonnummer för detta syfte. E-postleverantören ger den registrerade en

[53] Artikel 13.4.

del av den information som krävs enligt artikel 13.1 och 13.2 om behandling av telefonnummer (t.ex. ändamål och rättslig grund för behandling, mottagare och lagringstid) men inte annan information som den registrerade fick sex månader tidigare och som inte har ändrats sedan dess (t.ex. identitet och kontaktuppgifter för den personuppgiftsansvarige och dataskyddsombudet, information om den registrerades rättigheter och rätten att inge klagomål till relevant tillsynsmyndighet). Enligt bästa praxis bör dock all information ges igen till den registrerade, men den registrerade bör också med lätthet kunna se vilken information som är ny. Den nya behandlingen med anledning av snabbmeddelandetjänsten kan påverka den registrerade på ett sådant sätt att han eller hon skulle behöva utöva en rättighet som han eller hon glömt bort, eftersom information om denna gavs sex månader tidigare. Genom att den registrerade får all information igen blir det lättare att säkerställa att den registrerade fortfarande är välinformerad om hur personuppgifterna används och om sina rättigheter.

Undantag till artikel 14

57. Till artikel 14 finns många fler undantag till den personuppgiftsansvariges informationsskyldighet i fall där personuppgifter inte har erhållits från den registrerade. Dessa undantag bör som en allmän regel tolkas och tillämpas på ett snävt sätt. Bortsett från sådana situationer där den registrerade redan förfogar över informationen i fråga (artikel 14.5 a) ges även följande undantag i artikel 14.5:

- Tillhandahållandet av sådan information är omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, eller fall där det skulle göra det omöjligt att uppfylla eller avsevärt försvåra uppfyllandet av målen.
- Erhållande eller utlämnande av personuppgifter föreskrivs genom EU-rätten eller nationell rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen.
- Tystnadsplikt (inbegripet andra lagstadgade sekretessförpliktelser) enligt nationell rätt eller EU-rätt innebär att personuppgifterna måste förbli konfidentiella.

Visar sig vara omöjligt, oproportionell ansträngning och avsevärt försvårande av uppfyllandet av målen

58. I artikel 14.5 b anges tre olika situationer där skyldigheten att tillhandahålla sådan information som avses i artikel 14.1, 14.2 och 14.4 upphävs:

(i) Där det visar sig vara omöjligt (särskilt för behandling för arkivändamål, vetenskapliga/historiska forskningsändamål eller statistiska ändamål).

(ii) Där det skulle medföra en oproportionell ansträngning (särskilt när det gäller behandling för arkivändamål, vetenskapliga/historiska forskningsändamål eller statistiska ändamål).

(iii) Där tillhandahållandet av informationen enligt artikel 14.1 skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen.

"Visar sig vara omöjligt"

59. Den situation där det "visar sig vara omöjligt" enligt artikel 14.5 b att tillhandahålla informationen är en "allt eller inget"-situation, eftersom något antingen är omöjligt eller inte; det finns inga grader av omöjlighet. Om en personuppgiftsansvarig avser att åberopa detta undantag måste den därför visa vilka faktorer som faktiskt *hindrar den* från att ge informationen i fråga till de registrerade. Om de faktorer som orsakade denna "omöjlighet" inte längre föreligger efter en viss tid och det blir möjligt att tillhandahålla de registrerade informationen, bör den personuppgiftsansvarige göra detta utan dröjsmål. I praktiken kommer det att finnas mycket få situationer där en personuppgiftsansvarig kan visa att det faktiskt är omöjligt att tillhandahålla informationen till de registrerade. Detta visas i följande exempel.

Exempel

En registrerad tecknar sig för en abonnemangstjänst på nätet som man betalar för i efterskott. Efter registreringen inhämtar den personuppgiftsansvarige kredituppgifter om den registrerade från ett kreditupplysningsföretag för att avgöra om tjänsten ska tillhandahållas eller inte. Den personuppgiftsansvarige har som regel att informera registrerade om att kredituppgifterna har inhämtats inom tre månader, i enlighet med artikel 14.3 a. Den registrerades adress och telefonnummer finns dock inte i de allmänna registren (den registrerade bor i själva verket utomlands). Den registrerade angav aldrig någon e-postadress när han eller hon registrerade sig för tjänsten alternativt en felaktig e-postadress. Den personuppgiftsansvarige inser att det inte finns några möjligheter att ta direktkontakt med den registrerade. I detta fall kan dock den personuppgiftsansvarige informera om att kreditupplysning har tagits via sin webbplats, innan registreringen sker. Det skulle vara omöjligt att ge information enligt artikel 14 i detta fall.

