



JURIDISKA FAKULTETEN
vid Lunds universitet

Emilia Löfgren

Samtycket enligt den allmänna dataskyddsförordningen

Personuppgiftsansvarigas ansvar och registrerade personers
rätt till öppenhet och självbestämmande

JURM02 Examensarbete

Uppsats på juristprogrammet
30 högskolepoäng

Handledare: Docenten Vilhelm Persson

Termin: HT2017

Innehåll

FÖRORD	4
SUMMERY	5
SAMMANFATTNING	7
1 INLEDNING	9
1.1 Syfte och frågeställning	10
1.2 Disposition	10
1.3 Avgränsningar	11
1.4 Metod	11
1.5 Material	12
1.6 Forskningsläge	14
2 GRUNDLÄGGANDE REGLER OCH RÄTTIGHETER	16
2.1 Inledning	16
2.2 Internationell och nationell rätt	16
2.3 Vad avses med personlig integritet?	17
3 GRUNDLÄGGANDE OM DATASKYDDSFÖRORDNINGEN I FÖRHÅLLANDE TILL PUL	19
3.1 Bakgrund	19
3.2 Materiellt tillämpningsområde	19
3.2.1 Personuppgifter	20
3.2.2 Känsliga personuppgifter	21
3.2.3 Personuppgiftsansvarig	22
3.2.4 Behandling	23
3.2.4.1 Automatisk behandling	23
3.2.4.2 Manuell behandling	24
3.2.4.3 Missbruksregeln, 5 a § PUL	24
3.3 Territoriellt tillämpningsområde	26
3.3.1 Etableringsprincipen	26
3.3.2 Effektlandsprincipen	28
3.3.3 Förhållandet till tredje land och dataskyddslagen	29
4 LAGLIG BEHANDLING	30

4.1	Allmänt om behandlingar	30
4.1.1	Laglighet, korrekthet och öppenhet	30
4.1.2	Ändamålsbegränsning och uppgiftsminimering	31
4.1.3	Korrekthet, lagringsminimering, integritet och konfidentialitet	33
4.2	Lagliga grunder för behandling	35
4.2.1	Samtycke som laglig grund	36
4.2.1.1	Frivillighet	37
4.2.1.2	Specifikt och informerat	39
4.2.1.3	Otvetydig viljeyttring	43
4.2.2	Barns samtycke	45
4.2.2.1	Barns samtycke i PUL och direktivet	45
4.2.2.2	Förordningens art. 8	46
4.2.3	Uttryckligt samtycke	52
5	ANALYS	55
5.1	Villkor, rättigheter och ansvar	55
5.2	När barns samtycke ska lämnas	59
6	SLUTSATS	62
	KÄLLFÖRTECKNING	64
	RÄTTFALLSFÖRTECKNING	70

Förord

Resan som utgör juristprogrammet i Lund är en lång, slingring, tuff och fantastisk väg. Men tiden går fort vilket jag inser nu när jag själv står inför examen. De som har gjort att tiden har flugit iväg är de fantastiska vänner jag har funnit under min tid som student. Tillsammans har vi tagit oss igenom det mesta och vi har hunnit med en hel del galenskaper på vägen. Ni har utgjort kärnan i mitt studentliv och resan vi alla har tagit är större än jag tror någon av oss kunde förstå sig då vi träffades för första gången. Ni är alla fantastiska.

Vidare skulle jag vilja rikta ett enormt tack till min familj som alltid ställer upp oavsett vad. Ett tack ska även riktas till Paula Eninge som givit mig chansen att testa vingarna nu efter min examen. Jag vill även tacka min handledare Vilhelm Persson som har varit en god rådgivare genom hela arbetes gång. Ett särskilt tack ska även riktas till Jonas Ledendal som har assisterat och varit ett bollplank under det här arbetet.

Lund, den 2 januari 2018

Emilia Löfgren

Summery

The General Data Protection Regulation (GDPR) replaces the Data Protection Directive (Directive) in 2018. The European Commission has stated that the Directive no longer provides the protection of personal integrity that individuals are entitled to. The GDPR will harmonize the rules and its purpose is to give individuals a greater control over their data and ensure the free movement of personal data within the European Union. In Sweden, there is a proposal for a new national data protection law to complement the GDPR and replace the current Personal Data Act.

This essay will investigate if and if so, to what extent, the definition and principles of consent has changed through the GDPR in comparison to the Directive and the Personal Data Act. It will also investigate how the GDPR may affect individuals' control of their personal data as well as the liability of the controller. The current legislation has no precedent ruling hence information about the reasoning behind the GDPR has been collected from the recitals of the GDPR as well as statements by working groups that the Commission has appointed. Furthermore, rulings under the Directive have been used if applicable in relation to the GDPR. Commentary on the Personal Data Act has been used for an understanding on how this has been applied in Sweden. Articles written about the GDPR and the new rules have been used to highlight problems and/or issues highlighted by those knowledgeable on the subject.

The material scope of the GDPR will not change to any great extent compared to the Personal Data Act. However, as the Personal Data Act disappears any automated processing of personal data will now fall within the scope of the GDPR, which has not been the case in the Personal Data Act. The Territorial scope will expand, mainly in relation to controllers or processors established outside the EU that directs their services to individuals within the Union. The GDPR will also clarify the conditions for valid processing and consent. For example, it will require a higher level of transparency and put further demands on controllers with regards to processing and consent.

