



Artikel 29-gruppen
Riktlinjer om samtycke enligt förordning (EU) 2016/679

Antagna den 28 november 2017

Senast granskade och antagna den 10 april 2018

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ
BEHANDLINGEN AV PERSONUPPGIFTER

som inrättats genom 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,

HAR ANTAGIT FÖLJANDE RIKTLINJER:

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

För sekretariatet svarar direktorat C (Grundläggande rättigheter och unionsmedborgarskap) vid Europeiska kommissionens generaldirektorat för rättsliga frågor, B-1049 Bryssel, Belgien, Kontor MO-59 02/013.

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

Innehåll

1.	Inledning	3
2.	Samtycke enligt artikel 4.11 i GDPR	4
3.	Delar av giltigt samtycke.....	5
3.1.	Fritt/frivilligt samtycke	5
3.1.1.	Maktobalans	6
3.1.2.	Villkor.....	8
3.1.3.	Granularitet	10
3.1.4.	Problem	11
3.2.	Specifikt	12
3.3.	Informerat	13
3.3.1.	Minimikrav avseende innehåll för att samtycke ska vara "informerat"	13
3.3.2.	Informationsskyldighet.....	14
3.4.	Otvetydig viljeyttring	16
4.	Erhållande av uttryckligt samtycke.....	18
5.	Ytterligare villkor för erhållande av giltigt samtycke.....	21
5.1.	Bevis på samtycke.....	21
5.2.	Återkallande av samtycke.....	22
6.	Interaktion mellan samtycke och andra lagliga grunder i artikel 6 i GDPR	24
7.	Särskilda problemområden i GDPR	24
7.1.	Barn (artikel 8)	24
7.1.1.	Informationssamhällets tjänster	25
7.1.2.	Erbjuds direkt till barn	26
7.1.3.	Ålder	26
7.1.4.	Barns samtycke och föräldraansvar.....	27
7.2.	Vetenskaplig forskning	29
7.3.	De registrerades rättigheter	31
8.	Erhållet samtycke enligt direktiv 95/46/EG.....	31

1. Inledning

I dessa riktlinjer görs en grundlig analys av begreppet samtycke i förordning (EU) 2016/679, den allmänna dataskyddsförordningen (nedan kallad *GDPR*). Begreppet samtycke såsom det används i dataskyddsdirektivet (nedan kallat *direktiv 95/46/EG*) och direktivet om integritet och elektronisk kommunikation har förändrats. I GDPR görs ett ytterligare förtydligande och en specificering av kraven för erhållande och uppvisande av giltigt samtycke. I dessa riktlinjer läggs fokus på dessa förändringar genom praktisk vägledning för att säkerställa förenlighet med GDPR och med utgångspunkt i yttrande 15/2011 om definitionen av begreppet "samtycke". De personuppgiftsansvariga är skyldiga att finna nya vägar för att hitta nya lösningar inom lagens ramar och bättre stödja skyddet av registrerades personuppgifter och intressen.

Samtycke förblir en av de sex lagliga grunderna för behandling av personuppgifter, såsom anges i artikel 6 i GDPR¹. Vid inledandet av verksamhet som medför behandling av personuppgifter måste en personuppgiftsansvarig alltid ta sig tid och fundera över vilken som är den lämpliga rättsliga grunden för den avsedda behandlingen.

Generellt sett kan samtycke enbart vara den lämpliga rättsliga grunden om den registrerade erbjuds kontroll och får en genuin valmöjlighet att godta eller vägra godta de villkor som ges eller att vägra godta dem utan problem. När den personuppgiftsansvarige ber om samtycke måste han eller hon bedöma huruvida samtliga villkor kommer att uppfyllas för erhållandet av giltigt samtycke. Om samtycke erhålls helt i linje med GDPR är samtycke ett verktyg som ger de registrerade kontroll över huruvida deras personuppgifter kommer att behandlas. I annat fall blir de registrerades kontroll skenbar och samtycke kommer då att vara en ogiltig grund för behandling, vilket innebär att behandlingen blir olaglig².

Artikel 29-gruppens befintliga yttranden om samtycke³ är fortsatt relevanta, i de fall där de är förenliga med den nya rättsliga ramen, eftersom GDPR är en kodifiering av artikel 29-gruppens nuvarande riktlinjer och allmänna goda praxis och eftersom de viktigaste delarna av samtycke är desamma i GDPR. I detta dokument ersätter inte artikel 29-gruppen tidigare yttranden om särskilda frågor som rör bland annat hänvisning till samtycke enligt direktiv 95/46/EG. I stället vidareutvecklar och kompletterar artikel 29-gruppen dessa.

Såsom anges i yttrande 15/2011 om definitionen av begreppet "samtycke" bör uppmaningar till personer om att acceptera uppgiftsbehandling omfattas av strikta krav, eftersom det handlar om de registrerades grundläggande rättigheter och om att den personuppgiftsansvarige vill inleda en uppgiftsbehandling som skulle vara olaglig utan den registrerades samtycke⁴. Samtyckets avgörande roll betonas i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *EU-stadgan om de grundläggande rättigheterna*). Ett erhållet samtycke

¹ I artikel 9 i GDPR ges en lista över möjliga undantag till förbudet mot behandling av särskilda kategorier av uppgifter. Ett av undantagen är då den registrerade lämnar uttryckligt samtycke till användning av sådana uppgifter.

² Se även yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), s. 6–8, och/eller yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG (WP 217), s. 9, 10, 13 och 14.

³ Framför allt yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187).

⁴ Yttrande 15/2011, sidan om definitionen av begreppet "samtycke" (WP 187), s. 8.

innebär inte heller att man kan kringgå eller på något sätt förminska den personuppgiftsansvariges skyldigheter att iaktta behandlingsprinciperna i GDPR, särskilt artikel 5 i GDPR i fråga om korrekthet, nödvändighet och proportionalitet samt datakvalitet. Behandlingen av personuppgifter grundar sig på den registrerades samtycke, men detta innebär inte att uppgifter som inte är nödvändiga för ett särskilt ändamål får behandlas, vilket i grund och botten skulle vara oskäligt⁵.

Artikel 29-gruppen är samtidigt medveten om den översyn som görs av direktivet om integritet och elektronisk kommunikation (2002/58/EG). Begreppet samtycke i förslaget till förordning om integritet och elektronisk kommunikation hänger fortfarande samman med begreppet samtycke i GDPR⁶. Organisationer behöver sannolikt samtycke enligt instrumentet för integritet och elektronisk kommunikation för merparten marknadsföringsmeddelanden på nätet eller marknadsföringssamtal och webbaserade spårningsverktyg, inklusive genom användning av kakor eller appar eller annan programvara. Artikel 29-gruppen har redan utfärdat rekommendationer och gett vägledning till EU-lagstiftaren när det gäller förslaget till förordning om integritet och elektronisk kommunikation⁷.

När det gäller det nuvarande direktivet om integritet och elektronisk kommunikation noterar artikel 29-gruppen att hänvisningar till det upphävda direktivet ska anses vara hänvisningar till GDPR⁸. Detta gäller även hänvisningar till samtycke i det nuvarande direktivet 2002/58/EG, eftersom förordningen om integritet och elektronisk kommunikation inte kommer att ha trätt i kraft den 25 maj 2018. Enligt artikel 95 i GDPR ska inga ytterligare förpliktelser föreläggas när det gäller behandling inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät, i den mån som särskilda skyldigheter för samma ändamål införs genom direktivet om integritet och elektronisk kommunikation. Artikel 29-arbetsgruppen noterar att kraven om samtycke enligt GDPR inte ska betraktas som någon ”ytterligare förpliktelse” utan snarare som förhandsvillkor för laglig behandling. Därför är GDPR:s villkor för erhållande av giltigt samtycke tillämpliga i situationer som omfattas av direktivet om integritet och elektronisk kommunikation.

2. Samtycke enligt artikel 4.11 i GDPR

I artikel 4.11 i GDPR definieras samtycke på följande sätt: *”varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.”*

⁵ Se även yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187) och artikel 5 i GDPR.

⁶ Enligt artikel 9 i den föreslagna förordningen om integritet och elektronisk kommunikation gäller den definition av och de villkor för samtycke som anges i artiklarna 4.11 och 7 i GDPR.

⁷ Se *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)* (ung. yttrande 3/2016 om utvärdering och översyn av direktivet om integritet och elektronisk kommunikation [ej översatt till svenska]) (WP 240).

⁸ Se artikel 94 i GDPR.

Grundbegreppet samtycke är detsamma som i direktiv 95/46/EG och samtycke är en av de rättsliga grunder som behandling av personuppgifter måste grundas på, enligt artikel 6 i GDPR⁹. Förutom den ändrade definitionen i artikel 4.11 innehåller GDPR ytterligare vägledning i artikel 7 samt i skälen 32, 33, 42 och 43 när det gäller hur den personuppgiftsansvarige måste agera för att iaktta samtyckeskravets viktigaste delar.

Det faktum att särskilda bestämmelser och skäl om återkallande av samtycke har tagits med bekräftar att samtycke bör vara ett återkalleligt beslut och att den registrerade fortsätter att ha en viss kontroll.

3. Delar av giltigt samtycke

Enligt artikel 4.11 i GDPR innebär samtycke av den registrerade varje slag av

- frivillig,
- specifik,
- informerad och
- otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

I nedanstående avsnitt görs en analys av i vilken utsträckning ordalydelsen i artikel 4.11 innebär att de personuppgiftsansvariga måste ändra sina begäranden/formulär avseende samtycke, för att säkerställa förenlighet med GDPR¹⁰.

3.1. Fritt/frivilligt samtycke¹¹

Delen ”fritt” innebär att de registrerade har kontroll och möjlighet att välja fritt. I GDPR anges den allmänna regeln att om de registrerade saknar möjlighet att välja fritt, känner sig tvingade att ge sitt samtycke eller kommer att få utstå negativa konsekvenser om de inte samtycker, kommer samtycket

⁹ I direktiv 95/46/EG definierades samtycke som ”*varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom*”, vilket måste ges på ett otvetydigt sätt för att personuppgifterna ska få behandlas (artikel 7 a i direktiv 95/46/EG). Se artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187) för exempel på lämpligheten av samtycke som rättslig grund. I detta yttrande gav artikel 29-gruppen vägledning för att särskilja fall där samtycke är en lämplig rättslig grund från de där grunden legitimt intresse (eventuellt med en *opt out*-lösning) är tillräcklig eller ett avtalsförhållande är att rekommendera. Se även artikel 29-gruppens yttrande 6/2014, punkt III.1.2, sidan 14 och följande sidor. Uttryckligt samtycke är också ett av undantagen till förbudet mot behandling av särskilda kategorier av uppgifter: se artikel 9 i GDPR.

¹⁰ För vägledning när det gäller pågående behandling som grundar sig på samtycke i direktiv 95/46/EG, se kapitel 7 i detta dokument och skäl 171 i GDPR.

¹¹ Artikel 29-gruppen har i flera yttranden undersökt samtyckets gränser i situationer där det inte kan ges frivilligt. Så gjorde artikel 29-gruppen framför allt i sitt yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), *Working Document on the processing of personal data relating to health in electronic health records* (ung. arbetsdokumentet om behandling av personuppgifter rörande hälsa i elektroniska patientjournaler) (WP 131), yttrande 8/2001 om behandling av personuppgifter i anställningsförhållanden (WP 48) och andra yttrandet 4/2009 om Internationella antidopningsbyråns (Wada) internationella standard för skydd av privatlivet och personuppgifter, om bestämmelser på området i Wadas internationella antidopningsregler och om andra frågor som gäller privatlivet i samband med Wadas och (nationella) antidopningsorganisationers bekämpning av dopning inom idrotten (WP 162).

att vara ogiltigt¹². Om samtycke ingår som en ej förhandlingsbar del av villkoren antas samtycket inte vara frivilligt. På samma sätt kommer samtycke inte anses vara frivilligt om de registrerade inte kan vägra eller ta tillbaka sitt samtycke utan problem¹³. Begreppet ojämlikhet mellan den personuppgiftsansvarige och den registrerade beaktas också i GDPR.

Vid bedömning av huruvida samtycke är frivilligt bör hänsyn även tas till den särskilda situation då samtycke förenas med ett avtal eller tillhandahållande av en tjänst såsom anges i artikel 7.4. Artikel 7.4 har avfattats på ett icke uttömmande sätt genom orden ”bland annat”, som innebär att det kan finnas en rad andra situationer som omfattas av bestämmelsen. Varje slags otillbörligt tryck eller påverkan på den registrerade (vilket kan te sig på flera olika sätt) som hindrar honom eller henne från att utöva sin fria vilja ska generellt sett innebära att samtycket blir ogiltigt.

[Exempel 1]

I en fotoredigeringsapp uppmanas användarna att ha GPS-lokaliseringen aktiverad för tjänsten. I appen informeras användarna även om att de insamlade uppgifterna kommer att användas för beteendestyrd nätannonsering. Vare sig geolokalisering eller beteendestyrd nätannonsering är nödvändigt för tillhandahållandet av fotoredigerings-tjänsten och går utöver tillhandahållandet av huvudtjänsten i fråga. Eftersom användarna inte kan använda appen utan att ge sitt samtycke till dessa ändamål, kan samtycket inte anses ha getts frivilligt.