Omöjlighet att meddela uppgifternas källa

60. I skäl 61 anges följande: "*Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.*" Kravet att de registrerade ska få information om personuppgifternas källa kan endast upphävas då detta är omöjligt eftersom samtliga personuppgifter för en och samma registrerad person inte kan hämtas från en viss källa. Detta krav kan inte upphävas enbart eftersom en personuppgiftsansvarig har upprättat en databas med personuppgifter för flera registrerade utifrån mer än en källa, om det är möjligt (om än tidskrävande eller mödosamt) att fastställa

den källa från vilken samtliga personuppgifter för de registrerade har hämtats. Med tanke på kraven om inbyggt dataskydd och dataskydd som standard[54] bör öppenhetsmekanismer integreras i behandlingssystemen från början, så att alla källor till personuppgifter som mottagits av en organisation kan spåras och spåras tillbaka till källan när som helst under uppgiftsbehandlingen (se punkt 43 ovan).

Oproportionell ansträngning

61. Enligt artikel 14.5 b kan "oproportionell ansträngning" också vara tillämpligt, precis som "visar sig vara omöjligt", särskilt för behandling "*för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1*". I skäl 62 hänvisas även till fall där det skulle medföra oproportionella ansträngningar att tillhandahålla den registrerade informationen, och vidare anges att antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder bör beaktas i detta avseende. Med tanke på den tonvikt som läggs i skäl 62 och artikel 14.5 b vid arkiv- och forskningsändamål och statistiska ändamål när det gäller tillämpningen av detta undantag, anser artikel 29-arbetsgruppen att undantaget inte bör åberopas *rutinmässigt* av de personuppgiftsansvariga som inte behandlar personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Artikel 29-arbetsgruppen betonar att villkoren i artikel 89.1 fortfarande måste följas och att tillhandahållandet av informationen måste medföra en oproportionell ansträngning, i fall där behandling görs för dessa ändamål.

62. Vid fastställande av vad som kan utgöra antingen en omöjlighet eller en oproportionell ansträngning enligt artikel 14.5 b är det viktigt att det inte finns några liknande undantag enligt artikel 13 (i fall där personuppgifter inhämtas från den registrerade). Den enda skillnaden mellan den situation som avses i artikel 13 respektive artikel 14 är att personuppgifter inte inhämtas från den registrerade i den sistnämnda artikeln. Omöjlighet eller oproportionell ansträngning uppstår därmed vanligtvis vid omständigheter som inte är tillämpliga om personuppgifterna inhämtas från den registrerade. Omöjligheten eller den oproportionella ansträngningen måste med andra ord ha direkt koppling till det faktum att personuppgifterna har erhållits från annat håll än från den registrerade.

Exempel

Ett stort storstadssjukhus kräver att alla patienter för dagliga ingrepp, längre sjukhusvistelser och läkarbesök ska fylla i ett patientinformationsformulär där uppgifter om två "närmast anhöriga" ska anges. Med tanke på det mycket stora antal patienter som passerar sjukhuset varje dag skulle det medföra en oproportionell ansträngning från sjukhusets sida att varje dag tillhandahålla den information som krävs enligt artikel 14 till alla de personer som har angetts som "närmast anhöriga" på de formulär som patienterna har fyllt i.

[54] Artikel 25.

63. De faktorer som avses i skäl 62 ovan (antal registrerade, uppgifternas ålder och lämpliga skyddsåtgärder) kan visa vilka slags problem som medför att en personuppgiftsansvarig måste göra en oproportionell ansträngning för att delge de registrerade informationen enligt artikel 14.

Exempel

Historieforskare som försöker spåra släktlinjer via efternamn får indirekt ett stort dataset avseende 20 000 registrerade. Datasetet inhämtades dock för 50 år sedan, har inte uppdaterats sedan dess och innehåller inga kontaktuppgifter. Med tanke på datasetets storlek och framför allt uppgifternas ålder skulle det medföra en oproportionell ansträngning för forskarna att försöka spåra var och en av de registrerade för att ge dem information enligt artikel 14.