The conditions for valid consent will largely be the same in the GDPR as in the Personal Data Act and in the Directive, but the condition on informing the data subject will be strengthened. Long complicated legal texts will no longer be a valid way of informing the subject about the processing. Instead this information will need to be separated or otherwise clearly distinguished if it forms part of an agreement. The GDPR also clarifies what information the personal data controller has to provide, such as the individual's right to withdraw consent and what the data specifically will be used for. In order to be valid, consent will also need to be given through a clear affirmative action.

One of the biggest changes in the GDPR are the rules regarding the ability for children to give valid consent in relation to the offer of *Information Society*

Services. While an assessment of the child's maturity and understanding has been used to decide if a child can give legal consent in both the Personal Data Act and in the Directive, an age limit is now introduced through the GDPR. Its purpose is to strengthen children's rights. The GDPR sets this age limit at 16 years. When a child is below the age of 16, valid consent must instead be given by the holder of parental responsibility. The change has been criticized since it will not be harmonizing, it is unclear how safe verifications of age can be gathered, how extensive the parental responsibility will be and how this may affect children's right to privacy in relation to their parents. In Sweden, the proposal is to reduce the age limit to 13 years and this has received similar criticisms during consultations about the proposal.

As the consent of "common" personal data will change and become stricter, this means that explicit consent, which is required to process sensitive data, use profiling or for transferring information to third countries, will also have to become stricter even though the requirement is the same as in the Personal Data Protection Act and the Directive.

Although the lawfulness of consent doesn't change much through the GDPR, the consent needs to be interpreted in relation to the purpose of the GDPR in order to strengthen the personal integrity. The condition to make information clearer, more accessible and easily communicated will likely have the impact for several controllers that they need to review how they provide their information. This can directly affect situations where information and consent are given orally, which is common in a store situation when an individual wants to become a member of their customer club. How controllers gather consent and the individual's right to be able to choose to consent to only one out of several specific purposes of processing data, along the exemption that has exempted most automatic processing from the Personal Data Act will require controllers to value and reevaluate the data they process.

Furthermore, it remains to be seen what age limit will be implemented in different Member States and how children will be protected. Controllers will only need to take reasonable steps to ensure that valid consent is obtained and children will most likely find new ways to leave valid consent on their own. In relation to the Swedish law proposal, it also must be questioned whether children from the age of 13 years are mature enough to understand the meaning of consent. To ensure their right to be protected the age probably should be raised to at least 15 years.

The GDPR will lead to increased demands and increased responsibility for controllers. In regard of the high sanction fees if controllers do not comply with the requirements of the GDPR, it is most likely that personal data administrators will ensure that all necessary measures are taken to avoid legal sanctions. The GDPR will, inter alia through the information requirement, also provide data subjects with increased opportunities to control how their personal data is handled. However, it will be up to the data subjects to access the information given to them for the consent to have its full effect.

Sammanfattning

Den allmänna dataskyddsförordningen (förordningen) kommer att ersätta dataskyddsdirektivet (direktivet) år 2018. Europeiska kommissionen har ansett att direktivet inte längre ger det skydd av den personliga integriteten som enskilda har rätt till. Förordningen ska därför harmonisera reglerna, ge enskilda en ökad kontroll och samtidigt gynna den fria rörligheten av personuppgifter inom den Europeiska Unionen. I Sverige finns det förslag om att en nationell dataskyddslag ska införas för att komplettera förordningen och ersätta PUL.

Detta arbete ska utreda om, och i så fall hur, samtycket har förändrats i förordningen i förhållande till direktivet och PUL. Arbetet ska även granska hur förordningen kan komma att påverka den enskildes kontroll över sina personuppgifter och den personuppgiftsansvarigas ansvarsskyldighet. Eftersom förordningen i nuläget saknar prejudicerande domar har skälen till förordningen samt uttalanden från de arbetsgrupper som tillsats av Kommissionen utgjort några av de grundläggande källorna. Vidare har prejudicerande domar under direktivet använts eftersom förordningen bygger vidare på direktivet. Lagkommentarer för PUL har använts för att belysa hur PUL har tillämpats. Vetenskapliga artiklar som berör förordningen har använts för att belysa problem eller frågor som finns rörande denna.

Förordningens materiella tillämpningsområde kommer inte förändras i någon större utsträckning i förhållande till PUL. Ett undantag är dock att missbruksregeln i PUL försvinner. Detta gör att samtliga automatiska behandlingar kommer omfattas av förordningens tillämpningsområde. Det territoriella tillämpningsområdet kommer att expandera och även förordningen kommer att bli tillämplig för alla personuppgiftsansvariga i tredje land som riktar sina tjänster till enskilda inom unionen.

Kravet på samtycke i förordningen är till stor del likvärdigt det som stipuleras i PUL och direktivet. I förordningen stärks emellertid informationskravet och långa juridiska texter kommer inte få användas för att lämna information till enskilda. Informationen som lämnas ska även vara lättillgänglig. Förordningen klargör även vilken information som den personuppgiftsansvarige ska lämna till den registrerade. Exempelvis ska den registrerade informeras om rätten att återta ett samtycke. Vidare framgår det att ett samtycke endast kan lämnas genom en otvetydig viljeyttring och det specificeras att denna måste vara en entydig, bekräftande handling eller ett uttryckligt yttrande.