3.1.1. Maktobalans

I skäl 43¹⁴ anges det tydligt att det är osannolikt att **offentliga myndigheter** kan hänvisa till samtycke till behandling, eftersom det ofta föreligger en tydlig maktobalans mellan den personuppgiftsansvarige och den registrerade när den personuppgiftsansvarige är en offentlig myndighet. Det är också tydligt i de flesta fall att den registrerade faktiskt inte kommer att ha något annat val än att godta den personuppgiftsansvariges behandling (behandlingsvillkor). Artikel 29-arbetsgruppen anser att det finns andra lagliga grunder som i princip är mer lämpliga för offentliga myndigheters verksamhet¹⁵.

Utan att det påverkar dessa allmänna överväganden är det inte helt uteslutet för offentliga myndigheter att använda sig av samtycke som en laglig grund för behandling av uppgifter enligt GDPR:s rättsliga ram. Följande exempel visar att samtycke kan vara lämpligt i vissa situationer:

[Exempel 2] En kommun planerar vägunderhållsarbeten. Eftersom vägarbetena kan störa trafiken under en lång tid ger kommunen medborgarna möjlighet att via en e-postlista få uppdateringar om arbetenas fortskridande och om förväntade förseningar. Kommunen klargör att medborgarna inte är skyldiga att delta och begär deras samtycke för att få använda e-postadresserna (enbart) för detta syfte. De medborgare som inte ger sitt samtycke kommer inte att gå miste om några av kommunens huvudtjänster eller möjligheten att utöva någon viss

¹² Se yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 12.

¹³ Se skälen 42 och 43 i GDPR och artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet ”samtycke”, antaget den 13 juli 2011 (WP 187), s. 12.

¹⁴ Skäl 43 i GDPR har följande lydelse: ”För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. [...]”

¹⁵ Se artikel 6 i GDPR, särskilt punkt 1 c och 1 e.

rättighet, så de kan fritt ge eller vägra ge sitt samtycke till att uppgifterna används på detta sätt. All information om vägarbetena kommer också att finnas på kommunens webbplats.

[Exempel 3] En privatperson som äger mark behöver vissa tillstånd dels från kommunen, dels från den provins som kommunen tillhör. Båda dessa offentliga organ kräver samma uppgifter för att utfärda sina tillstånd men de har inte åtkomst till varandras databaser. Därför begär de samma uppgifter och markägaren skickar sina personuppgifter till båda organen. Kommunen och provinsmyndigheten begär markägarens samtycke till att ärendena slås ihop, för att undvika dubbla förfaranden och dubbel korrespondens. Båda organen försäkrar att detta är frivilligt och att man kommer att fortsätta behandla tillståndsansökningarna separat, om markägaren beslutar att inte ge sitt samtycke till att uppgifterna slås ihop. Markägaren får fritt samtycka till att myndigheterna slår ihop ärendena.

[Exempel 4] En statlig skola begär elevernas samtycke för att få använda bilder på dem i en tryckt elevtidning. Samtycke i sådana situationer skulle vara en genuin valmöjlighet så länge som eleverna inte nekas utbildning eller tjänster. Eleverna kan utan problem vägra ge samtycke till att bilderna används¹⁶.

En maktobalans uppstår även på **sysselsättningsområdet**¹⁷. Med tanke på den beroendeställning som följer av ett anställningsförhållande är det osannolikt att den registrerade kan vägra ge sin arbetsgivare samtycke till behandling av personuppgifter utan att vara rädd för eller löpa verklig risk för negativa konsekvenser till följd av sin vägran. Det är osannolikt att en arbetstagare fritt skulle kunna svara på en begäran om samtycke från sin arbetsgivare för att denne till exempel ska få aktivera övervakningssystem som kameraövervakning på arbetsplatsen eller fylla i bedömningsformulär, utan att arbetstagaren känner sig tvingad att ge sitt samtycke¹⁸. Artikel 29-gruppen anser därför att det är problematiskt att arbetsgivare behandlar befintliga eller framtida anställdas personuppgifter baserat på samtycke, eftersom det är osannolikt att samtycket ges frivilligt. Vid sådan databehandling på arbetsplatsen kan och bör den lagliga grunden i de allra flesta fall inte utgöras av arbetstagarens samtycke (artikel 6.1 a) på grund av hur förhållandet mellan arbetsgivare och arbetstagare är beskaffat¹⁹.

Detta innebär dock inte att arbetsgivare aldrig får använda samtycke som en laglig grund för behandling av personuppgifter. Det kan finnas situationer där arbetsgivaren kan visa att samtycket faktiskt har getts frivilligt. Med tanke på maktobalansen mellan en arbetsgivare och personalen, kan arbetstagarna endast ge sitt fria samtycke i undantagsfall, när inga negativa konsekvenser kommer att uppstå oavsett om de ger sitt samtycke eller inte²⁰.

[Exempel 5]

¹⁶ Med statlig skola avses i detta exempel en statligt finansierad skola eller någon annan utbildningsinrättning som uppfyller kraven för en offentlig myndighet eller ett offentligt organ enligt nationell rätt.

¹⁷ Se även artikel 88 i GDPR, där behovet av skydd för arbetstagarnas särskilda intressen betonas och där en möjlighet för undantag i medlemsstaternas lagstiftning införs. Se även skäl 155.

¹⁸ Se yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), s. 12–14, *Opinion 8/2001 on the processing of personal data in the employment context* (ung. yttrande 8/2001 om behandling av personuppgifter i anställningsförhållanden) (WP 48), kapitel 10, arbetsdokumentet om övervakning av elektroniska kommunikationer på arbetsplatsen (WP 55), punkt 4.2, och yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen (WP 249), punkt 6.2.

¹⁹ Se yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen, s. 6–7.

²⁰ Se även yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen (WP 249), punkt 6.2.

En filmbesättning ska filma i en viss del av ett kontor. Arbetsgivaren ber alla de anställda som har sin plats i denna del att ge samtycke till att bli filmade, eftersom de kan komma med i bakgrunden i filmen. De som inte vill bli filmade straffas inte på något sätt för det men får i stället likvärdiga platser någon annanstans i byggnaden under det att filminspelningen pågår.

Maktobalans kan inte bara uppstå mellan myndigheter och arbetsgivare utan även i andra situationer. Såsom artikel 29-gruppen betonat i flera yttranden kan samtycke endast vara giltigt om den registrerade får möjlighet att välja fritt och om det inte finns någon risk för bedrägeri, trakasserier, tvång eller betydande negativa konsekvenser (t.ex. betydande tilläggskostnader) om inget samtycke ges. Samtycket anses inte ges fritt i fall där det finns något inslag av tvång, påtryckningar eller oförmåga att utöva fri vilja.

3.1.2. Villkor

Artikel 7.4 i GDPR²¹ har en avgörande betydelse när man ska bedöma huruvida samtycke lämnas frivilligt.

I artikel 7.4 i GDPR anges det bland annat att sådan paketering anses vara högst icke önskvärd då samtycke ges mot godtagande av vissa villkor eller då bestämmelserna i ett avtal eller en tjänst binds till en begäran om samtycke för behandling av personuppgifter som inte är nödvändig för genomförandet av avtalet eller tjänsten. Om samtycke lämnas i en sådan situation anses det inte ha lämnats frivilligt (skäl 43). Syftet med artikel 7.4 är att säkerställa att syftet med behandlingen av personuppgifterna inte är dolt eller har förenats med avtalsbestämmelserna för en tjänst för vilken personuppgifterna inte är nödvändiga. På så sätt säkerställer man genom GDPR att behandling av personuppgifter för vilken samtycke begärs inte direkt eller indirekt får ställas som krav för genomförandet av ett avtal. De båda lagliga grunderna för laglig behandling av personuppgifter, det vill säga samtycke och avtal, får inte slås ihop eller suddas ut.

Ett tvång om att samtycka till användning av personuppgifter utöver vad som är strikt nödvändigt begränsar de registrerades valmöjligheter och hindrar frivilligt samtycke. Eftersom dataskyddslagstiftningen syftar till att skydda de grundläggande rättigheterna är det viktigt att en individ har kontroll över sina personuppgifter, och det finns en stark presumtion att samtycke till behandling av personuppgifter som inte är nödvändig inte kan anses vara tvingande hänsyn i utbyte mot genomförandet av ett avtal eller tillhandahållandet av en tjänst.

Närhelst de personuppgiftsansvariga binder en begäran om samtycke till genomförandet av ett avtal riskerar de registrerade därför att bli nekade tjänster som de begärt om de inte vill ställa sina personuppgifter till förfogande för behandling.

²¹ Artikel 7.4 i GDPR: ”Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.” Se även skäl 43 i GDPR där följande anges: ”[...] Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.”

För att bedöma huruvida sådan paketering eller bindning föreligger är det viktigt att fastställa själva syftet med avtalet och vilka uppgifter som är nödvändiga för genomförandet av detta.

Enligt artikel 29-gruppens yttrande 6/2014 måste en strikt tolkning göras av begreppet ”nödvändig för att fullgöra ett avtal”. Behandlingen måste vara nödvändig för fullgörandet av avtalet med varje enskild registrerad person. Detta kan exempelvis inbegripa behandling av den registrerades adress, så att varor som köpts på nätet kan levereras, eller behandling av kontokortsuppgifter för att underlätta betalning. När det gäller anställningar kan denna grund till exempel möjliggöra behandling av löne- och bankkontouppgifter, så att löner kan utbetalas²². Det måste finnas en direkt och objektiv koppling mellan behandlingen av uppgifterna och syftet med genomförandet av avtalet.

Om en registeransvarig försöker behandla personuppgifter som i själva verket inte är nödvändiga för genomförandet av ett avtal, är samtycke inte den lämpliga lagliga grunden²³.

Artikel 7.4 är endast relevant om de begärda uppgifterna **inte** är nödvändiga för genomförandet av avtalet (inklusive tillhandahållandet av en tjänst) och om genomförandet av avtalet har gjorts beroende av samtycke till erhållandet av sådana uppgifter. Omvänt gäller att artikel 7.4 inte är tillämplig om behandlingen **är** nödvändig för genomförandet av avtalet (inklusive tillhandahållandet av en tjänst).

[Exempel 6]

En bank ber om kundernas samtycke till att tredje part använder deras betalningsuppgifter för direkt marknadsföring. Sådan behandling är inte nödvändig för att genomföra avtalet med kunden och tillhandahålla ordinarie bankkontotjänster. Samtycket kan inte lämnas frivilligt om kundens vägran att ge sitt samtycke till sådan behandling skulle leda till att kunden nekas banktjänster, får sitt bankkonto stängt eller, beroende på fallet i fråga, får en förhöjd avgift.

Lagstiftarens val att betona bland annat villkorlighet som en anledning att misstänka att frivilligt samtycke saknas visar att förekomsten av villkorlighet måste granskas noggrant. Begreppet ”största hänsyn” i artikel 7.4 vittnar om att den personuppgiftsansvarige måste iaktta särskild försiktighet när ett avtal (som skulle kunna inbegripa tillhandahållande av en tjänst) innehåller en begäran om samtycke till behandling av personuppgifter.

Eftersom ordalydelsen i artikel 7.4 är allmänt hållen kan det finnas ett mycket begränsat utrymme för fall där sådan villkorlighet inte skulle göra samtycket ogiltigt. Ordet ”antas” i skäl 43 visar dock tydligt att det är mycket sällsynt med sådana fall.

Bevisbördan i artikel 7.4 ligger hur som helst på den personuppgiftsansvarige²⁴. Denna särskilda bestämmelse återspeglar den allmänna ansvarsprincip som genomsyrar hela GDPR. När artikel 7.4

²² För ytterligare information och exempel, se yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, s. 16–17, vilket artikel 29-arbetsgruppen antog den 9 april 2014, (WP 217).

²³ Den lämpliga lagliga grunden skulle då kunna vara artikel 6.1 b (avtal).

²⁴ Se även artikel 7.1 i GDPR, där det anges att den personuppgiftsansvarige måste kunna visa att den registrerade har gett sitt frivilliga samtycke.

är tillämplig kommer det dock att vara svårare för den personuppgiftsansvarige att bevisa att samtycke lämnats frivilligt av den registrerade²⁵.

Den personuppgiftsansvarige skulle kunna hävda att organisationen erbjuder de registrerade en genuin valmöjlighet om de kan välja mellan en tjänst som inkluderar samtycke till användning av personuppgifter för andra ändamål och en likvärdig tjänst från samma personuppgiftsansvarige som inte inkluderar samtycke till användning av uppgifter för andra ändamål. Så länge som det finns en möjlighet att få avtalet genomfört eller den avtalade tjänsten tillhandahållen av den personuppgiftsansvarige utan att samtycka till att uppgifterna används för andra ändamål innebär detta att tjänsten inte längre är villkorlig. Båda tjänsterna måste dock vara helt likvärdiga.