64. Om en personuppgiftsansvarig avser att åberopa undantaget i artikel 14.5 b eftersom det skulle medföra en oproportionell ansträngning att tillhandahålla informationen, bör den personuppgiftsansvarige bedöma den ansträngning som krävs för att tillhandahålla informationen till den registrerade och jämföra den med konsekvenserna och effekterna för den registrerade om informationen inte tillhandahålls. Den personuppgiftsansvarige bör dokumentera denna bedömning i överensstämmelse med sina ansvarsskyldigheter. Enligt artikel 14.5 b måste den personuppgiftsansvarige i ett sådant fall vidta lämpliga åtgärder för att skydda den registrerades rättigheter, friheter och berättigade intressen. Detta gäller även om en personuppgiftsansvarig kommer fram till att det visar sig vara omöjligt att tillhandahålla informationen eller att det sannolikt kommer att göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen. En lämplig åtgärd, såsom anges i artikel 14.5 b, som de personuppgiftsansvariga alltid måste vidta är att göra uppgifterna tillgängliga för allmänheten. De kan göra detta på flera olika sätt, till exempel genom att offentliggöra informationen på sin webbplats eller genom att aktivt utannonsera informationen i en tidning eller på affischer i sina lokaler. Andra åtgärder som kan vara lämpliga, förutom att göra informationen tillgänglig för allmänheten, beror på omständigheterna kring behandlingen men kan inbegripa följande: att genomföra en konsekvensbedömning avseende dataskydd, att använda sig av pseudonymisering av uppgifterna, att minimera antalet insamlade uppgifter och lagringstiden samt att vidta tekniska och organisatoriska åtgärder för att garantera en hög säkerhetsnivå. Dessutom kan det finnas situationer där en personuppgiftsansvarig behandlar personuppgifter som inte innebär att den registrerade måste identifieras (t.ex. pseudonymiserade uppgifter). I sådana fall kan artikel 11.1 också vara relevant eftersom det där anges att den personuppgiftsansvarige inte ska vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade enbart för att följa dataskyddsförordningen.

Avsevärt försvårande av uppfyllandet av målen

65. Artikel 14.5 b avser en sista situation där en personuppgiftsansvarigs tillhandahållande av information till den registrerade enligt artikel 14.1 kan göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med behandlingen. För att kunna åberopa detta undantag måste de personuppgiftsansvariga visa att målen med behandlingen skulle gå förlorade om enbart sådan information som avses i artikel 14.1 skulle tillhandahållas. Ett åberopande av denna aspekt av artikel 14.5 b förutsätter i synnerhet att uppgifterna behandlas med respekt för samtliga principer i artikel 5 och framför allt att behandlingen av personuppgifterna under alla omständigheter är rättvis och baseras på en rättslig grund.

Exempel

Bank A omfattas av ett tvingande krav enligt penningtvättslagstiftningen att rapportera misstänkt aktivitet på bankkonton vid banken till relevant ekobrottsmyndighet. Bank A får information från bank B (som finns i en annan medlemsstat) att en kontoinnehavare har begärt överföring av pengar till ett annat konto vid bank A, vilket verkar misstänksamt. Bank A överlämnar uppgifterna om kontoinnehavaren och den misstänkta verksamheten till relevant ekobrottsmyndighet. Enligt gällande penningtvättslagstiftning är det straffbart för en anmälande bank att "tipsa" kontoinnehavaren om att han eller hon kan vara föremål för en utredning. Artikel 14.5 b är tillämplig i en sådan situation eftersom det avsevärt skulle försvåra uppfyllandet av målen med lagstiftningen, däribland förebyggande av "tipsning", om den registrerade (kontoinnehavaren hos bank A) skulle få information enligt artikel 14 om behandling av hans eller hennes personuppgifter som mottagits av bank B. Allmän information bör dock ges till samtliga kontoinnehavare hos bank A när de öppnar ett konto om att deras personuppgifter får behandlas i syfte att bekämpa penningtvätt.