Ett nytt tillskott i förordningen är reglerna rörande barns möjligheter att lämna giltiga samtycken för tjänster som erbjuds online. I direktivet och PUL har en bedömning av barns mognad och förståelse gjorts i varje enskilt fall för att bedöma ifall ett barn kunnat lämna giltiga samtycken. I förordningen införs istället en åldersgräns på 16 år. Före denna ålder kan inte ett barn lämna giltiga

samtycken utan samtycket lämnas istället av den eller de som har föräldraansvaret å barnets vägnar. Regeln har mött kritik eftersom den inte är harmoniserande för medlemsstaterna. Vidare har det ansetts oklart hur en säker verifiering ska kunna genomföras så att inte barnet, utan den föräldraansvarige, lämnat samtycket. Det har även ifrågasatts vilken omfattning regeln kan få för de med föräldraansvar och att regeln även kan komma att strida mot barns rätt till personlig integritet gentemot sina föräldrar. I Sverige finns som förslag att åldersgränsen ska sänkas till 13 år, vilken är den lägsta ålder förordningen tillåter medlemsstaterna att lagstifta om. Detta förslag har mötts med både positiv och negativ kritik från de olika remissinstanserna.

Samtycket kommer att stärkas i förordningen, bland annat med hänsyn till det stärkta informationskravet och förtydligandet av vad som utgör en otvetydig viljeyttring. Då kravet på ett ”vanligt” samtycke förstärks innebär detta även att det uttryckliga samtycket, som exempelvis krävs för en behandling av känsliga personuppgifter, stärks genom förordningen.

För personuppgiftsansvariga innebär de ökade kraven i förordningen att de måste se över hur de lämnar information, vilka personuppgifter de hanterar och på vilka lagliga grunder dessa hanteras. Detta gäller särskilt i förhållande till de personuppgifter som hanterats med stöd av 5 a § PUL. Personuppgiftsansvariga måste även se över hur de inhämtar samtycken och att de uppfyller de krav som förordningen ställer då detta sker. Eftersom det är den personuppgiftsansvarige som ska visa att ett giltigt samtycke har lämnats kan det rekommenderas att samtycket ska lämnas skriftligt, även om samtycket inte har något formkrav.

Rättsläget för hur de nya reglerna om barns möjligheter att lämna samtycken är idag oklart. Personuppgiftsansvariga kommer enbart vara skyldiga att vidta rimliga åtgärder att verifiera att giltiga samtycken lämnats, men det är oklart vad som avses med rimliga åtgärder. Vidare är det, bland annat, oklart vad som kommer avgöra om en tjänst riktar sig direkt till barn. Det återstår att se om det svenska lagförslaget på att sänka åldern till 13 år består. Det kan ifrågasättas om barn är mogna nog att förstå innebörden av ett samtycke vid denna ålder samtidigt som de har rätt till självbestämmande och informationsfrihet. Åldersgränsen bör dock, enligt undertecknad, höjas till 15 år med hänsyn till barns möjlighet till en större mognad och förståelse än vad som kan förväntas vid 13 års ålder.

Förordningen kommer medföra ökade krav och ett ökat ansvar för personuppgiftsansvariga. Med hänsyn till de höga sanktionsavgifter som kan dömas ut om personuppgiftsansvariga inte efterlever de krav som ställs i förordningen så är det troligt att personuppgiftsansvariga kommer att tillse att nödvändiga åtgärder genomförs för att undvika rättsliga sanktionsavgifter. Förordningen kommer, bland annat genom informationskravet, även att ge registrerade ökade möjligheter att ta kontroll över hur deras personuppgifter hanteras. Det kommer dock vara upp till de registrerade att läsa och ta till sig den information som delges dem för att samtycket ska uppnå sin fulla effekt.

1 Inledning

Den 25 maj 2018 kommer den nya allmänna dataskyddsförordningen (vidare förordningen), EU 2016/679,¹ börja tillämpas såsom lag i Sverige. Förordningen upphäver det nuvarande gällande dataskyddsdirektivet (vidare direktivet) 95/46/EG² som reglerar rätten att behandla³ personuppgifter⁴ inom EU. I SOU 2017:39 har det lagts fram ett förslag om att upphäva den i Sverige gällande personuppgiftslagen (1998:204), PUL, som implementerade direktivet i svensk rätt, och ersätta PUL med en ny dataskyddslag som ska komplettera förordningen.⁵ Den nya förordningen har satt igång en omfattande process inom både privat och offentlig sektor för att säkerställa att organisationer, företag och myndigheter uppfyller de striktare regler som ska tillämpas genom förordningen samt för att undvika de strängare vitessanktioner som kommer att kunna tillämpas mot de som brister i ansvar.

Förordningens syften är att stärka den personliga integriteten och skyddet för fysiska personer vid behandlingen av deras personuppgifter, samt att säkerställa fri rörlighet för personuppgifter inom unionen.⁶ I skälen till förordningen har det påpekats att rätten till personlig integritet är en grundläggande mänsklig rättighet som bör respekteras oavsett medborgarskap eller hemvistland. Detta är av extra vikt eftersom den inre marknaden ökat sedan EU:s bildande och behandlingen av personuppgifter mellan olika aktörer har ökat markant. Även den tekniska utvecklingen och globaliseringen har bidragit till den ökade spridningen och användandet av personuppgifter inom såväl den privata som den offentliga sektorn.⁷

Utvecklingen har medfört att personuppgifter idag finns tillgängliga världen över och att de har blivit en värdefull valuta som inte sällan används som betalmedel på den digitala marknaden. Något så vardagligt som riktad reklam från en webbsida omfattar ett utbyte och en överföring av personuppgifter mellan olika företag för att, utefter individens preferenser, kunna ge ett riktat erbjudande.⁸

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning); På engelska: General Data Protection Regulation, förkortat GDPR.

² Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

³ Definieras i avsnitt 3.2.4.

⁴ Definieras i avsnitt 3.2.1

⁵ SOU 2017:39 *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*, s. 19.

⁶ Art. 1 och skäl 4 – 10 samt 166, 170, i allmän dataskyddsförordning (EU) 2016/679.