Artikel 29-gruppen anser att samtycke inte kan anses ha lämnats frivilligt om en personuppgiftsansvarig hävdar att den registrerade kan välja mellan den personuppgiftsansvariges tjänst som inkluderar samtycke till användning av personuppgifter för andra ändamål och en likvärdig tjänst från en annan personuppgiftsansvarig. I ett sådant fall skulle valfriheten styras av vad andra marknadsaktörer gör och huruvida en viss registrerad person anser att den andra personuppgiftsansvariges tjänst är helt likvärdig. Dessutom skulle de personuppgiftsansvariga bli skyldiga att övervaka marknadsutvecklingen för att säkerställa samtyckets fortsatta giltighet för uppgiftsbehandlingen i fråga, eftersom en konkurrent kan ändra sina tjänster i ett senare skede. Detta argument innebär således att samtycket inte är förenligt med GDPR.

3.1.3. Granularitet

En tjänst kan inbegripa flera olika behandlingar för mer än ett ändamål. I sådana fall bör de registrerade fritt kunna välja vilket ändamål de godtar i stället för att tvingas samtycka till ett paket med flera ändamål med behandlingen. I vissa fall kan flera samtycken vara motiverade för att en tjänst ska få börja erbjudas enligt GDPR.

I skäl 43 klargörs det att samtycke inte anses vara frivilligt om processen/förfarandet för erhållandet av samtycke inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter (t.ex. endast för viss behandling och inte för annan), trots att detta är lämpligt i det enskilda fallet. I skäl 32 anges följande: *”Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjäna flera olika syften, bör samtycke ges för samtliga syften.”*

Valfrihet saknas om den personuppgiftsansvarige har bakat ihop flera olika syften med behandlingen och inte har försökt få separat samtycke för vart och ett av dessa. En sådan granularitet har ett nära samband med det faktum att samtycket måste vara specifikt, vilket behandlas i avsnitt 3.2 nedan. När uppgifter behandlas för flera olika ändamål kan villkoren för

²⁵ Införandet av denna punkt är i viss mån en kodifiering av artikel 29-gruppens befintliga riktlinjer. Såsom anges i yttrande 15/2011 kan det finnas en stark presumtion när den registrerade står i ett beroendeförhållande till den personuppgiftsansvarige – på grund av förhållandets natur eller på grund av särskilda omständigheter – att möjligheten till frivilligt samtycke är begränsad i sådana situationer (t.ex. i ett anställningsförhållande eller om insamlingen av uppgifterna sköts av en offentlig myndighet). När artikel 7.4 är tillämplig kommer det dock att vara svårare för den personuppgiftsansvarige att bevisa att samtycke lämnats frivilligt av den registrerade. Se yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 12–17.

giltigt samtycke uppfyllas genom granularitet, det vill säga särskiljande av syftena och erhållande av samtycke för vart och ett av dessa.

[Exempel 7]

I en och samma begäran ber en återförsäljare om sina kunders samtycke till att få använda deras personuppgifter och skicka reklam till dem via e-post samt även ge deras personuppgifter till andra företag inom koncernen. Ett sådant samtycke är inte granulärt eftersom det inte finns några separata samtycken för de olika syftena, och därför kommer inte samtycket att vara giltigt. I detta fall bör ett särskilt samtycke erhållas för att kontaktuppgifterna ska få skickas till affärspartnerna. Ett sådant särskilt samtycke kommer att anses vara giltigt för varje partner (se även avsnitt 3.3.1), vars identitet har uppgetts för den registrerade när samtycket erhålls, i den mån som samtycket skickas till dem för samma ändamål (i detta exempel: i marknadsföringssyfte).

3.1.4. Problem

Den personuppgiftsansvarige måste visa att den registrerade kan vägra eller ta tillbaka sitt samtycke utan problem (skäl 42). Den personuppgiftsansvarige måste till exempel bevisa att ett återkallande av samtycket inte medför några kostnader för den registrerade och därmed ingen tydlig nackdel för de som återkallar sitt samtycke.

Andra exempel på problem är bedrägeri, trakasserier, tvång eller betydande negativa konsekvenser om den registrerade inte samtycker. Den personuppgiftsansvarige bör kunna bevisa att den registrerade har haft en fri eller genuin valmöjlighet att samtycka eller inte samtycka och att den registrerade utan problem har kunnat återkalla samtycket.

Om en personuppgiftsansvarig kan visa att en tjänst inbegriper en möjlighet att återkalla samtycket utan negativa konsekvenser, till exempel utan att genomförandet av tjänsten försämrats till användarens nackdel, kan detta tjäna som bevis för att samtycket lämnats frivilligt. GDPR innebär inte att alla incitament utesluts, men det är den personuppgiftsansvariges skyldighet att visa att samtycket lämnades frivilligt under alla omständigheter.

[Exempel 8]

När en användare laddar ner en livsstilsapp begärs användarens samtycke till att appen ska få åtkomst till mobilens accelerometer. Detta är inte nödvändigt för att appen ska fungera men är användbart för den personuppgiftsansvarige som vill veta mer om användarens rörelse och aktivitetsnivåer. När användaren senare återkallar samtycket informeras hon om att appen nu bara fungerar i begränsad utsträckning. Detta är ett exempel på problem enligt skäl 42, vilket innebär att samtycket aldrig erhållits på ett giltigt sätt (och att den personuppgiftsansvarige därmed måste radera alla de uppgifter som samlats in på detta sätt om användarens rörelse).

[Exempel 9]

En registrerad börjar prenumerera på ett nyhetsbrev från en klädåterförsäljare med allmänna rabatter. Återförsäljaren ber om den registrerades samtycke för att få mer information om den registrerades shoppingpreferenser och skraddarsy erbjudanden till honom eller henne baserat på tidigare shoppinghistorik eller ett frågeformulär som är frivilligt att fylla i. När den registrerade sedan återkallar sitt samtycke får han eller hon återigen bara icke-personliga moderabatter. Detta utgör inte ett problem, eftersom endast det tillåtliga incitamentet tagits bort.

[Exempel 10]

En modetidning ger sina läsare möjlighet att köpa nya make up-produkter innan de lanseras för allmänheten.

Produkterna kommer att släppas för försäljning inom kort, men läsarna erbjuds en exklusiv förhandsvisning av dem. För att kunna ta del av denna förmån måste läsarna ange sin postadress och anmäla sig till tidningens e-postlista. Postadressen är nödvändig för frakten och e-postlistan används för att skicka reklamerbjudanden om produkter som kosmetika eller t-shirtar året runt.

Företaget förklarar att uppgifterna i e-postlistan endast kommer att användas av tidningen själv för att skicka produkter och pappersreklam och att de inte kommer att delas med något annat företag.

Om läsarna inte vill ange sin adress av denna anledning föreligger inget problem, eftersom de kommer att kunna få tillgång till produkterna ändå.

3.2. Specifikt

I artikel 6.1 a bekräftas att den registrerade måste ha lämnat sitt samtycke för "ett eller flera specifika" ändamål och att han eller hon har en valmöjlighet med avseende på vart och ett av dessa²⁶. Kravet att samtycket måste vara "*specifikt*" syftar till att säkerställa en viss användarkontroll och insyn för den registrerade. Detta krav har inte förändrats genom GDPR och är fortfarande nära kopplat till kravet om "informerat" samtycke. Samtidigt måste kravet tolkas i linje med kravet om "granularitet" för att "frivilligt" samtycke ska erhållas²⁷. Sammanfattningsvis måste den personuppgiftsansvarige tillämpa följande för att respektera delen om "specifikt" samtycke:

- (i) Specifiering av ändamål som ett skydd mot funktionsglidning.
- (ii) Granularitet vid begäranden om samtycke.
- (iii) Ett tydligt särskiljande av uppgifter som rör erhållet samtycke för uppgiftsbehandling från andra slags uppgifter.

Ad. (i): Enligt artikel 5.1 b i GDPR ska ett särskilt, uttryckligen angett och berättigat ändamål för den avsedda behandlingen alltid fastställas innan ett giltigt samtycke erhålls.²⁸ Kravet om ett specifikt samtycke i kombination med begreppet ändamålsbegränsningar i artikel 5.1 b fungerar som ett skydd mot att de ändamål för vilka uppgifterna behandlas gradvis utökas eller suddas ut, efter att den registrerade har samtyckt till den inledande insamlingen av uppgifterna. Denna företeelse, som även kallas för funktionsglidning, utgör en risk för de registrerade, eftersom det kan leda till att den personuppgiftsansvarige eller tredje part använder uppgifterna på ett oväntat sätt och att den registrerade förlorar sin kontroll över uppgifterna.

Om den personuppgiftsansvarige hänvisar till artikel 6.1 a måste de registrerade alltid ge sitt samtycke till ett specifikt behandlingssyfte²⁹. I linje med begreppet *ändamålsbegränsning* (se artikel 5.1 b och skäl 32) får samtycket avse flera olika behandlingar, så länge som dessa tjänar samma syfte. Särskilt samtycke kan givetvis endast erhållas när de registrerade har informerats om just de avsedda syftena med behandlingen av deras personuppgifter.

²⁶ Ytterligare vägledning om fastställande av "ändamål" ges i *Opinion 3/2013 on purpose limitation* (ung. yttrande 3/2013 om ändamålsbegränsning) (WP 203).

²⁷ Enligt skäl 43 i GDPR krävs separata samtycken för olika behandlingar av personuppgifter, närhelst så är lämpligt. Det bör ges möjlighet till granulärt samtycke för att de registrerade ska kunna ge separata samtycken för olika ändamål.

²⁸ Se *Opinion 3/2013 on purpose limitation* (artikel 29-gruppens yttrande 3/2013 om ändamålsbegränsning) (WP 203), s. 16: *Ett vagt eller allmänt syfte, till exempel bättre användarupplevelse, marknadsföringssyfte, it-säkerhetssyfte eller framtida forskning kommer därför generellt sett inte att uppfylla kriterierna för ett specifikt syfte.*

²⁹ Detta är i linje med artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), t.ex. på s. 17.

Utan hinder av bestämmelserna om syftenas förenlighet måste samtycket ges specifikt för ändamålet. De registrerade ska ge sitt samtycke i vetskap om att de har kontrollen och att deras uppgifter endast kommer att behandlas för de specifika ändamålen. Om en personuppgiftsansvarig behandlar uppgifter på grundval av samtycke och vill behandla uppgifterna även för ett annat ändamål, måste den personuppgiftsansvarige erhålla ytterligare samtycke för detta ändamål om det inte finns någon annan rättslig grund som bättre återspeglar situationen.

[Exempel 11] Ett kabel-tv-nätverk samlar in abonnenternas personuppgifter, grundat på deras samtycke, för att ge dem personliga förslag på nya filmer som de kan vara intresserade av baserat på deras tittarhistorik. Efter en tid beslutar tv-nätverket att låta tredje part skicka (eller visa) riktad reklam baserat på abonnenternas tittarhistorik. Eftersom detta är ett nytt ändamål krävs ett nytt samtycke.

Ad. (ii): Samtyckesmekanismerna får inte vara granulära enbart för att uppfylla frivillighetskravet utan även för att uppfylla kravet om ”särskilt” samtycke. Detta innebär att en personuppgiftsansvarig som begär samtycke för flera olika ändamål bör ge möjlighet till *opt-in* för respektive ändamål, så att användarna kan ge särskilt samtycke till specifika ändamål.

Ad. (iii): Avslutningsvis bör de personuppgiftsansvariga tillhandahålla särskild information tillsammans med varje separat samtyckesbegäran om de uppgifter som behandlas för respektive ändamål, för att göra de registrerade medvetna om vad de olika möjligheterna innebär. De registrerade får därför möjlighet att ge särskilt samtycke. Denna fråga överlappar kravet om att de personuppgiftsansvariga måste ge tydlig information, såsom beskrivs i punkt 3.3 nedan.

3.3. Informerat

Genom GDPR förstärks kravet att samtycke måste vara informerat. På grundval av artikel 5 i GDPR är öppenhetskravet en av de grundläggande principerna och har nära anknytning till principerna om korrekthet och laglighet. Det är nödvändigt att de registrerade får information innan de ger sitt samtycke för att de ska kunna fatta informerade beslut, förstå vad de går med på och bland annat utöva sin rätt att återkalla sitt samtycke. Om den personuppgiftsansvarige inte ger lättillgänglig information blir användarkontrollen skenbar och samtycke en ogiltig grund för behandling.

Konsekvensen av att inte uppfylla kraven om informerat samtycke är att samtycket blir ogiltigt och att den personuppgiftsansvarige kanske bryter mot artikel 6 i GDPR.

3.3.1. Minimikrav avseende innehåll för att samtycke ska vara ”informerat”

För att samtycke ska vara informerat måste den registrerade informeras om vissa delar som är nödvändiga som beslutsunderlag. Artikel 29-gruppen anser därför att åtminstone följande uppgifter krävs för erhållande av ett giltigt samtycke:

- (i) Den personuppgiftsansvariges identitet.³⁰
- (ii) Syftet med var och en av de behandlingar för vilka samtycke begärs³¹.

³⁰ Se även skäl 42 i GDPR: ”[...] För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. [...]”

³¹ Se skäl 42 i GDPR.