Erhållande eller utlämnande av uppgifter föreskrivs uttryckligen i lag

66. Enligt artikel 14.5 c gäller inte informationskraven i artikel 14.1, 14.2 och 14.4 i den mån som erhållandet eller utlämnandet av uppgifter "*uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av*". Detta undantag görs beroende på den lag som fastställer "*lämpliga åtgärder för att skydda den registrerades berättigade intressen*". En sådan lag måste direkt avse den personuppgiftsansvarige som bör omfattas av ett obligatoriskt krav i fråga om erhållande eller utlämnande. De personuppgiftsansvariga måste därför kunna visa på vilket sätt lagen i fråga är tillämplig för dem och att de därmed måste antingen erhålla eller utlämna personuppgifterna i fråga enligt denna. Det är upp till unionen eller medlemsstaterna att utforma lagen på ett sådant sätt att den fastställer "*lämpliga åtgärder för att skydda den registrerades berättigade intressen*". Därför bör den personuppgiftsansvarige säkerställa (och kunna visa) att erhållandet eller utlämnandet av personuppgifter överensstämmer med dessa åtgärder. Vidare bör den personuppgiftsansvarige klargöra för de registrerade att personuppgifter erhålls och utlämnas i enlighet med lagen i fråga, om inget rättsligt förbud finns som hindrar den personuppgiftsansvarige från att göra detta. Detta är i linje med skäl 41 i

dataskyddsförordningen där det anges att en rättslig grund eller lagstiftningsåtgärd bör vara tydlig och precis och att dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna. Artikel 14.5 c tillämpas dock inte om den personuppgiftsansvarige måste erhålla personuppgifter *direkt från den registrerade*, i vilket fall artikel 13 är tillämplig. I detta fall är den personuppgiftsansvarige enligt dataskyddsförordningen endast befriad från skyldigheten att tillhandahålla den registrerade information om behandlingen genom undantaget i artikel 13.4 (dvs. om och i den mån den registrerade redan förfogar över informationen). Såsom anges i punkt 68 nedan får medlemsstaterna också införa nationella lagstiftningsåtgärder, i enlighet med artikel 23, om ytterligare särskilda begränsningar av rätten till insyn enligt artikel 12 och rätten till information enligt artiklarna 13 och 14.

Exempel

En skattemyndighet omfattas av ett tvingande krav enligt nationell rätt att erhålla uppgifter från arbetsgivare om arbetstagarnas löner. Personuppgifterna erhålls inte från de registrerade och därför omfattas skattemyndigheten av kraven i artikel 14. Eftersom skattemyndighetens erhållande av personuppgifter från arbetsgivarna uttryckligen fastställs i lag är informationskraven i artikel 14 inte tillämpliga på skattemyndigheten i detta fall.

Konfidentialitet på grund av sekretessförpliktelser

67. I artikel 14.5 d ges ett undantag till informationskravet för personuppgiftsansvariga i fall där "*personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser*". Om en personuppgiftsansvarig avser att åberopa detta undantag måste den personuppgiftsansvarige kunna visa att undantaget kan tillämpas och att tystnadsplikten direkt avser den personuppgiftsansvarige, vilket gör att all sådan information som anges i artikel 14.1, 14.2 och 14.4 inte kan tillhandahållas den registrerade.

Exempel

En läkare (personuppgiftsansvarig) har tystnadsplikt gällande patienters medicinska uppgifter. En patient (gentemot vilken tystnadsplikten gäller) ger läkaren hälsoinformation om en genetisk sjukdom, som några av hennes nära släktingar också har. Patienten ger även läkaren vissa personuppgifter om de släktingar (de registrerade) som har samma sjukdom. Läkaren måste inte ge släktingarna sådan information som avses i artikel 14, eftersom undantaget i artikel 14.5 d är tillämpligt. Om läkaren skulle ge information enligt artikel 14 till släktingarna skulle han bryta mot sin tystnadsplikt gentemot patienten.