⁷ Skäl 1–6 i allmän dataskyddsförordning (EU) 2016/679.

⁸ Larsson, S. & Ledendal, J: *Personuppgifter som betalmedel*, Konsumentverkets rapport 2017:4, s. 9, 14–18.

Utvecklingen har enligt kommissionen medfört större risker för individens personliga integritet. Det krävs därmed striktare och mer harmoniserade regler kring hur personuppgifter inom EU får behandlas för att stärka skyddet av den personliga integriteten samt ge fysiska personer kontroll över sina personuppgifter.⁹ Redan Integritetskommittén diskuterade i sitt delbetänkande SOU 2016:41 problematiken kring att omfattande behandlingar av personuppgifter görs av flera aktörer på marknaden. I delbetänkandet påpekades även att detta har försvårat för den enskilde att ha kunskap om hur dennes uppgifter behandlas och att möjligheten att påverka hur uppgifterna behandlas ständigt har minskat.¹⁰ Den nya förordningen har som ambition att tjäna individen så att den återigen kan få kontroll över sina personuppgifter och stärka dennes rättsliga säkerhet.¹¹

Det är därför intressant att studera och granska förordningen i förhållande till den lagliga grund för behandling där den enskilde ska ha störst inverkan på vilka personuppgifter som behandlas, nämligen samtycket. Att försöka utröna hur reglerna förändras och huruvida en sådan förändring skulle kunna inverka på den enskildes rätt till personlig integritet, samt den potentiella påverkan på olika företag eller organisationer är också intressant.

1.1 Syfte och frågeställning

Uppsatsen har till syfte att granska samtycket enligt den allmänna dataskyddsförordningen i förhållande till personuppgiftslagen och dataskyddsdirektivet för att utröna huruvida samtyckets roll kommer att förstärkas genom förordningen och hur detta, i sådant fall, skulle kunna påverka registrerade och personuppgiftsansvariga i förordningen.

Syftet följer av följande frågeställningar:

- Har samtycket förstärkts genom förordningen och har i så fall den personuppgiftsansvariges ansvarsskyldighet utökats genom förordningen?
- Kommer registrerade genom samtycket att erhålla ett starkare skydd och en ökad kontroll över sina personuppgifter i enlighet med förordningens syfte?

1.2 Disposition

Arbetet ger först en presentation av ämnet, den personliga integriteten och grundläggande begrepp inom ämnet. Förståelsen för vad reglerna ska skydda är en grundläggande del av förståelsen av förordningen. Tillämpningsområdet är viktigt för att förstå innebörden av dess omfattning och i vilken utsträckning förordningen kan komma att påverka rättsläget. Därefter följer en presentation av de krav och villkor som den personuppgiftsansvarige ska uppfylla både före, under och efter en behandling av personuppgifter som är

⁹ Skäl 4–10 i allmän dataskyddsförordning (EU) 2016/679.

¹⁰ SOU 2016:41, s. 50 f.

¹¹ Skäl 4-10 i allmän dataskyddsförordning (EU) 2016/679.

essentiella för att kraven i förordningen ska uppfyllas. Kraven för hur giltiga samtycken ska lämnas beskrivs sedan närmare i detalj, innan arbetet utvecklar hur samtycke ska lämnas av barn och därefter i vilka situationer uttryckliga samtycken ska tillämpas. Löpande genom texten och inom de olika områdena finns hänvisningar till hur rätten har tillämpats och vilka krav som har ställs i PUL och direktivet för att ge en tydligare jämförelse mellan reglerna.

Sedan följer en analys av ämnet där en diskussion görs utifrån de krav som ställs i förordningen rörande samtycket och dess tillämpningsområde i förhållande till den personuppgiftsansvarige samt syftet för vilket förordningen tillkommit i förhållande till personuppgiftslagen. Här belyses eventuella oklarheter kring reglerna och vad en följd av dessa kan bli. Uppsatsen avslutas med en slutsats där ambitionen är att syftet och frågeställningen besvaras.

1.3 Avgränsningar

Arbetet fokuserar på de grundläggande reglerna kring samtycke och de krav som ställs i den allmänna dataskyddsförordningen för att giltiga samtycken ska kunna lämnas. Det belyses vilka rättigheter den enskilde erhåller genom samtycket samt vilka effekter det får för den som samlar in och behandlar personuppgifter. Eftersom arbetet berör samtyckets roll i förordningen omfattas även reglerna kring barns möjligheter att lämna giltiga samtycken. Med hänsyn till att arbetet generellt avser att utreda samtycket berörs inte mer specifika områden såsom hälsa, brottskämpning, rikets säkerhet eller vissa av de undantag som uppkommer vid myndigheters behandling av personuppgifter. Eftersom arbetet fokuserar på den allmänna dataskyddsförordningen omfattas inte speciallagstiftning såsom e-direktivet. Arbetet behandlar inte heller förordningens förhållande till yttrandefrihetslagstiftningen. De redogjorda avgränsningarna har, utöver skälen som redogjorts ovan, fått göras med hänsyn till arbetets begränsade omfattning.

1.4 Metod

Vid ett juridiskt arbete kan olika rättsvetenskapliga metoder vara omfattande och överlappa varandra. En metod inom rättsvetenskapen är den rättsdogmatiska metoden, men vad denna rent faktiskt omfattar är oklart. Denna problematik har lyfts fram av professor Claes Sandgren som framhåller att olika delar *kan* anses omfattas av denna metod, bland annat rättskälleläran samt forskares allmänna erfarenheter inom ett ämne.¹² Den klassiska rättskälleläran har ansetts bestå av lagtext, prejudicerande domar och förarbeten.¹³

¹² Sandgren, C., *Är rättsdogmatiken dogmatisk?*, Ingår i Tidsskrift for Rettsvitenskap, TtR, Vol. 118, nr 4-5, ; 2005, s. 648-656. s. 648 f., s. 652.