- (iii) Vilken (typ av) information som kommer att samlas in och användas.³²
- (iv) Förekomsten av rätten att återkalla samtycket³³.
- (v) Information om användningen av uppgifterna för automatiserat beslutsfattande i enlighet med artikel 22.2 c³⁴ i förekommande fall.
- (vi) De eventuella riskerna med överföring av personuppgifter i avsaknad av ett lämpligt beslut och lämpliga skyddsåtgärder, såsom anges i artikel 46³⁵.

När det gäller punkterna (i) och (iii) noterar artikel 29-gruppen att i ett fall där det erhållna samtycket ska åberopas av flera (gemensamt) personuppgiftsansvariga eller om uppgifterna ska överföras till eller behandlas av andra personuppgiftsansvariga som vill hänvisa till det ursprungliga samtycket, ska namnen på alla dessa organisationer anges. De personuppgiftsansvarigas namn måste inte anges för uppfyllandet av samtyckeskraven, men för att respektera artiklarna 13 och 14 i GDPR måste de personuppgiftsansvariga lämna en fullständig förteckning över mottagare eller kategorier av mottagare inklusive personuppgiftsbiträden. Avslutningsvis noterar artikel 29-gruppen att det, beroende på omständigheterna och sammanhanget i ett visst fall, kan behövas mer uppgifter för att den registrerade ska få fullständig inblick i den behandling som avses.

3.3.2. Informationsskyldighet

I GDPR fastställs det inte i vilken form uppgifterna ska lämnas för att kraven om informerat samtycke ska vara uppfyllda. Detta innebär att giltiga uppgifter får lämnas på olika sätt, till exempel skriftligen eller muntligen eller via röst- eller videosamtal. Genom GDPR införs dock flera krav om informerat samtycke, framför allt i artikel 7.2 och skäl 32. Detta leder till en högre standard när det gäller uppgifternas tydlighet och tillgänglighet.

När de personuppgiftsansvariga begär samtycke bör de se till att alltid använda ett klart och tydligt språk. Detta innebär att budskapet ska vara lättbegripligt för gemene man och inte bara för jurister. De personuppgiftsansvariga får inte använda långa integritetspolicyer som är svåra att förstå eller meddelanden som är fulla med juridisk jargong. Begäran om samtycke måste läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lättillgänglig form. Detta krav innebär i grund och botten att uppgifter som behövs för att fatta informerade beslut om huruvida samtycke ska lämnas inte får döljas i allmänna villkor³⁶.

En personuppgiftsansvarig måste se till att samtycke lämnas på grundval av information som gör att de registrerade lätt kan identifiera den personuppgiftsansvarige och förstå vad de går med på. Den personuppgiftsansvarige måste tydligt ange syftet med den uppgiftsbehandling för vilken samtycke krävs³⁷.

³² Se även artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), s. 19–20.

³³ Se artikel 7.3 i GDPR.

³⁴ Se även *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251) (ung. artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering med avseende på förordning (EU) 2016/679), punkt IV.B, sidan 20 och följande sidor (ej översatt till svenska).

³⁵ Enligt artikel 49.1 a måste särskild information ges om att sådana lämpliga skyddsåtgärder som avses i artikel 46 saknas, när uttryckligt samtycke begärs. Se även artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), s. 19.

³⁶ Förklaringen om samtycke måste kallas så. Fraser som "Jag förstår att ..." uppfyller inte kraven för ett tydligt språk.

³⁷ Se artiklarna 4.11 och 7.2 i GDPR.

Annan specifik vägledning om tillgängligheten har getts i artikel 29-gruppens riktlinjer om öppenhet. Om samtycke ska ges elektroniskt måste begäran vara tydlig och koncis. Skiktad och granulär information kan vara ett lämpligt sätt att respektera det dubbla kravet om exakthet och fullständighet å ena sidan och begriplighet å andra sidan.

De personuppgiftsansvariga måste bedöma vilken typ av målgrupp som ger personuppgifter till deras organisation. Om målgruppen till exempel inkluderar registrerade som är minderåriga förväntas den personuppgiftsansvarige se till att informationen är begriplig för minderåriga³⁸. Efter att ha identifierat målgruppen måste de personuppgiftsansvariga avgöra vilken information som de bör ge och därefter hur de ska lämna informationen till de registrerade.

I artikel 7.2 behandlas på förhand utformade skriftliga samtyckesförklaringar som också avser andra frågor. När samtycke begärs i ett avtal (i pappersformat) bör begäran om samtycke tydligt kunna särskiljas från de andra frågorna. Om pappersavtalet innehåller flera aspekter som inte rör samtycket till användning av personuppgifter bör samtycket hanteras på ett mycket tydligt sätt eller i ett separat dokument. Om samtycke begärs elektroniskt måste begäran också göras separat och på ett tydligt sätt. Den får inte bara ingå som en punkt i villkoren, såsom anges i skäl 32³⁹. När det gäller mobil utrustning med mindre skärmar eller fall där informationsutrymmet är begränsat kan informationen presenteras på ett skiktat sätt, där så är lämpligt, för att undvika onödiga störningar i användarupplevelse eller produktdesign.

En personuppgiftsansvarig som hänvisar till den registrerades samtycke måste också fullgöra de separata informationsskyldigheter som anges i artiklarna 13 och 14 för att respektera GDPR. Fullgörandet av informationsskyldigheterna och respekten för kravet om informerat samtycke kan i praktiken leda till ett integrerat synsätt i flera fall. Detta avsnitt har dock avfattats i vetskap om att ett giltigt ”informerat” samtycke kan föreligga, även om inte samtliga delar av artikel 13 och/eller artikel 14 nämns när samtycke begärs (detta bör dock självklart anges någon annanstans, exempelvis i ett företags integritetspolicy. Artikel 29-gruppen har utfärdat separata riktlinjer om öppenhetskravet.

[Exempel 12]

Företag X är en personuppgiftsansvarig som mottagit klagomål om att det är oklart för de registrerade vilka ändamål de samtycker till när det gäller behandlingen av deras personuppgifter. Företaget ser ett behov av att kontrollera att informationen i samtyckesbegäran är begriplig för de registrerade. X anordnar frivilliga testpaneler bestående av olika kategorier av kunder och låter dem ta del av nya uppdateringar av samtyckesinformationen innan den sprids externt. Testpanelen väljs med respekt för principen om oberoende och utifrån standarder som säkerställer ett representativt, opartiskt utfall. Panelen får ett frågeformulär där de anger vad de har förstått av informationen och hur de skulle poängsätta den i fråga om informationens begriplighet och relevans. Den personuppgiftsansvarige fortsätter sina tester fram tills panelen anger att

³⁸ Se även skäl 58 om begriplig information för barn.

³⁹ Se även skäl 42 och direktiv 93/13/EEG, framför allt artikel 5 (klart och begripligt formulerade villkor och vid tveksamhet att den för konsumenten mest gynnsamma tolkningen ska gälla) och artikel 6 (om oskäligen villkors ogiltighet och om att avtalet ska förbli gällande utan dessa villkor endast om det fortfarande är rimligt och att hela avtalet ska vara ogiltigt i annat fall).

informationen är begriplig. X avfattar en rapport om testet och bevarar denna för framtida referens. Detta är ett exempel på hur X kan bevisa att de registrerade fått tydlig information innan de samtyckte till X behandling av deras personuppgifter.

[Exempel 13]

Ett företag behandlar personuppgifter baserat på samtycke. Företaget använder sig av en skiktad integritetspolicy som inbegriper en begäran om samtycke. Företaget avslöjar alla grundläggande uppgifter om den personuppgiftsansvarige och den planerade behandlingen av personuppgifter⁴⁰. Företaget anger dock inte några kontaktuppgifter till sitt dataskyddsombud i policyns första informationsskikt. För att ha en giltig laglig grund i enlighet med artikel 6 erhöll den personuppgiftsansvarige ett giltigt "informerat" samtycke, även eftersom dataskyddsombudets kontaktuppgifter inte lämnades till den registrerade (i det första informationsskiktet), i enlighet med artiklarna 13.1 b eller 14.1 b i GDPR.

3.4. Otvetydig viljeyttring

Det framgår tydligt av GDPR att samtycke kräver ett utlåtande från den registrerade eller en tydlig bekräftelse, vilket innebär att samtycket alltid måste ges aktivt eller genom en förklaring. Det måste vara uppenbart att den registrerade har samtyckt till behandlingen i fråga.

Enligt artikel 2 h i direktiv 95/46/EG är samtycke en "viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom". Artikel 4.11 i GDPR bygger på denna definition och klargör att giltigt samtycke kräver en *otvetydig* viljeyttring genom ett *uttalande eller genom en entydig bekräftande handling*, i linje med artikel 29-gruppens tidigare riktlinjer.

En "entydig bekräftande handling" innebär att den registrerade måste ha utfört en medveten handling för att samtycka till behandlingen i fråga⁴¹. I skäl 32 ges ytterligare vägledning i detta avseende. Samtycke kan inhämtas genom en skriftlig eller (inspelad) muntlig förklaring, inklusive på elektronisk väg.

Kriteriet "skriftlig förklaring" uppfylls kanske bokstavligen bäst genom att se till att en registrerad person uttryckligen anger vad han eller hon går med på i ett brev eller e-postmeddelande till den personuppgiftsansvarige. Detta är dock sällan realistiskt. Skriftliga förklaringar kan vara utformade på flera olika sätt och vara olika omfattande för att uppfylla kraven i GDPR.

⁴⁰ När den personuppgiftsansvariges identitet eller syftet med behandlingen inte tydligt framgår av det första informationsskiktet i den skiktade integritetspolicy (utan i andra underordnade skikt), kommer det att bli svårt för den personuppgiftsansvarige att bevisa att den registrerade har lämnat informerat samtycke, om inte den personuppgiftsansvarige kan visa att den registrerade fick tillgång till sådan information innan han eller hon lämnade sitt samtycke.

⁴¹ Se bilaga 2, s. 20 och även s. 105–106 i arbetsdokumentet från kommissionens avdelningar (*Commission Staff Working Paper, Impact Assessment*; ej översatt till svenska): *Såsom anges i artikel 29-gruppens yttrande om samtycke förefaller det nödvändigt att klargöra att giltigt samtycke kräver mekanismer som gör att det inte råder några tvivel om den registrerades avsikt att samtycka, och att användning – i den digitala miljön – av standardalternativ som den registrerade måste ändra för att avvisa behandlingen ("tyst samtycke") i sig inte utgör otvetydigt samtycke. På så sätt skulle enskilda personer få större kontroll över sina egna personuppgifter, närhelst behandlingen baseras på deras samtycke. Detta skulle inte få några större konsekvenser för de personuppgiftsansvariga eftersom det enbart förtydligar och bättre förklarar konsekvenserna av det befintliga direktivet med avseende på villkoren för ett giltigt och meningsfullt samtycke från den registrerades sida. I den mån som "uttryckligt" samtycke – i stället för "otvetydigt" samtycke – skulle förtydliga villkoren för samtycke och samtyckets kvalitet och avsikten inte är att utöka antalet fall och situationer där (uttryckligt) samtycke bör användas som grund för behandlingen, förväntas inte denna åtgärd få några större konsekvenser för de personuppgiftsansvariga.*

Utan att det påverkar befintlig (nationell) avtalsrätt kan samtycke erhållas genom en inspelad muntlig förklaring. Vederbörlig hänsyn måste dock tas till den information som den registrerade får innan han eller hon lämnar sitt samtycke. Enligt GDPR är det inte tillåtet med på förhand ikryssade rutor. Tysthet eller inaktivitet från den registrerades sida samt enbart ett utnyttjande av en tjänst får inte betraktas som ett aktivt val.

[Exempel 14]

Vid installation av en programvara begär appen den registrerades samtycke för användning av icke-anonymiserade kashrapporter för att förbättra programvaran. Begäran om samtycke åtföljs av en skiktad integritetspolicy med nödvändig information. Genom att bocka i den frivilliga rutan "Jag samtycker" kan användaren göra en "entydig bekräftande handling" för att samtycka till behandlingen.

En personuppgiftsansvarig måste också vara medveten om att samtycke inte får erhållas genom att den registrerade godtar ett avtal eller allmänna villkor för en viss tjänst. Tyst godkännande av allmänna villkor får inte betraktas som en entydig bekräftande handling för samtycke till behandling av personuppgifter. Enligt GDPR får inte de personuppgiftsansvariga använda sig av på förhand ikryssade rutor eller *opt out*-alternativ som kräver en åtgärd från den registrerades sida för att ett avtal inte ska träda i kraft (t.ex. *opt out*-rutor)⁴².

Om samtycke ska ges på elektronisk begäran, får inte begäran om samtycke *onödigtvis* störa användningen av den tjänst som den avser⁴³. En aktiv bekräftande åtgärd genom vilken den registrerade lämnar sitt samtycke kan vara nödvändig när ett mindre kränkande eller störande tillvägagångssätt skulle leda till tvetydighet. Det kan därför vara nödvändigt att en begäran om samtycke stör användarupplevelsen i viss mån för att begäran ska bli ändamålsenlig.