Begränsningar av de registrerades rättigheter

68. I artikel 23 anges att medlemsstaterna (eller EU) ska lagstifta om ytterligare begränsningar av tillämpningsområdet för de registrerades rättigheter i fråga om insyn och de registrerades materiella rättigheter[55] om sådana åtgärder vidtas med respekt för andemeningen i de grundläggande rättigheterna och friheterna och är nödvändiga och proportionella för att säkerställa de tio mål som anges i artikel 23.1 a–j. Om sådana nationella åtgärder antingen inskränker de registrerades särskilda rättigheter eller de allmänna insynsskyldigheterna, som i annat fall skulle tillämpas på personuppgiftsansvariga enligt dataskyddsförordningen, bör de personuppgiftsansvariga kunna visa på vilket sätt den nationella bestämmelsen är tillämplig. Såsom anges i artikel 23.2 h måste lagstiftningsåtgärden inbegripa en bestämmelse om de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen. I linje med detta och med rättviseprincipen bör de personuppgiftsansvariga också informera de registrerade om att de åberopar (eller kommer att åberopa, om en särskild rättighet utövas av de registrerade) en sådan *nationell lagstiftningsbegränsning* av de registrerades rättigheter eller av öppenhetsskyldigheten, såvida detta inte skulle inverka menligt på lagstiftningsbegränsningen. Öppenhet innebär därför att de personuppgiftsansvariga i förhand ska ge information till de registrerade om deras rättigheter och eventuella begränsningar av dessa som de personuppgiftsansvariga avser att åberopa, så att de registrerade inte blir överraskade över en påstådd begränsning av en särskild rättighet när de försöker utöva denna gentemot de personuppgiftsansvariga. När det gäller pseudonymisering och uppgiftsminimering, och i den mån som de personuppgiftsansvariga avser att åberopa artikel 11 i dataskyddsförordningen, har artikel 29-arbetsgruppen tidigare slagit fast i yttrande 3/2017[56] att artikel 11 i dataskyddsförordningen ”bör tolkas som ett sätt att genomföra en 'genuin' minimering av uppgifter, men utan att hindra utövandet av den registrerades rättigheter” och att utövandet av dessa rättigheter ”ska möjliggöras med hjälp av 'kompletterande uppgifter' som tillhandahållits av den registrerade”.

69. Enligt artikel 85 måste medlemsstaterna dessutom i lag förena rätten till integritet med yttrande- och informationsfriheten. Detta innebär bland annat att medlemsstaterna ska införa lämpliga undantag eller avvikelser från vissa bestämmelser i dataskyddsförordningen (inklusive från öppenhetskraven i artiklarna 12–14) för sådan behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, om dessa är nödvändiga för att förena de båda rättigheterna.

Öppenhet och personuppgiftsincidenter

[55] Såsom anges i artiklarna 12–22 och 34, samt i artikel 5 i den mån som bestämmelserna överensstämmer med de rättigheter och skyldigheter som anges i artiklarna 12–22.

[56] Yttrande 03/2017 om behandling av personuppgifter inom ramen för samverkande intelligenta transportsystem (C-ITS), punkt 4.2.

70. Artikel 29-arbetsgruppen har tagit fram särskilda riktlinjer om personuppgiftsincidenter[57], men enligt dessa måste en personuppgiftsansvarigs skyldigheter att anmäla personuppgiftsincidenter till den registrerade vara helt förenliga med öppenhetskraven i artikel 12[58]. En anmälan av personuppgiftsincidenter måste uppfylla samma krav, såsom anges ovan (framför allt kravet om ett klart och tydligt språk), som annan kommunikation med de registrerade om deras rättigheter eller vid förmedling av information enligt artiklarna 13 och 14.

[57] Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679), WP 250.

[58] Detta klargörs i artikel 12.1 som särskilt hänvisar till "[…] all kommunikation enligt artiklarna 15–22 **och 34** vilken avser behandling […]" [fetmarkering tillagd].

Bilaga
Information som måste tillhandahållas den registrerade enligt artiklarna 13 eller 14

Obligatoriska uppgifter	Åberopad artikel (om personuppgifterna insamlas direkt från den registrerade)	Åberopad artikel (om personuppgifterna inte insamlas direkt från den registrerade)	Artikel 29-arbetsgruppens kommentarer till informationskravet
Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.[59]	Artikel 13.1 a	Artikel 14.1 a	Dessa uppgifter bör göra det lätt att identifiera den personuppgiftsansvarige och företrädesvis möjliggöra olika typer av kommunikation med den personuppgiftsansvarige (t.ex. telefonnummer, e-postadress och postadress).
Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall	Artikel 13.1 b	Artikel 14.1 b	Se artikel 29-arbetsgruppens riktlinjer om dataskyddsombud[60]
Ändamålen med behandlingen och dess rättsliga grund	Artikel 13.1 c	Artikel 14.1 c	Förutom ändamålen med den behandling som personuppgifterna är avsedda för, måste den relevanta rättsliga grund som åberopas enligt artikel 6 anges. Vid särskilda kategorier av personuppgifter bör relevant bestämmelse i artikel 9 (och i tillämpliga fall den EU-lag eller nationella lag enligt vilken uppgifterna behandlas) anges. Enligt artikel 10 måste den EU-lag eller nationella lag som är tillämplig på behandlingen anges om personuppgifterna rör fällande domar i brottmål och överträdelser