¹³ Peczenik, A., *Juridikens metodproblem: Rättskällelära och lagtolkning*, 2: a upplagan, Almqvist och Wikson, Stockholm, 1980, s. 49 f.

Det finns dock skilda åsikter huruvida doktrin och även övrig praxis ska falla under detta begrepp.¹⁴ Därav beskrivs istället metoden som använts i arbetet nedan fritt, med en grund i rättsdogmatiken.

Eftersom detta arbete omfattar ett ämne som både är gammalt och nytt, där den nya förordningen ännu inte trätt i kraft och tolkningar av denna från prejudicerande instanser saknas, har ett bredare område av källor använts. Till största del har den grundläggande informationen erhållits genom förordningens skäl. I förhållande till PUL har likvärdig information erhållits genom doktrin, lagkommentarer och förarbeten till lagen. Även Datainspektionens utlåtanden och material har använts då Datainspektionen är tillsynsmyndighet för behandling av personuppgifter inom Sverige.

För att kunna analysera hur och om förordningen kommer att påverka rättsläget samt den registrerades eller den personuppgiftsansvariges positioner, har även vetenskapliga artiklar och yttranden över den nya förordningen använts. Vidare har Kommissionens arbetsgrupp, art. 29-gruppen som presenteras nedan i avsnitt 1.5, riktlinjer och tolkningar av förordningen och direktivet använts för att uppnå syftet samt ge en bild av rättslagets utveckling. Den svenska tolkningen som gjorts av förordningen har främst underbyggts av dataskyddsutredningen i SOU 2017:39 som har lagt fram ett lagförslag på kompletterande svensk lagstiftning till förordningen. Även äldre utredningar har använts för att förstå PUL:s utveckling och tillämpning i det nuvarande rättsläget.

Vidare har 16 remissinstansers uttalanden inhämtats och sammanställts för att bland annat bidra till tolkningen och argumentationen kring giltiga samtycken för barn och för att belysa den nationella diskussionen rörande dessa regler i förhållande till de unionsrättsliga reglerna.

Eftersom förordningen utgör unionsrätt och framöver ska tolkas unionskonformt har det varit naturligt att underbygga arbetet till stor del på utlåtanden av EU-rättsliga organ, men även att inhämta artiklar samt yttranden från olika medlemsstater inom unionen. Prejudicerande rättsfall för direktivet, och därmed även PUL, har använts i arbetet eftersom förordningen har till avsikt att bygga vidare på direktivet. Rättsfallen har därmed ansetts ha en högre relevans rörande hur förordningen kan komma att tolkas och tillämpas.

1.5 Material

Majoriteten av det material som ligger till grund för detta arbete har utgivits på engelska och har inte funnits tillgängligt på svenska. Detta material har översatts av författaren under arbetets gång med beaktande av de svenska språkversionerna av den allmänna dataskyddsförordningen och dataskyddsdirektivet för en så konform och korrekt översättning som möjligt. Författaren reserverar sig emellertid för att felaktigheter kan förekomma.

¹⁴ Sandgren, C: Är rättsdogmatiken dogmatisk; 2005, s. 648 ff.

Arbetet bygger främst på förarbeten, de angivna skälen i förordningen som är avsedda att användas vid dess tolkning, lagkommentarer och doktrin. Det ska påpekas att skälen till förordningen inte alltid ger svar på hur samtliga begrepp i denna ska tolkas. Utgivna icke-bindande riktlinjer och tolkningar av art. 29-gruppen rörande tolkningen av dataskyddsdirektivet och dataskyddsförordningen har också utgjort ett grundläggande material i arbetet. Art. 29-gruppen är en arbetsgrupp som tillkom genom art. 29 i dataskyddsdirektivet. Gruppen har till syfte att utgöra ett skydd för enskilda. Den är sammansatt av en företrädare från varje tillsynsmyndighet i medlemsländerna, en företrädare för den, eller de, myndigheter som inrättats för gemenskapens institutioner och organ, samt en företrädare från Europeiska kommissionen. Gruppen ska vara rådgivande och oberoende, uppföra rekommendationer rörande databehandling och utreda frågor¹⁵ som rör tillämpningen av direktivet och förordningen. Art. 29-gruppens uttalanden är inte prejudicerande och reflekterar inte Europeiska kommissionens syn eller inställning.¹⁶ Dess icke bindande riktlinjer och uttalanden får, enligt undertecknad, dock anses utgöra viktiga hjälpmedel vid tolkningen av reglerna rörande datadirektivet och dataskyddsförordningen. Både nationella tillsynsmyndigheter, utredningar¹⁷ samt forskare på området hänvisar till Art. 29-gruppens uttalanden. Gruppens tolkningar av EU-rätten på detta område får därmed anses ge en god indikation på hur EU-rätten ska tillämpas och vad som krävs för att den ska uppfyllas.