De personuppgiftsansvariga får dock utveckla ett samtyckesflöde som passar just deras organisation inom ramen för kraven i GDPR. Fysiska åtgärder kan i detta avseende uppfylla kraven för en entydig bekräftande handling i enlighet med GDPR.

De personuppgiftsansvariga bör utveckla samtyckesmekanismer som är entydiga för de registrerade. De personuppgiftsansvariga måste undvika tvetydighet och säkerställa att den åtgärd genom vilken samtycke ges kan särskiljas från andra åtgärder. Att en registrerad helt enkelt fortsätter att använda en webbplats som tidigare, är därför inget agerande som visar på hans eller hennes vilja att samtycka till en viss behandling av personuppgifter.

[Exempel 15]

Att svajpa en rad på en skärm, vinka framför en smartkamera och snurra en smarttelefon medurs eller i en åtta kan vara olika sätt för att ange samtycke, så länge som tydlig information ges och det är tydligt att åtgärden i fråga innebär att man samtycker till en specifik begäran (t.ex. om man svajpar raden till vänster samtycker man till att X använder personuppgifterna för ändamål Y, och upprepar åtgärden för att bekräfta). Den

⁴² Se artikel 7.2. Se även artikel 29-gruppens arbetsdokument om erhållande av samtycke för kakor (*Working Document 02/2013 providing guidance on obtaining consent for cookies*) (WP 208), s. 3–6 (ej översatt till svenska).

⁴³ Se skäl 32 i GDPR.

personuppgiftsansvarige måste kunna bevisa att samtycket har erhållits på detta sätt och de registrerade måste kunna återkalla sitt samtycke lika lätt som de lämnat det.

[Exempel 16]

Att skrolla ner på eller svajpa genom en webbplats uppfyller inte kraven för en entydig bekräftande handling. Skälet till detta är att varningen om att ett fortsatt skrollande kommer att innebära samtycke kan vara svårt att särskilja och/eller kan missas när den registrerade snabbt skrollar igenom stora mängder text, och vidare är en sådan åtgärd inte tillräckligt otvetydig.

I digitala sammanhang kräver många tjänster personuppgifter för att de ska fungera, och därför får de registrerade multipla begäranden om samtycke som de dagligen måste svara på genom att klicka och svajpa. Detta kan resultera i en viss mån av ”klicktrötthet”; när en varning har dykt upp för många gånger minskar den faktiska varningseffekten för samtyckesmekanismen.

Detta leder till en situation där användarna inte längre läser förfrågningar om samtycke. Detta utgör en särskild risk för de registrerade, eftersom samtycke vanligtvis begärs för åtgärder som är i princip olagliga utan deras medgivande. I GDPR blir de personuppgiftsansvariga skyldiga att finna lösningar på detta problem.

En vanlig lösning inom internetvärlden är att internetanvändares samtycke erhålls via deras webbläsarinställningar. Sådana inställningar bör utvecklas i överensstämmelse med villkoren för giltigt samtycke i GDPR, så att samtycket blir granulärt för respektive ändamål och de personuppgiftsansvarigas namn anges i informationen och så vidare.

Samtycke måste hur som helst alltid erhållas innan den personuppgiftsansvarige påbörjar sin behandling av personuppgifter för vilket samtycke krävs. Artikel 29-gruppen har i tidigare yttranden konsekvent hävdat att samtycke bör ges innan personuppgifter behandlas⁴⁴. Det anges inte bokstavligen i artikel 4.11 i GDPR att samtycke måste ges före behandlingen, men detta är helt klart underförstått. Den inledande frasen i artikel 6.1 och ordalydelsen ”har lämnat” i artikel 6.1 a stöder denna tolkning. Den logiska följden av artikel 6 och skäl 40 är att en giltig laglig grund måste finnas innan personuppgifter börjar behandlas. Därför bör samtycke ges före detta. I princip kan det räcka att begära de registrerades samtycke en gång. De personuppgiftsansvariga måste dock erhålla nytt och specifikt samtycke om ändamålen med behandlingen av uppgifterna förändras efter att samtycket erhöles eller om ytterligare ändamål införs.

4. Erhållande av uttryckligt samtycke

Uttryckligt samtycke krävs i vissa situationer där allvarliga risker för dataskydd uppstår, det vill säga där det anses vara lämpligt att enskilda har omfattande kontroll över sina personuppgifter. Enligt GDPR är uttryckligt samtycke viktigt i artikel 9 om behandling av särskilda kategorier av personuppgifter, bestämmelserna om överföringar av personuppgifter till tredjeländer eller

⁴⁴ Artikel 29-gruppen har hela tiden stått fast vid denna ståndpunkt sedan antagandet av yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 30–31.

internationella organisationer vid avsaknad av lämpliga skyddsåtgärder enligt artikel 49⁴⁵ och i artikel 22 om automatiserat individuellt beslutsfattande, inklusive profilering⁴⁶.

Enligt GDPR är ett ”uttalande” eller en ”entydig bekräftande handling” en förutsättning för ett regelrätt samtycke. Eftersom kravet om regelrätt samtycke i GDPR redan är striktare än samtyckeskravet i direktiv 95/46/EG måste det förtydligas vilka extra ansträngningar en personuppgiftsansvarig måste göra för att erhålla den registrerades *uttryckliga* samtycke i linje med GDPR.

Med begreppet *uttryckligt* avses hur den registrerade lämnar sitt samtycke. Det innebär att den registrerade måste avge en uttrycklig samtyckesförklaring. Ett självklart sätt att se till att samtycket är uttryckligt är att uttryckligen bekräfta sitt samtycke i en skriftlig förklaring. Där så är lämpligt skulle den personuppgiftsansvarige kunna säkerställa att den skriftliga förklaringen undertecknas av den registrerade, för att undanröja alla eventuella tvivel och risker för bristande bevisning i framtiden⁴⁷.

En sådan skriftlig förklaring är dock inte det enda sättet att erhålla uttryckligt samtycke, och det vore felaktigt att säga att skriftliga och undertecknade förklaringar föreskrivs i GDPR i alla de fall som kräver ett giltigt uttryckligt samtycke. I digitala eller internetrelaterade sammanhang kan de registrerade få avge den begärda förklaringen genom att fylla i ett elektroniskt formulär, skicka ett e-postmeddelande, ladda upp ett skannat dokument med deras underskrift eller använda sig av elektronisk underskrift. Teoretiskt sett kan även muntliga förklaringar vara tillräckligt uttryckliga för att ett giltigt uttryckligt samtycke ska erhållas. Det kan dock vara svårt att bevisa för den personuppgiftsansvarige att samtliga villkor för giltigt uttryckligt samtycke var uppfyllda när förklaringen spelades in.

En organisation kan också erhålla uttryckligt samtycke genom en telefonkonversation, förutsatt att informationen om valmöjligheten är opartisk, begriplig och tydlig och att den registrerade ombeds ge en särskild bekräftelse (t.ex. genom att trycka på en knapp eller ge en muntlig bekräftelse).

[Exempel 17] En personuppgiftsansvarig får också erhålla uttryckligt samtycke från en besökare på sin webbplats via en skärm där uttryckligt samtycke ges i Ja- och Nej-rutor, förutsatt att samtycket tydligt framgår av texten, till exempel ”Jag samtycker härmed till behandling av mina personuppgifter” och inte ”Jag förstår att

⁴⁵ Enligt artikel 49.1 a i GDPR kan uttryckligt samtycke innebära ett upphävande av förbudet mot överföringar av personuppgifter till länder som saknar lämplig dataskyddslagstiftning. Notera även arbetsdokumentet om en gemensam tolkning av artikel 26.1 i direktiv

95/46/EG av den 24 oktober 1995 (WP 114), s. 11, där artikel 29-gruppen anger att samtycke inte får begäras för periodisk eller pågående överföring av personuppgifter.

⁴⁶ I artikel 22 i GDPR införs bestämmelser för att skydda registrerade mot beslutsfattande som enbart grundas på automatiserad behandling, inklusive profilering. Beslut som fattas på sådant sätt är tillåtna på vissa villkor enligt lag. Samtycke spelar en avgörande roll för denna skyddsmekanism, eftersom det klargörs i artikel 22.2 c i GDPR att en personuppgiftsansvarig får tillämpa automatiserat beslutsfattande, inbegripet profilering, som i betydande grad påverkar den enskilda personen, om det grundar sig på den registrerades uttryckliga samtycke. Artikel 29-gruppen har tagit fram separata riktlinjer om detta: *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679* (ung. artikel 29-gruppens riktlinjer av den 3 oktober 2017 om automatiserat individuellt beslutsfattande och profilering med avseende på förordning (EU) 2016/679) (WP 251) (ej översatta till svenska).

⁴⁷ Se även artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 25.

mina personuppgifter kommer att behandlas”. Givetvis bör villkoren för informerat samtycke liksom övriga villkor för erhållande av giltigt samtycke uppfyllas.

[Exempel 18] En plastikkirurgiklinik vill ha en patients uttryckliga samtycke för att få överföra hans journal till en expert som patienten vill ha ett andra utlåtande från. Journalen är en digital fil. Med tanke på informationens särskilda karaktär begär kliniken en elektronisk underskrift av den registrerade för att erhålla ett giltigt uttryckligt samtycke och kunna visa att uttryckligt samtycke har erhållits⁴⁸.

Den dubbla kontrollen av samtycket kan också vara ett sätt att kontrollera det uttryckliga samtyckets giltighet. Den registrerade kan till exempel informeras via e-post om att den personuppgiftsansvarige avser att behandla en journal med medicinska uppgifter. Den personuppgiftsansvarige förklarar i e-postmeddelandet att han begär samtycke för att få använda en viss uppsättning uppgifter för ett specifikt ändamål. Om den registrerade samtycker till att uppgifterna används ska den personuppgiftsansvarige be honom eller henne att svara genom ett e-postmeddelande som innehåller orden ”Jag samtycker”. När den registrerade har skickat sitt svar får han en verifieringslänk som han måste klicka på, eller ett sms-meddelande med en verifieringskod, för att bekräfta sitt samtycke.

Enligt artikel 9.2 betraktas inte ”nödvändig för att fullgöra ett avtal” som ett undantag till det allmänna förbudet mot att behandla särskilda kategorier av uppgifter. Personuppgiftsansvariga och medlemsstater som handskas med sådana situationer bör därför undersöka de särskilda undantagen i artikel 9.2 b–j. Om inget av undantagen i leden b–j är tillämpliga, är det enda lagliga undantaget för att behandla sådana uppgifter att erhålla uttryckligt samtycke i enlighet med villkoren för giltigt samtycke i GDPR.

[Exempel 19]

Ett flygbolag, Holiday Airways, erbjuder flygtjänster med assistans för passagerare som inte kan resa utan assistans, till exempel på grund av funktionsnedsättning. En kund bokar ett flyg från Amsterdam till Budapest och begär reseassistans för att kunna gå ombord på planet. Holiday Airways begär information om hennes hälsotillstånd för att kunna ge henne rätt tjänster (härav finns många möjligheter, t.ex. rullstol vid ankomstgaten eller en assistent som reser tillsammans med henne från A till B). Holiday Airways begär uttryckligt samtycke för att behandla kundens hälsouppgifter i syfte att ordna den begärda reseassistansen. - De uppgifter som behandlas utifrån samtycke bör vara nödvändiga för den begärda tjänsten. Dessutom finns flighter till Budapest utan reseassistans. Eftersom uppgifterna är nödvändiga för att tillhandahålla den begärda tjänsten är artikel 7.4 inte tillämplig.

[Exempel 20]

Ett framgångsrikt företag är specialiserat på att tillhandahålla specialtillverkade skid- och snowboardglasögon och andra typer av specialanpassade glasögon för utomhusaktiviteter. Tanken är att kunderna ska kunna bära dessa utan sina egna glasögon under. Företaget får ordrar från en central och levererar sina produkter från ett och samma ställe till hela EU. För att kunna tillhandahålla sina skräddarsydda produkter till närsynta kunder begär den personuppgiftsansvarige samtycke till att få använda uppgifter om kundernas ögontillstånd. Kunderna lämnar nödvändiga hälsouppgifter, till exempel deras receptuppgifter på nätet, när de gör sin beställning. I annat fall kan inte de skräddarsydda produkterna tillhandahållas. Företaget erbjuder också olika goggles med standardiserade korrigeringsvärden. De kunder som inte vill lämna sina hälsouppgifter kan välja

⁴⁸ Detta exempel påverkar inte bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

standardglasögonen. Följaktligen krävs uttryckligt samtycke enligt artikel 9, och samtycket kan anses ha lämnats frivilligt.

5. Ytterligare villkor för erhållande av giltigt samtycke

Genom GDPR införs krav om att personuppgiftsansvariga ska vidta ytterligare åtgärder för att säkerställa att de erhåller, bibehåller och kan bevisa att de har erhållit giltigt samtycke. I artikel 7 i GDPR anges dessa ytterligare villkor för giltigt samtycke, tillsammans med särskilda bestämmelser om att samtyckesregister ska föras och att de registrerade ska ha rätt att återkalla samtycket utan problem. Artikel 7 är även tillämplig för sådant samtycke som avses i andra artiklar i GDPR, till exempel artiklarna 8 och 9. Nedan ges vägledning om det ytterligare kravet att visa att giltigt samtycke erhållits och om återkallande av samtycke.