[59] Enligt definitionen i artikel 4.17 i dataskyddsförordningen (och enligt hänvisningen i skäl 80) avses med "företrädare" en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt dataskyddsförordningen. Denna skyldighet gäller i fall där de personuppgiftsansvariga eller personuppgiftsbiträdena inte är etablerade i EU men behandlar personuppgifter för registrerade som befinner sig i unionen och där behandlingen har anknytning till utbjudande av varor eller tjänster till sådana registrerade i EU eller övervakning av deras beteende.

[60] Riktlinjer om dataskyddsombud, WP 243 rev.01, senast granskade och antagna den 5 april 2017.

			eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1.
Om berättigade intressen (artikel 6.1 f) utgör den rättsliga grunden för behandlingen avses den personuppgiftsansvariges eller en tredje parts berättigade intressen.	Artikel 13.1 d	Artikel 14.2 b	Det särskilda intresset i fråga måste fastställas till förmån för den registrerade. Som bästa praxis kan den personuppgiftsansvarige även ge den registrerade uppgifter om den *bedömning* som måste göras för att artikel 6.1 f ska kunna åberopas som laglig grund för behandlingen, innan den registrerades personuppgifter inhämtas. För att undvika informationströtthet kan detta tas med i skiktade integritetspolicyer/integritetsmeddelanden (se punkt 35). Artikel 29-arbetsgruppen anser att det alltid tydligt bör framgå av informationen till de registrerade att de kan få information om bedömningen på begäran. Detta är nödvändigt för att säkerställa faktisk insyn i fall där de registrerade tvivlar på att bedömningen har gjorts på riktigt sätt eller om de vill inge ett klagomål till en tillsynsmyndighet.
De kategorier av personuppgifter som behandlingen gäller	Ej tillämpligt	Artikel 14.1 d	Denna information krävs i en sådan situation som avses i artikel 14, eftersom personuppgifterna inte har erhållits från den registrerade, som därför inte känner till vilka kategorier av personuppgifter den personuppgiftsansvarige har erhållit.
Vilka mottagare[61] (eller kategorier av mottagare) som erhåller personuppgifterna	Artikel 13.1 e	Artikel 14.1 e	I artikel 4.9 definieras begreppet "mottagare" som "*en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas*, ***vare sig det är en tredje part eller inte***"

[61] Enligt definitionen i artikel 4.9 i dataskyddsförordningen och hänvisningen i skäl 31.

			[fetmarkering tillagd]. En mottagare måste därför inte vara en tredje part. Andra personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden till vilka uppgifter överförs eller lämnas ut omfattas därmed av begreppet "mottagare", och information om sådana mottagare bör ges utöver information om tredjepartsmottagare. Namnen på de faktiska mottagarna av personuppgifterna eller kategorierna av mottagare måste anges. Enligt rättviseprincipen måste de personuppgiftsansvariga ge sådan information om mottagarna som är mest relevant för de registrerade. I praktiken är detta mottagarnas namn, så att de registrerade vet exakt vem som har deras personuppgifter. Om de personuppgiftsansvariga väljer att ange kategorier av mottagare 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 belägenhet.
Uppgifter om överföring till tredjeländer med tillhörande fakta och uppgifter om relevanta skyddsåtgärder[62] (däribland förekomsten eller	Artikel 13.1 f	Artikel 14.1 f	Uppgifter bör ges om relevant artikel i dataskyddsförordningen för överföring och tillhörande mekanism (t.ex. beslut om adekvat skyddsnivå enligt artikel 45/bindande företagsbestämmelser enligt artikel 47/standardiserade dataskyddsbestämmelser enligt artikel 46.2/undantag och