Plattformen ”Better Internet for Kids” (BIK) arbetar, å Europeiska Kommissionens vägnar, med att skapa ett bättre och säkrare internet för barn och ungdomar. Deras uppdrag är att genom plattformen utbyta kunskap och resurser samt arbeta mot att barn och ungdomar ska få en större medvetenhet och kontroll över sin aktivitet online. Denna plattform har följt och utvärderat förordningen i de delar som den berör barns rättigheter och får därmed ses som en god källa på detta område.¹⁸

Vidare har även vetenskapliga artiklar och utgivna riktlinjer använts för att tolka förordningen och se vilka förändringar som denna har medfört. Artiklarna och de utgivna riktlinjerna som har använts är framtagna och utgivna av forskare som är verksamma på olika universitet i Europa respektive advokatbyråer inom Europa och har erhållits genom, bland annat, LUBsearch och Google Scholar. De får därmed anses ha relevans. Artiklarna har även belyst viss problematik som skulle kunna uppkomma genom förordningen. Det ska påpekas att en stor del av materialet är författat av forskare i olika medlemsstater inom EU eller medlemmar i EES. Detta har

¹⁵ Art. 29 i direktiv 95/46/EG.

¹⁶ Europeiska kommissionen, Article 29 Data Protection Working Party, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=59485>, (besökt 2017-12-20).

¹⁷ Se bl.a. SOU 2017:39 s. 138 där utredningen hänvisar till definitionen av särskilt och informerat samtycke som gjorts av art. 29-gruppen; Information Commissioners Office m.fl.

¹⁸ Better Internet for Kids, <<https://www.betterinternetforkids.eu/web/portal/about>>, (besökt 2017-12-22).

tagits i beaktande under arbetets gång. Att majoriteten av det material som har använts utgjort jämförelser mellan förordningen och direktivet har inte ansetts påverka materialets värde för arbetet då detta har bidragit med att klargöra skillnaderna mellan lagtexterna.

Rörande den nationella rätten och PUL har främst Sven Ömans och Hans-Olof Lindbloms kommentarer till PUL använts för tolkningen av lagen tillsammans med Datainspektionens material. Öman och Lindblom har hänvisats till i SOU 2017:39. Roger Petersson och Klas Reinholdsson har författat en något mer lättillgänglig kommentar rörande förståelsen av PUL och har bidragit med ytterligare en dimension av reglernas tolkning.

Eftersom det saknas domar rörande förordningen har de rättsfall som använts varit prejudicerande för antingen direktivet eller PUL. I och med att förordningen ska bygga vidare på direktivet får ändå de mest centrala rättsfallen anses ha betydelse för förordningen. Delar av EU-domstolens viktigaste avgöranden har kodifierats i förordningen och får därmed fortfarande anses ha en viktig betydelse vid tolkningen av denna.

Det ska även belysas att eftersom förordningen inte börjat tillämpas i skrivande stund har det funnits en begränsning av hur förordningen och dess regler har kunnat tolkas i de angivna materialen. Vissa tolkningsfrågor saknar alltså svar, framförallt rörande hur nya krav eller striktare lagstiftning ska tillämpas. Det ska även beaktas av läsaren att visst material inte har funnits att tillgå. Bland annat finns fortfarande möjligheten att, rörande art. 29-gruppens riktlinjer för samtycke i förordningen, lämna remissvar och ställa frågor rörande samtycket. Svaren på dessa har arbetsgruppen ännu inte hunnit publicera. Nationellt har inte propositionen rörande den föreslagna nya dataskyddslagen publicerats.

1.6 Forskningsläge

Forskningsläget på området är för närvarande expansivt. Det finns många artiklar och riktlinjer som är framtagna av advokatbyråer och forskare som publicerats på området. En mycket stor del av den doktrin som produceras på området är från olika medlemsstater inom EU och publiceras därför på engelska. Nationellt har Datainspektionen tagit fram riktlinjer rörande den allmänna dataskyddsförordningen och PUL. Det har även de senaste åren genomförts ett stort antal statliga utredningar rörande den personliga integriteten. SOU 2017:52 fokuserar exempelvis på hur den personliga integriteten ska stärkas i Sverige. Som en följd av dataskyddsförordningen, och även rättsläget i stort, har utredningar även genomförts för att stärka den personliga integriteten inom Rättsmedicinalverkets verksamhet (SOU 2017:80), för att harmonisera den svenska rätten med reglerna om lagring och integritet inom brottsväsendet (SOU 2017:75), för att reglera behandlingen av personuppgifter inom domstolsväsendet genom en ny Brottsdatalog (SOU 2017:74) samt harmonisera den svenska lagstiftningen rörande kamerabevakning med förordningen genom en ny lag på detta område (SOU 2017:55).

Jonas Ledendal vid Institutionen för handelsrätt vid Lunds universitet deltar i ett forskningsprojekt "Sjyst data!" med syftet att ta fram riktlinjer för kommersiell hantering och användning av data i förhållande till dataskyddsförordningen. Projektet fokuserar även på hur användardata utgör valuta på den digitala marknaden.¹⁹ Rörande barns roll i dataskyddsförordningen kan denna reglering följas genom Europa kommissionens projekt BIK. På deras hemsida publiceras artiklar och det går att ytterligare fördjupa sig inom ämnet. Rörande konceptet "risk" i förordningen har Milda Macenaite publicerat en artikel på området. Orla Lynskey har i en artikel rörande den nytillkomna rättigheten till dataportabilitet utrett vilka konsekvenser denna kan få på området. Sahkila Bu-Phasa har publicerat en utredande artikel om vilken effekt förordningen kan få på sådana överföringar av uppgifter som görs till tredje land.

Förutom det extensiva lagarbetet samt de många artiklar som publiceras inom olika delar av ämnet ska det belysas att även art. 29-gruppen fortsatt kommer utreda och publicera tolkningar av förordningen. Vidare sker även nu en revidering av e-dataskyddsdirektivet²⁰ som ska ersättas av e-skyddsförordningen²¹. Även denna kommer därmed bli direkt tillämplig i svensk rätt. E-skyddsförordningen är *lex specialis* till den allmänna dataskyddsförordningen och förhållandet häremellan är ett område som vore värt att närmre undersöka.