5.1. Bevis på samtycke

Av artikel 7.1 i GDPR framgår det tydligt att den personuppgiftsansvarige har en uttrycklig skyldighet att styrka de registrerades samtycke. Enligt artikel 7.1 vilar bevisbördan på den personuppgiftsansvarige.

Skäl 42 har följande lydelse: *"När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen."*

De personuppgiftsansvariga får ta fram metoder för att följa denna bestämmelse på ett sätt som passar deras dagliga verksamhet. Samtidigt bör den personuppgiftsansvariges skyldighet att styrka att giltigt samtycke har erhållits inte i sig leda till att behandlingen av personuppgifter ökar på ett överdrivet sätt. Detta innebär att de personuppgiftsansvariga bör ha tillräckliga uppgifter för att visa en koppling till behandlingen (visa att samtycke erhållits), men de bör inte samla in mer uppgifter än nödvändigt.

Det är upp till den personuppgiftsansvarige att bevisa att giltigt samtycke har erhållits från den registrerade. I GDPR anges det inte exakt hur detta ska ske. Den personuppgiftsansvarige måste dock kunna styrka samtycket från en registrerad i ett visst fall. Skyldigheten att styrka samtycke föreligger så länge som behandlingen av uppgifterna pågår. När behandlingen har avslutats bör samtyckesbeviset inte bevaras längre än vad som är strikt nödvändigt för att uppfylla en rättslig förpliktelse eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk, i enlighet med artikel 17.3 b och e.

Den personuppgiftsansvarige kan till exempel föra ett register över erhållna förklaringar, så att han eller hon kan visa hur samtycket erhållits, när samtycket erhöles och den information som då lämnades till den registrerade. Den personuppgiftsansvarige ska också kunna visa att den registrerade har informerats och att den personuppgiftsansvariges arbetsflöde har uppfyllt alla relevanta kriterier för ett giltigt samtycke. Den logiska grunden till denna skyldighet i GDPR är att de personuppgiftsansvariga måste vara ansvarsskyldiga när det gäller erhållandet av giltigt samtycke från de registrerade och för de samtyckesmekanismer som de har infört. I internetsammanhang skulle till exempel en personuppgiftsansvarig kunna bevara information om den session då samtycket lämnades, tillsammans med information om arbetsflödet vid tiden för

sessionen, och en kopia av den information som då gavs till den registrerade. Det skulle inte vara tillräckligt att enbart hänvisa till en korrekt konfiguration på webbplatsen i fråga.

[Exempel 21] Ett sjukhus startar ett program för vetenskaplig forskning (kallat projekt X) för vilket man behöver riktiga patienters tandläkarjournaler. Deltagarna rekryteras via telefonsamtal till patienter som frivilligt har samtyckt till att finnas med på en lista över kandidater som kan kontaktas för ändamålet. Den personuppgiftsansvarige begär uttryckligt samtycke från de registrerade för att få använda deras tandläkarjournaler. Samtycket erhålls via telefon genom att man spelar in en muntlig förklaring från den registrerade om att han eller hon bekräftar sitt samtycke till att personuppgifterna används för projekt X.

Det finns ingen specifik tidsgräns i GDPR för hur länge ett samtycke gäller. Detta beror på sammanhanget, omfattningen av det ursprungliga samtycket och den registrerades förväntningar. Det ursprungliga samtycket är inte längre giltigt om behandlingen förändras eller utvecklas på ett betydande sätt. Om så är fallet måste ett nytt samtycke erhållas.

Artikel 29-gruppen rekommenderar en bästa praxis där samtycket bör uppdateras med lämpliga mellanrum. Genom att ge all information än en gång blir det lättare att se till att de registrerade fortfarande är välinformerade om hur deras personuppgifter används och hur de kan utöva sina rättigheter⁴⁹.

5.2.Återkallande av samtycke

Återkallande av samtycke utgör en viktig del i GDPR. Bestämmelserna och skälen om återkallande av samtycke i GDPR kan betraktas som en kodifiering av den befintliga tolkningen av frågan i artikel 29-gruppens yttranden⁵⁰.

I artikel 7.3 i GDPR föreskrivs att den personuppgiftsansvarige måste se till att den registrerade kan återkalla samtycket när som helst och lika lätt som att lämna det. Enligt GDPR måste inte samtycke ges och återkallas genom en och samma handling.

När samtycke erhålls elektroniskt genom ett enda musklick, en svajp eller ett tangenttryck måste de registrerade i praktiken kunna återkalla samtycket lika lätt. Om samtycke erhålls genom ett tjänstspecifikt användargränssnitt (t.ex. via en webbplats, en app, ett inloggningskonto, gränssnittet till en sakernas internet-enhet eller e-post), måste den registrerade utan tvivel kunna återkalla samtycket via samma elektroniska gränssnitt, eftersom det skulle kräva en omotiverad ansträngning att byta till ett annat gränssnitt enbart för att återkalla samtycket. Dessutom bör den registrerade kunna återkalla samtycket utan problem. Detta innebär bland annat att en personuppgiftsansvarig måste se till att det inte kostar något att återkalla samtycket och att det hela inte innebär att tjänsten försämras⁵¹.

⁴⁹ Se artikel 29-gruppens riktlinjer om öppenhet. [Inför citat]

⁵⁰ Artikel 29-gruppen har behandlat frågan i yttrandet om samtycke (se yttrande 15/2011 om definitionen av begreppet "samtycke" (WP 187), s. 9, 13, 20, 27 och 32–33) och yttrandet om användning av lokaliseringssuppgifter m.m. (se yttrande 5/2005 om användning av lokaliseringssuppgifter för att tillhandahålla mervärdestjänster (WP 115), s. 7).

⁵¹ Se även artikel 29-gruppens yttrande 4/2010 över FEDMA:s europeiska uppförandekodex för användning av personuppgifter i direkt marknadsföring (WP 174) och yttrande 5/2005 om användning av lokaliseringssuppgifter för att tillhandahålla mervärdestjänster (WP 115).

[Exempel 22] En musikfestival säljer biljetter genom ett biljettombud på nätet. För varje biljett som säljs på nätet krävs samtycke för att ombudet ska få använda kontaktuppgifterna i reklam syfte. Kunderna kan svara ”Ja” eller ”Nej” på frågan om de samtycker eller ej. Den personuppgiftsansvarige informerar kunderna om att de har möjlighet att återkalla sitt samtycke. För att göra detta kan de kontakta en teletjänstcentral på arbetsdagar kl. 08.00–17.00 utan kostnad. Den personuppgiftsansvarige i detta exempel respekterar inte artikel 7.3 i GDPR. För att återkalla samtycket i detta fall måste ett telefonsamtal göras under arbetstid, vilket är mer mödosamt än det musklick som krävs för att lämna samtycket via biljettförsäljaren på nätet, som har öppet 24 timmar om dygnet, 7 dagar i veckan.

Kravet att det ska vara lätt att återkalla samtycket anges i GDPR som en nödvändig del för att samtycket ska vara giltigt. Om rätten till återkallande inte uppfyller kraven i GDPR är den personuppgiftsansvariges samtyckesmekanism inte förenlig med förordningen. Såsom anges i avsnitt 3.1 om villkoret för *informerat* samtycke måste den personuppgiftsansvarige, innan samtycket lämnas, informera den registrerade om hans eller hennes rätt att återkalla samtycket, i enlighet med artikel 7.3 i GDPR. Dessutom måste den personuppgiftsansvarige som en del av öppenhetsskyldigheten informera de registrerade om hur de kan utöva sina rättigheter⁵².

Den allmänna regeln är att om samtycke återkallas måste all behandling av personuppgifter som baseras på samtycke och som ägde rum innan samtycket återkallades och i enlighet med GDPR förbli laglig, men den personuppgiftsansvarige måste dock stoppa behandlingen i fråga. Om det inte finns någon annan laglig grund som motiverar behandlingen (t.ex. ytterligare lagring) av uppgifterna, bör uppgifterna raderas av den personuppgiftsansvarige⁵³.

Såsom tidigare nämnts i dessa riktlinjer är det mycket viktigt att de personuppgiftsansvariga bedömer de ändamål som uppgifterna faktiskt behandlas för och de lagliga grunderna för detta innan de samlar in uppgifter. Företag behöver ofta personuppgifter för flera olika syften, och behandlingen baseras inte sällan på mer än en laglig grund (t.ex. kan kunduppgifter baseras på avtal och samtycke). Ett återkallande av ett samtycke innebär därmed inte att en personuppgiftsansvarig måste radera de uppgifter som behandlas för ett ändamål som baseras på genomförandet av avtalet med den registrerade. Därför bör de personuppgiftsansvariga redan från början ha klart för sig vilka ändamål som är tillämpliga för respektive uppgiftskategori och vilken den lagliga grunden är.

De personuppgiftsansvariga är skyldiga att radera uppgifter som behandlats baserat på samtycke så snart som samtycket återkallats, eftersom man kan anta att det inte finns något annat ändamål som motiverar ytterligare lagring⁵⁴.

Bortsett från denna situation, som omfattas av artikel 17.1 b, kan en enskild registrerad person begära radering av andra uppgifter om honom eller henne vilka behandlas utifrån en annan rättslig grund, till exempel artikel 6.1 b⁵⁵. De personuppgiftsansvariga är skyldiga att bedöma huruvida

⁵² Skäl 39 i GDPR, där det hänvisas till artiklarna 13 och 14 i förordningen, har följande lydelse: ”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.”

⁵³ Se artikel 17.1 b och 17.3 i GDPR.

⁵⁴ I detta fall måste det finnas en separat rättslig grund för det andra ändamål som motiverar behandling. Detta innebär inte att den personuppgiftsansvarige kan byta från samtycke till en annan laglig grund (se avsnitt 6 nedan).

⁵⁵ Se artikel 17, inklusive eventuella undantag, och skäl 65 i GDPR.

fortsatt behandling av uppgifterna i fråga är lämpligt, även om de registrerade inte har begärt att de ska raderas⁵⁶.

I fall där den registrerade återkallar sitt samtycke och den personuppgiftsansvarige vill fortsätta behandla personuppgifterna utifrån en annan laglig grund, får de inte i tysthet övergå från samtycke (vilket har återkallats) till denna andra lagliga grund. En förändring i den lagliga grunden för behandlingen måste meddelas den registrerade i enlighet med upplysningskraven i artiklarna 13 och 14 och den allmänna öppenhetsprincipen.

6. Interaktion mellan samtycke och andra lagliga grunder i artikel 6 i GDPR

I artikel 6 fastställs villkoren för laglig behandling av personuppgifter och vidare anges vilka sex lagliga grunder som en personuppgiftsansvarig kan åberopa. Det måste fastställas vilken av dessa sex grunder som kommer att tillämpas innan behandlingen inleds och med avseende på ett specifikt ändamål⁵⁷.

Det är viktigt att notera i detta avseende att om de personuppgiftsansvariga väljer att åberopa samtycke för någon del av behandlingen måste de vara beredda att respektera detta val och stoppa denna del av behandlingen om en enskild person återkallar sitt samtycke. Det vore i grund och botten orättvist gentemot de enskilda personerna att ge budskapet att uppgifterna kommer att behandlas baserat på samtycke samtidigt som man faktiskt hänvisar till en annan laglig grund.

Med andra ord får inte den personuppgiftsansvarige byta från samtycke till andra rättsliga grunder. Det är till exempel inte tillåtet att retroaktivt använda berättigat intresse som grund för att motivera behandlingen, om det har uppstått problem med att erhålla giltigt samtycke. På grund av kravet att de personuppgiftsansvariga måste ange laglig grund när personuppgifterna inhämtas, måste de ha bestämt vilken den lagliga grunden är innan de samlar in uppgifterna.

7. Särskilda problemområden i GDPR

7.1. Barn (artikel 8)

Jämfört med det nuvarande direktivet ger GDPR ytterligare en skyddsnivå vid behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn. I artikel 8 införs ytterligare skyldigheter för att säkerställa en högre dataskyddsnivå för barn när det gäller informationssamhällets tjänster. Skälen till det ökade skyddet anges i skäl 38: *"[...] barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. [...]"* I skäl 38 anges även följande: *"Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas."* Orden "i synnerhet" visar att det särskilda skyddet inte är begränsat till marknadsföring eller profilering utan att det innefattar "insamling av personuppgifter med avseende på barn".

⁵⁶ Se även artikel 5.1 e i GDPR.

⁵⁷ Enligt artikel 13.1 c och/eller artikel 14.1 c måste den personuppgiftsansvarige informera den registrerade om detta.

Enligt artikel 8.1 ska behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år, när informationssamhällets tjänster erbjuds direkt till ett barn. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån som samtycke ges eller godkänns av den person som har föräldraansvar för barnet⁵⁸. När det gäller åldersgränsen för giltigt samtycke medger GDPR en viss flexibilitet, och medlemsstaterna får föreskriva en lägre ålder i sin nationella rätt i detta syfte, men denna får inte vara lägre än 13 år.