[62] Såsom anges i artikel 46.2 och 46.3.

avsaknaden av ett beslut om adekvat skyddsnivå[63]) och om hur man kan få en kopia av dessa eller var dessa har ställts till förfogande.			skyddsåtgärder enligt artikel 49 osv.). Vidare bör information ges om var och hur man kan få tillgång till eller erhålla handlingen i fråga, t.ex. genom att länka till den använda mekanismen. Enligt rättviseprincipen bör den information som ges om överföring till tredjeländer vara så meningsfull som möjligt för de registrerade. Detta innebär generellt sett att tredjeländernas namn ska anges.
Lagringstiden (eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period)	Artikel 13.2 a	Artikel 14.2 a	Detta har samband med kravet om uppgiftsminimering i artikel 5.1 c och om lagringsbegränsning i artikel 5.1 e. Lagringstiden (eller de kriterier som används för att fastställa denna) kan styras av faktorer som lagstadgade krav eller riktlinjer inom branschen, men den bör anges på ett sådant sätt att den registrerade, utifrån sin egen situation, kan bedöma lagringstiden för särskilda uppgifter/ändamål. Det räcker inte att den personuppgiftsansvarige generellt anger att personuppgifterna bevaras så länge som är nödvändigt för de berättigade ändamålen med behandlingen. I relevanta fall bör olika lagringstider anges för olika kategorier av personuppgifter och/eller olika behandlingsändamål, inklusive arkiveringstid i lämpliga fall.
Den registrerades rättigheter till • tillgång, • rättelse,	Artikel 13.2 b	Artikel 14.2 c	Denna information bör vara specifik för behandlingen i fråga och inbegripa en sammanfattning av vad rättigheten innebär, hur den registrerade kan gå till väga för att

[63] I enlighet med artikel 45.

• radering, • begränsning av behandling, • invändning mot behandling och • dataportabilitet.			utöva den och vilka begränsningar som rättigheten eventuellt omfattas av (se punkt 68 ovan). I synnerhet måste rätten att invända mot behandling uttryckligen meddelas den registrerade senast vid den första kommunikationen med den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information[64]. När det gäller rätten till dataportabilitet, se artikel 29-arbetsgruppens riktlinjer om rätten till dataportabilitet[65].
I fall där behandlingen baseras på samtycke (eller uttryckligt samtycke), rätten att när som helst återkalla sitt samtycke	Artikel 13.2 c	Artikel 14.2 d	Denna information bör inbegripa uppgifter om hur samtycke kan återkallas, med hänsyn till det faktum att det ska vara lika lätt för den registrerade att återkalla som att ge sitt samtycke[66].
Rätten att inge klagomål till en tillsynsmyndighet	Artikel 13.2 d	Artikel 14.2 e	I denna information bör det förklaras att den registrerade, i enlighet med artikel 77, har rätt att inge klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där en påstådd överträdelse av dataskyddsförordningen har gjorts.
Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt	Artikel 13.2 e	Ej tillämpligt	I ett anställningsavtal kan det till exempel vara ett avtalsenligt krav att tillhandahålla viss information till en nuvarande eller potentiell arbetsgivare. På onlineformulär bör det tydligt anges vilka fält som måste fyllas i eller inte, och vilka följderna kan

[64] Artikel 21.4 och skäl 70 (som är tillämpligt vid direktmarknadsföring).

[65] Riktlinjer om rätten till dataportabilitet, WP 242 rev.01, senast reviderade och antagna den 5 april 2017.

[66] Artikel 7.3.

huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.			komma att bli om sådana fält inte fylls i.
Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor	Ej tillämpligt	Artikel 14.2 f	Uppgifternas specifika källa bör anges om detta inte är omöjligt – se punkt 60 för mer information. Om den specifika källan inte har något namn bör bland annat följande uppgifter anges: källornas art (dvs. om de är offentliga eller privata) och typen av organisation/bransch/sektor.
Förekomsten av automatiserat beslutsfattande, inbegripet profilering och, i tillämpliga fall, meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade	Artikel 13.2 f	Artikel 14.2 g	Se artikel 29-arbetsgruppens riktlinjer om automatiserat beslutsfattande och profilering[67].

[67] Riktlinjer om automatiserat beslutsfattande och profilering enligt förordning (EU) 2016/679).