¹⁹ Se <<https://www.acreo.se/Sjyst-data-personlig-integritet-affarsnytta> och [http://portal.research.lu.se/portal/sv/projects/sjyst-data\(360314a3-0e43-4fb2-a0ea-46539bcf7a33\).html](http://portal.research.lu.se/portal/sv/projects/sjyst-data(360314a3-0e43-4fb2-a0ea-46539bcf7a33).html)>, (besökt: 2017-12-22).

²⁰ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation.).

²¹ För mer information och för att se förslaget: <<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>>.

2 Grundläggande regler och rättigheter

2.1 Inledning

Förordningen grundar sig ursprungligen i den grundläggande rätten för den enskildes skydd av den personliga integriteten vid behandlingar av dennes personuppgifter.²² Denna rätt är erkänd i den Europiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) samt Europeiska unionens stadga om de grundläggande rättigheterna (EU-stadgan).²³ Möjligheten för den registrerade att lämna sitt samtycke som en laglig grund för en behandling av personuppgifter erkänns i EU-stadgan.²⁴

2.2 Internationell och nationell rätt

EKMR är inkorporerad i svensk rätt.²⁵ Den berör inte direkt behandlingen av personuppgifter men sådan behandling anses ändå kunna falla inom tillämpningsområdet för art. 8 i EKMR vilken reglerar rätten till skydd för den enskildes privat- och familjeliv. Artikeln ska alltså beaktas vid tillämpningen av nationella regler rörande personuppgifter. Vikten av den enskildes skydd rörande behandlingar av dennes personuppgifter har av Europarådet även befasts, utöver EKMR, genom Dataskyddskonventionen som har antagits av EU:s samtliga medlemsländer.²⁶ Dataskyddskonventionen ställer krav på hur personuppgifter får inhämtas och på att de ska vara relevanta i förhållande till det syfte de samlas in för.²⁷

I EU-stadgan regleras rätten till privatliv i art. 7 medan det i art. 8 framgår att varje enskild person har rätt till skydd av de personuppgifter som berör denne. EU-domstolen har uttalat att varje behandling av en enskilds personuppgifter därmed, i princip, ska utgöra ett intrång i den enskildes rätt till privatliv och

²² Díaz Díaz, E., *The new European Union General Regulation on Data Protection and the legal consequences for institutions*, in Church, Communication and Culture, 1:1, 206-239, Informa UK Limited, Taylor & Francis Group, publicerad 2016-10-27, s. 215 f. <<https://doi.org/10.1080/23753234.2016.1240912>>, (besökt: 2017-12-20).

²³ SOU 2017:39, s. 65 f.

²⁴ Macenaite, M. & Kosta, E., *Consent for processing children's personal data in the EU: following in the US footsteps?* in Information & Communications Technology Law, 26:2, 146-197 Informa UK Limited, Taylor & Francis Group, publicerad: 2017-05-10, s. 156, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-20)

²⁵ Öman, S. och Lindblom, H., *Personuppgiftslagen – en kommentar*, 4:e upplagan, Vällingby, 2011, s. 65 f.

²⁶ SOU 2017:39, s. 65 f.

²⁷ Petersson, R. och Reinholdsson, K., *Personuppgiftslagen i praktiken*, 5:e upplagan, Norstedts juridik, Vällingby, 2012, s.33.

till skydd av sina personuppgifter.²⁸ I art. 8 framgår det dock även att personuppgifter får behandlas i enlighet med bestämda ändamål och om behandlingen är grundad på den enskildes samtycke. Den enskilde ska vidare ha rätt att få tillgång till sina personuppgifter samt kunna begära att få dessa rättade.²⁹

Rätten till personlig integritet, och erkännandet av samtycket såsom en rättslig grund för att göra intrång i den personliga integriteten finns även uttryckt i svensk grundlag genom 2 kap. 6 § 2 st. regeringsformen (RF). Regeln infördes år 2010 för att uttryckligt stärka den personliga integriteten för enskilda även i svensk rätt.³⁰

2.3 Vad avses med personlig integritet?

I art. 8 EKMR, art.7 och 8 i EU-stadgan samt 2 kap 6 § 2 st. RF framgår att det är den personliga integriteten, eller privatlivet, som ska skyddas. Begreppet *personlig integritet* saknar emellertid en klar och tydlig definition eftersom skyddet av den privata sfären inte är absolut. Finns det andra grundläggande rättigheter som skulle väga tyngre än rätten till personlig integritet får den senare ge vika. Begreppet *personlig integritet* är även subjektivt och kan ges olika betydelser beroende på religion, politik eller samhällsstrukturer.³¹ I SOU 2016:41, *Hur står det till med den personliga integriteten*, framhöll integritetskommittén svårigheten med att definiera begreppet och att flera länders rättsordningar saknar en definition av detta.³² Kommittén beskrev hur begreppet ofta handlar om den enskildes rätt att själv kunna bestämma och kontrollera hur dennes personliga information används, sprids eller behandlas. Kommittén framhöll emellertid även att *personlig integritet* i andra fall kan handla om rätten till skydd mot insyn i det som omfattar ”*jaget*” och det privata livet. Den framhöll även svårigheten med att bedöma när en enskild uppgift kan gå från att vara oskyldig till att bli känslig för den enskilde om uppgiften lämnas ut och kan kopplas samman med andra uppgifter.³³

Integritetskommittén hänvisade till utredningen som gjordes i SOU 2004:6, *Översyn av personuppgiftslagen*.³⁴ I SOU 2004:6, som fokuserade på automatiserad behandling, framhölls att några av de viktigaste faktorerna rörande begreppet personlig integritet är hur personuppgifter samlas in, vad syftet med deras behandling är, vem som behandlar dem och i vilken omfattning de samlas in.³⁵ Integritetskommittén konstaterade tillslut att den

²⁸ C-297/12, *Michael Schwarz mot Stadt Bochum*, EU:C:2013:670, p. 25–26.