Såsom anges i avsnitt 3.1 om informerat samtycke ska informationen vara begriplig för den målgrupp som den personuppgiftsansvarige vänder sig till, med särskild hänsyn tagen till barns ställning. För att erhålla ”informerat samtycke” från ett barn måste den personuppgiftsansvarige förklara på ett språk som är klart och tydligt för barn hur man avser att behandla de personuppgifter som insamlas⁵⁹. Om det är föräldern som ska ge sitt samtycke kan vissa uppgifter krävas för att vuxna ska kunna fatta ett informerat beslut.

Av ovanstående framgår det att artikel 8 endast ska tillämpas när följande villkor är uppfyllda:

- Behandlingen rör erbjudande av informationssamhällets tjänster direkt till ett barn.^{60, 61}
- Behandling som grundar sig på samtycke.

7.1.1. Informationssamhällets tjänster

För att fastställa tillämpningsområdet för begreppet ”informationssamhällets tjänster” i GDPR hänvisas det i artikel 4.25 i GDPR till direktiv (EU) 2015/1535.

Artikel 29-gruppen hänvisar även till EU-domstolens rättspraxis⁶² vid bedömningen av definitionens tillämpningsområde. EU-domstolen har framhållit att *informationssamhällets tjänster* omfattar avtal och andra tjänster som ingås eller sänds online. Om en tjänst har två ekonomiskt

⁵⁸ Utan påverkan på medlemsstatens möjlighet att i sin lag avvika från åldersgränsen, se artikel 8.1.

⁵⁹ I skäl 58 i GDPR bekräftas denna skyldighet på nytt, genom att den personuppgiftsansvarige, vid behov, ska se till att den information som ges är begriplig för barn.

⁶⁰ Enligt artikel 4.25 i GDPR avses med informationssamhällets tjänster alla tjänster enligt definitionen i artikel 1.1 b i direktiv (EU) 2015/1535: ”b) tjänst: alla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I denna definition avses med i) på distans: tjänster som tillhandahålls utan att parterna är närvarande samtidigt, ii) på elektronisk väg: en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling (inbegripet digital signalkomprimering) och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel, iii) på individuell begäran av en tjänstemottagare: en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran.” En vägledande förteckning över tjänster som inte omfattas av denna definition finns i bilaga I till nämnda direktiv. Se även skäl 18 i direktiv 2000/31/EG.

⁶¹ Enligt artikel 1 i FN:s konvention om barnets rättigheter avses med barn ”varje människa under 18 år, om inte barnet blir myndigt enligt den lag som gäller för barnet”, se Förenta Nationerna, Generalförsamlingens resolution 44/25 av den 20 november 1989 (barnrättskonventionen).

⁶² Domstolens dom av den 2 december 2010, Ker-Optika/ÀNTSZ Dél-dunántúli Regionális Intézet, C-108/09, punkterna 22 och 28. När det gäller ”blandade tjänster” hänvisar artikel 29-gruppen även till domen av den 20 december 2017, Asociación Profesional Elite Taxi/Uber Systems Spain SL, C-434/15, punkt 40. Där anges att informationssamhällets tjänster som utgör en integrerad del av en helhetstjänst som huvudsakligen inte består av informationssamhällets tjänster (i detta fall transporttjänst) inte får anses uppfylla kraven för informationssamhällets tjänster.

oberoende delar, där den ena är en onlinedel, till exempel anbud och godtagande av anbud vid ingående av ett avtal eller information om produkter eller tjänster, inbegripet marknadsföring, definieras denna del som informationssamhällets tjänster. Den andra delen är då fysisk leverans eller distribution av varor som inte omfattas av begreppet informationssamhällets tjänster. Onlineleverans av en tjänst skulle omfattas av begreppet *informationssamhällets tjänster* i artikel 8 i GDPR.

7.1.2. Erbjuds direkt till barn

Inbegripandet av ordalydelsen ”erbjuds direkt till barn” tyder på att artikel 8 endast ska tillämpas på vissa och inte samtliga informationssamhällestjänster. Om en leverantör av informationssamhällets tjänster klargör för potentiella användare att den endast erbjuder sina tjänster till personer över 18 år och detta inte undermineras av andra bevis (t.ex. innehållet på webbplatsen eller försäljningsplaner) kommer tjänsten inte att anses erbjudas ”direkt till barn” i detta avseende och således kommer artikel 8 inte att tillämpas.

7.1.3. Ålder

I GDPR anges följande: *”Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.”* Den personuppgiftsansvarige måste känna till de olika nationella lagarna och beakta målgruppen för tjänsterna. Det bör framför allt noteras att en personuppgiftsansvarig som tillhandahåller en gränsöverskridande tjänst inte alltid kan hänvisa till att han eller hon enbart följer lagen i den medlemsstat där han eller hon har sitt huvudsakliga verksamhetsställe. Den personuppgiftsansvarige kan dock behöva följa de nationella lagarna i var och en av de medlemsstater som han eller hon erbjuder informationssamhällestjänsterna i. Detta beror på huruvida en medlemsstat väljer att använda den personuppgiftsansvariges huvudsakliga verksamhetsställe eller den registrerades hemvist som referenspunkt i sin nationella lagstiftning. Medlemsstaterna ska först och främst ta hänsyn till barnets bästa när de gör sitt val. Artikel 29-gruppen uppmuntrar medlemsstaterna att försöka finna en harmoniserad lösning på denna fråga.

När de personuppgiftsansvariga tillhandahåller informationssamhällets tjänster till barn grundat på samtycke förväntas de göra rimliga ansträngningar för att kontrollera att användaren innehar åldern för digitalt samtycke, och dessa åtgärder bör stå i proportion till behandlingens art och risker.

Om användarna uppger att de innehar åldern för digitalt samtycke kan den personuppgiftsansvarige göra lämpliga kontroller för att kontrollera att uttalandet är riktigt. Det finns inga uttryckliga krav i GDPR om att rimliga ansträngningar måste göras för att kontrollera åldern. Däremot är detta underförstått, eftersom behandlingen av personuppgifter kommer att vara olaglig om ett barn ger sitt samtycke trots att det inte innehar åldern för giltigt samtycke.

Om användaren uppger att han eller hon inte innehar åldern för digitalt samtycke kan den personuppgiftsansvarige godta uttalandet utan ytterligare kontroller men måste då gå vidare och få föräldrarnas godkännande samt kontrollera att den person som lämnar samtycke har föräldraansvar för barnet.

Ålderskontrollen bör inte leda till orimlig behandling av personuppgifter. Den mekanism som valts för att kontrollera den registrerades ålder bör inbegripa en bedömning av riskerna med den föreslagna behandlingen. I vissa situationer där risken är låg kan det vara lämpligt att begära att nya abonnenter till en tjänst ska ange sitt födelseår eller fylla i ett formulär där de intygar att de (inte) är barn⁶³. Om tvivel uppstår bör den personuppgiftsansvarige se över sina ålderskontrollmekanismer i det särskilda fallet och överväga huruvida andra kontroller behöver göras⁶⁴.

7.1.4. Barns samtycke och föräldraansvar

När det gäller godkännande av en person som har föräldraansvar för barnet anges det inte i GDPR hur föräldrarnas samtycke ska inhämtas i praktiken eller hur det ska fastställas att någon har rätt att vidta denna åtgärd⁶⁵. Artikel 29-gruppen rekommenderar därför att man inför ett proportionerligt synsätt, i linje med artikel 8.2 och artikel 5.1 c i GDPR (uppgiftsminimering). Ett proportionerligt synsätt kan vara att inrikta sig på att erhålla en begränsad mängd uppgifter, såsom föräldrarnas eller vårdnadshavarens kontaktuppgifter.

Vad som är rimligt, både när det gäller att kontrollera att användaren är gammal nog att lämna sitt eget samtycke och när det gäller att kontrollera att en person som lämnar samtycke på ett barns vägnar innehar föräldraansvar för barnet, kan bero på vilka risker behandlingen medför och vilken teknik som finns till förfogande. I situationer där risken är låg kan det vara tillräckligt att kontrollera föräldraansvaret via e-post. Omvänt kan det i situationer där risken är hög vara lämpligt att begära mer bevisning, så att den personuppgiftsansvarige kan kontrollera och behålla sådana uppgifter som avses i artikel 7.1 i GDPR⁶⁶. Kontrolltjänster som utförs av betrodd tredje part kan erbjuda lösningar som minimerar den mängd personuppgifter som den personuppgiftsansvarige själv måste behandla.

[Exempel 23] En spelplattform på internet vill säkerställa att minderåriga kunder endast kan abonnera på dess tjänster med föräldrarnas eller vårdnadshavarnas samtycke. Den personuppgiftsansvarige vidtar följande åtgärder:

Steg 1: Den personuppgiftsansvarige begär att användaren uppger om han eller hon är under eller över 16 år (eller annan ålder för digitalt samtycke).

Om användaren uppger att han eller hon inte innehar åldern för digitalt samtycke sker följande:

Steg 2: Tjänsten informerar barnet om att en förälder eller vårdnadshavare måste lämna samtycke till eller godkänna behandlingen innan tjänsten tillhandahålls till barnet. Användaren ombeds uppge e-postadressen till en förälder eller vårdnadshavare.

Steg 3: Tjänsten kontakter föräldern eller vårdnadshavaren och får deras samtycke till behandlingen via e-post och vidtar rimliga åtgärder för att bekräfta att den vuxna personen har föräldraansvar.

Steg 4: Om invändningar görs vidtar plattformen ytterligare åtgärder för att kontrollera abonnentens ålder.

⁶³ Detta är kanske ingen vattentät lösning i samtliga fall, men det är ett exempel på hur saken kan hanteras.

⁶⁴ Se artikel 29-gruppens yttrande 5/2009 om sociala nätverk på Internet (WP 163).

⁶⁵ Artikel 29-gruppen noterar att den person som har föräldraansvar inte alltid är barnets biologiska förälder och att föräldraansvar kan innehållas av flera olika parter som kan vara både juridiska och fysiska personer.

⁶⁶ En förälder eller vårdnadshavare skulle till exempel kunna ombes betala 0,01 euro till den personuppgiftsansvarige via banköverföring och samtidigt ge en kortfattad bekräftelse i transaktionens meddelanderad att bankkontoinnehavaren har föräldraansvar för barnet. I lämpliga fall bör en alternativ kontrollmetod finnas för att förhindra otillbörlig diskriminering av personer som inte innehar något bankkonto.

Om plattformen har uppfyllt övriga samtyckeskrav kan plattformen följa de ytterligare kriterier som anges i artikel 8 i GDPR genom att vidta nämnda åtgärder.

Exemplet visar att den personuppgiftsansvarige kan skapa sig förutsättningar för att visa att rimliga ansträngningar har gjorts för att säkerställa att giltigt samtycke har erhållits, med avseende på tjänster som tillhandahålls till barn. Dessutom innehåller artikel 8.2 följande särskilda bestämmelse: *”Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.”*

Det är upp till den personuppgiftsansvarige att avgöra vilka åtgärder som är lämpliga i ett visst fall. De personuppgiftsansvariga bör som en allmän regel undvika kontrollösningar som medför en orimlig insamling av personuppgifter.

Artikel 29-gruppen inser att det kan vara en utmaning att kontrollera detta i vissa fall (t.ex. där barn som lämnar eget samtycke ännu inte har något ”identitetsfotavtryck” eller där det är svårt att kontrollera vem som innehar föräldraansvar). Detta kan beaktas vid beslut om vilka ansträngningar som är rimliga, men de personuppgiftsansvariga förväntas även ha ständig uppsikt över sina processer och tillgänglig teknik.

När det gäller den registrerades frihet att samtycka till behandling av sina personuppgifter och ha fullständig kontroll över denna, kan samtycke till behandling av ett barns personuppgifter vilket lämnats eller godkänts av en person med föräldraansvar bekräftas, ändras eller återkallas så snart den registrerade uppnår åldern för digitalt samtycke.

I praktiken innebär detta att om barnet inte vidtar någon åtgärd kommer den giltiga grunden för behandlingen att fortsätta vara det samtycke som lämnats eller godkänts av en person med föräldraansvar för behandlingen av personuppgifterna innan barnet uppnått åldern för digitalt samtycke.

Efter att barnet uppnått åldern för digitalt samtycke kommer det att ha möjlighet att återkalla samtycket självt, i linje med artikel 7.3. Enligt principerna om korrekthet och laglighet måste den personuppgiftsansvarige informera barnet om denna möjlighet⁶⁷.

Det är viktigt att påpeka det som anges i skäl 38, nämligen att samtycke från en förälder eller vårdnadshavare inte krävs för förebyggande eller rådgivande tjänster som erbjuds direkt till barn. Barnskyddstjänster som erbjuds på internet till ett barn via en onlinechatt kräver till exempel inget föregående tillstånd från föräldrarna.

Avslutningsvis anges det i GDPR att bestämmelserna om krav på tillstånd från föräldrarna gentemot minderåriga inte får påverka ”tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn”. Kraven vad gäller giltigt samtycke till användning av barns personuppgifter utgör därför en del av en

⁶⁷ Dessutom bör de registrerade vara medvetna om ”rätten att bli bortglömd” enligt artikel 17, vilken är särskilt relevant för samtycke som lämnas när den registrerade fortfarande är ett barn (se skäl 63).

rättslig ram som måste beaktas separat från nationell avtalsrätt. I dessa riktlinjer behandlas därför inte frågan om huruvida en minderårig får ingå avtal på internet enligt lag. Båda rättssystemen kan tillämpas samtidigt, och harmonisering av nationella avtalsrättsliga bestämmelser omfattas inte av GDPR:s tillämpningsområde.

7.2. Vetenskaplig forskning

Definitionen av vetenskapliga forskningsändamål har betydande förgreningar när det gäller de olika sätt på vilka en personuppgiftsansvarig kan behandla personuppgifter. I GDPR ges ingen definition av begreppet ”vetenskaplig forskning”. Skäl 159 har följande lydelse: ”[...] *Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning [...].*” Artikel 29-gruppen anser dock inte att begreppet får utökas till att omfatta mer än dess allmänna betydelse och är medveten om att ”vetenskaplig forskning” i detta sammanhang innebär ett forskningsprojekt som inrättats i överensstämmelse med relevanta metodologiska och etiska standarder inom sektorn, i enlighet med god praxis.

När samtycke utgör den rättsliga grunden för att bedriva forskning enligt GDPR bör sådant samtycke till användning av personuppgifter särskiljas från andra samtyckeskrav som fungerar som en etisk standard eller processuell skyldighet. Ett exempel på en sådan processuell skyldighet, där behandlingen inte baseras på samtycke utan på någon annan rättslig grund, ges i förordningen om kliniska prövningar. Inom ramen för dataskyddslagstiftningen skulle den sistnämnda formen av samtycke kunna betraktas som en ytterligare skyddsåtgärd⁶⁸. Samtidigt innebär inte GDPR att artikel 6 endast får tillämpas när det gäller samtycke, med avseende på behandling av personuppgifter för forskningsändamål. Så länge som lämpliga skyddsåtgärder finns, till exempel kraven i artikel 89.1, och behandlingen är rättvis, laglig, öppen och förenlig med uppgiftsminimeringsstandarder och individuella rättigheter kan andra lagliga grunder såsom artikel 6.1 e eller f vara tillgängliga⁶⁹. Detta gäller även särskilda kategorier av uppgifter, enligt undantaget i artikel 9.2 j⁷⁰.

Skäl 33 verkar ge en viss flexibilitet när det gäller graden av specificering och granularitet i ett samtycke som lämnas inom området för vetenskaplig forskning. Skäl 33 har följande lydelse: ”*Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iaktas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.*”

⁶⁸ Se även skäl 161 i GDPR.

⁶⁹ Artikel 6.1 c kan också vara tillämplig för delar av behandling som särskilt krävs enligt lag, såsom insamling av tillförlitliga och robusta uppgifter till följd av det protokoll som medlemsstaterna godkänt inom ramen för förordningen om kliniska prövningar.

⁷⁰ Särskild testning av läkemedel får ske på grundval av unionsrätten eller medlemsstaternas nationella rätt enligt artikel 9.2 i.

För det första bör det noteras att skäl 33 inte medför någon felaktig tillämpning av skyldigheterna när det gäller kravet om specifikt samtycke. Detta innebär i princip att vetenskapliga forskningsprojekt endast får inbegripa personuppgifter på grundval av samtycke om ändamålet är noga angett. I fall där syftena med en behandling av personuppgifter inom ett vetenskapligt forskningsprojekt inte kan specificeras från start, medger skäl 33 ett undantag där mer allmänna syften får anges.

Med tanke på de strikta villkor som anges i artikel 9 i GDPR när det gäller behandling av särskilda kategorier av uppgifter, noterar artikel 29-gruppen att tillämpningen av det flexibla synsättet i skäl 33 kommer att bli föremål för en striktare tolkning och kräver omfattande granskning när särskilda kategorier av uppgifter behandlas grundat på uttryckligt samtycke.

GDPR som helhet får inte tolkas på ett sådant sätt att en personuppgiftsansvarig kan kringgå den viktiga principen om att de ändamål för vilka den registrerades samtycke begärs måste specificeras. När forskningsändamål inte kan specificeras fullt ut måste en personuppgiftsansvarig försöka finna andra sätt för att säkerställa att själva andemeningen i samtyckeskraven delges på bästa sätt, till exempel för att de registrerade ska kunna samtycka till ett mer allmänt forskningsändamål och till särskilda skeden av ett forskningsprojekt som man redan från början vet kommer att äga rum. I takt med att forskningen fortgår kan samtycke för efterföljande steg i projektet erhållas innan de inleds. Ett sådant samtycke bör dock fortfarande följa tillämpliga etiska standarder för vetenskaplig forskning.

Dessutom kan den personuppgiftsansvarige vidta ytterligare skyddsåtgärder i sådana fall. I artikel 89.1 betonas bland annat behovet av skyddsåtgärder vid behandling av personuppgifter för vetenskapliga, historiska eller statistiska ändamål. Sådana ändamål ska *”omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter”*. Uppgiftsminimering, avidentifiering och datasäkerhet nämns som möjliga skyddsåtgärder.⁷¹ Avidentifiering är den bästa lösningen så snart ändamålet med forskningen kan uppfyllas utan behandling av personuppgifter.

Öppenhet är en ytterligare skyddsåtgärd när specifikt samtycke inte är tillåtet på grund av omständigheterna kring forskningen. Bristande specificering av syftet kan kompenseras genom att de personuppgiftsansvariga ger regelbunden information om hur syftet utvecklas i takt med att forskningsprojektet fortskrider, så att samtycket med tiden blir så specifikt som möjligt. På så sätt

⁷¹ Se t.ex. skäl 156. Behandlingen av personuppgifter för vetenskapliga ändamål bör även ske i enlighet med annan relevant lagstiftning, t.ex. lagstiftning om klinisk prövning (se skäl 156) och Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel. Se även artikel 29-gruppens yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 7: *”Att erhålla samtycke innebär dessutom inte ett upphävande av den registeransvariges skyldigheter enligt artikel 6 avseende korrekthet, nödvändighet och proportionalitet samt uppgifternas kvalitet. Även om behandlingen av personuppgifter bygger på den registrerades samtycke, så skulle det inte motivera att man samlar in uppgifter som inte är nödvändiga för det angivna syftet. [...] I princip ska samtycke inte betraktas som ett undantag från övriga principer för dataskydd, utan som ett ytterligare skydd. Det är i första hand en grund för lagenlighet och innebär inte att andra principer ska upphöra att gälla.”*

får de registrerade åtminstone en grundkännedom om läget, vilket innebär att de kan bedöma huruvida de ska utnyttja rätten att återkalla samtycket enligt artikel 7.3⁷².

Bristande specificering av syftet kan också uppvägas genom en omfattande forskningsplan som de registrerade kan ta del av innan de lämnar sitt samtycke⁷³. Denna forskningsplan bör innehålla så tydlig information som möjligt om planerade forskningsfrågor och arbetsmetoder. Forskningsplanen skulle också kunna bidra till förenlighet med artikel 7.1, eftersom de personuppgiftsansvariga måste visa vilken information de registrerade hade tillgång till vid tiden för samtycket för att kunna påvisa att samtycket är giltigt.

Det är viktigt att komma ihåg att de registrerade måste ha möjlighet att återkalla sitt samtycke när samtycke används som laglig grund för behandling. Artikel 29-gruppen noterar att ett återkallande av samtycke skulle kunna underminera viss vetenskaplig forskning som kräver uppgifter som kan kopplas till enskilda personer. Det framgår dock tydligt av GDPR att samtycke kan återkallas och att de personuppgiftsansvariga måste tillmötesgå en sådan begäran – inget undantag finns till detta krav när det gäller vetenskaplig forskning. Om de personuppgiftsansvariga mottar en begäran om återkallande måste de i princip radera personuppgifterna omedelbart, om de vill fortsätta använda uppgifterna för forskningsändamålen⁷⁴.

7.3. De registrerades rättigheter

Om en behandling av personuppgifter grundar sig på den registrerades samtycke kommer detta att påverka den enskildes rättigheter. De registrerade kan ha rätt till dataportabilitet (artikel 20) när behandlingen grundar sig på samtycke. Samtidigt gäller inte rätten att göra invändningar (artikel 21) när behandlingen grundar sig på samtycke, men rätten att när som helst återkalla sitt samtycke kan få ett liknande utfall.

I artiklarna 16–20 i GDPR anges att de registrerade (när behandlingen av uppgifterna grundar sig på samtycke) har rätt till radering när samtycket har återkallats samt rätt till begränsning, rättelse och tillgång⁷⁵.

8. Erhållet samtycke enligt direktiv 95/46/EG

Personuppgiftsansvariga som för närvarande behandlar personuppgifter grundat på samtycke i enlighet med nationell dataskyddslagstiftning måste inte per automatik göra en fullständig uppdatering av alla befintliga samtyckesförbindelser med registrerade som förberedelse för GDPR. Sådant samtycke som hittills har erhållits är fortfarande giltigt så länge som det överensstämmer med villkoren i GDPR.

⁷² Andra öppenhetsåtgärder kan också vara relevanta. När personuppgiftsansvariga behandlar uppgifter för vetenskapliga ändamål men inte kan ge fullständig information från start, skulle de kunna utse en särskild kontaktperson som de registrerade kan vända sig till med frågor.

⁷³ En sådan möjlighet ges i artikel 14 § 1 i Finlands personuppgiftslag (523/1999).

⁷⁴ Se även artikel 29-gruppens yttrande 05/2014 om oidentifieringsmetoder (WP 216).

⁷⁵ I fall där viss behandling av personuppgifter är begränsad i enlighet med artikel 18 i GDPR kan den registrerades samtycke krävas för att upphäva begränsningarna.

Det är viktigt att de personuppgiftsansvariga noggrant ser över befintliga arbetsprocesser och register, före den 25 maj 2018, för att förvissa sig om att befintliga samtycken uppfyller kraven i GDPR (se skäl 171 i GDPR⁷⁶). Genom GDPR höjs i praktiken ribban när det gäller införandet av samtyckesmekanismer och vidare införs flera nya krav om att personuppgiftsansvariga måste förändra sina samtyckesmekanismer i stället för att bara ta fram nya integritetspolicyer⁷⁷.

GDPR innehåller till exempel krav om att en personuppgiftsansvarig måste kunna visa att giltigt samtycke har erhållits, och därför kommer alla förmodade samtycken utan hänvisningar att automatiskt hamna under GDPR:s samtyckesstandard och behöva förnyas. På samma sätt kommer alla förmodade samtycken som grundas på en mer indirekt åtgärd från den registrerades sida (t.ex. en på förhand ikryssad *opt in*-ruta) inte heller att uppfylla kraven för GDPR:s samtyckesstandard, eftersom det enligt GDPR krävs ”ett uttalande” eller ”en entydig bekräftande handling”.

Dessutom kan de personuppgiftsansvariga behöva se över sina behandlingsprocesser och it-system för att kunna visa att samtycke erhållits eller möjliggöra en mer granulär viljeyttring. Vidare måste det finnas mekanismer för att de registrerade enkelt ska kunna återkalla sitt samtycke, och information måste ges om hur samtycket kan återkallas. Om befintliga förfaranden för erhållande och hantering av samtycke inte uppfyller GDPR:s standarder måste de personuppgiftsansvariga erhålla nya samtycken som är förenliga med GDPR.

Den utökade informationsskyldigheten i GDPR innebär däremot inte att sådant samtycke som lämnats innan GDPR träder i kraft blir ogiltigt, eftersom samtliga delar som anges i artiklarna 13 och 14 inte alltid måste finnas med som villkor för informerat samtycke (se s. 15 ovan). Enligt direktiv 95/46/EG var de personuppgiftsansvariga inte skyldiga att informera de registrerade om vilken grund behandlingen baserades på.

Om de personuppgiftsansvariga finner att ett samtycke som erhållits tidigare enligt den gamla lagstiftningen inte kommer att uppfylla standarden för samtycke enligt GDPR måste de vidta åtgärder för att följa denna standard, till exempel genom att förnya samtycket i överensstämmelse med GDPR. Enligt GDPR är det inte möjligt att byta från en laglig grund till en annan. Behandlingen måste stoppas om en personuppgiftsansvarig inte kan förnya samtycket i enlighet med kraven och dessutom – som en engångsåtgärd – inte kan övergå till kraven i GDPR genom att behandla personuppgifter baserat på en annan laglig grund och samtidigt se till att den fortsatta

⁷⁶ Skäl 171 i GDPR har följande lydelse: ”Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.”

⁷⁷ Såsom anges i inledningen görs det i GDPR ytterligare ett förtydligande och en specificering av kraven för erhållande och uppvisande av giltigt samtycke. Många av de nya kraven bygger på yttrande 15/2011 om definitionen av begreppet ”samtycke”.

behandlingen är rättvis och redogjord för. Den personuppgiftsansvarige måste under alla omständigheter iaktta principerna om laglig, rättvis och öppen behandling.

***** **DOKUMENTSLUT** *****