²⁹ SOU 2017:39, s. 67 och art. 8 EU-stadgan.

³⁰ Holmberg, E. mfl. Regeringsformen, kommentaren till 2 kap. 6 §, Zeteo, publicerad 2016-05-13, (besökt: 2017-09-27).

³¹ SOU 2004:6, *Översyn av personuppgiftslagen*, s. 27 ff.

³² SOU 2016:41, *Hur står det till med den personliga integriteten*, s. 147.

³³ SOU 2016:41, s. 136 – 139.

³⁴ SOU 2016:41 s. 145.

³⁵ SOU 2004:6, s. 27 ff.

delade slutsatsen som lagts fram i Ds 1994:51 i vilken det framgår att begreppet personlig integritet ska omfatta:

(...) vad som normalt framstår som angeläget att värna om för att den enskilde ska vara tillförsäkrad en rimlig, fredad, privat zon.

Vidare framhöll integritetskommittén att ett intrång i den personliga integriteten måste bedömas i det enskilda fallet utifrån, exempelvis, syftet och behovet av det aktuella intrånget samt vilken inverkan intrånget haft på den enskilde.³⁶

³⁶ SOU 2016:41 s. 147 ff.

3 Grundläggande om dataskyddsförordningen i förhållande till PUL

3.1 Bakgrund

Dataskyddsdirektivet (direktivet) tillkom med syftena att säkra den fria rörligheten av personuppgifter inom unionen och att skydda rätten till privatlivet i art. 8 EKMR. Detta skulle ske genom att skyddsnivån för fysiska personers fri- och rättigheter skulle vara likvärdiga i samtliga medlemsstater. Vidare skulle direktivet förstärka datakonventionen.³⁷ Implementeringen av direktivet har dock inte ansetts uppnå önskat resultat. Istället har det skapats en rättsosäkerhet inom EU som beror på ett bristande likvärdigt och harmoniserat skydd för personuppgifter mellan medlemsstaterna. De grundläggande syftena och de grundläggande målen med direktivet kvarstår därmed i den allmänna dataskyddsförordningen (förordningen) men denna ska på en unionsrättslig nivå harmonisera reglerna och även stärka skyddet för den enskilde.³⁸

Eftersom förordningen upphäver direktivet har det i SOU 2017:39 lagts fram ett förslag på att även upphäva PUL. I förordningen kommer det att finnas möjligheter till viss kompletterande nationell lagstiftning för medlemsstaterna.³⁹ I Sverige har det därmed i samband med förslaget att upphäva PUL även lagts fram ett förslag på en ny kompletterande dataskyddslag som ska införas och träda i kraft i samband med förordningen.⁴⁰

3.2 Materieellt tillämpningsområde

Förordningen ska som huvudregel tillämpas på alla behandlingar av personuppgifter som genomförs, oavsett om behandlingen är automatiserad eller manuell. Förordningen ska alltså vara teknikneutral.⁴¹ Detta är inte någon förändring i förhållande till direktivet.⁴² Även PUL har varit teknikneutral och omfattat alla behandlingar oavsett om de varit automatiska eller inte.⁴³ Av art. 2.2 i förordningen framgår att en behandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som rör allmän säkerhet ska falla utanför förordningens tillämpningsområde. Detsamma

³⁷ Skäl 8 – 11 i dir. 95/46/EG.

³⁸ Skäl 4 – 10 och 170 i allmän dataskyddsförordning (EU) 2016/679.

³⁹ Skäl 10 i allmän dataskyddsförordning (EU) 2016/679.

⁴⁰ SOU 2017:39, s. 72 – 78;

⁴¹ Skäl 15 i allmän dataskyddsförordning (EU) 2016/679.

⁴² Skäl 27 i dir. 95/46/EG.

⁴³ Se 3 § PUL, definitionen av ”behandling”.

gäller om behandlingen utförs av en fysisk person i en privat verksamhet eller om behandlingen utförs av en fysisk person och behandlingen har en koppling till dennes hushåll.⁴⁴ En begäran om att få ut ett stort antal känsliga, och eventuellt integritetskränkande, personuppgifter med motiveringen att de enbart ska användas för privat bruk har dock inte accepterats som privat verksamhet med hänsyn till den personliga integriteten i PUL.⁴⁵

3.2.1 Personuppgifter

Det framgår av art. 4.1 i förordningen att denna omfattar och är tillämplig på alla personuppgifter som är direkt eller indirekt hänförliga till identifierbara fysiska personer (vidare registrerade). Förordningen är däremot inte tillämplig på avlidna personer⁴⁶. I de fall uppgifter om den avlidne kan kopplas till en levande person, såsom en familjemedlem, kan uppgiften ändå utgöra en sådan personuppgift som ska omfattas av förordningen eftersom uppgiften är en personuppgift om familjemedlemmen. Så kan vara fallet om uppgifterna rör information om, exempelvis, en viss nedärvd sjukdom.⁴⁷ Personuppgifter om avlidna personer har inte heller omfattats av PUL, men personuppgifter som har rört, exempelvis, levande släktingar har omfattats.⁴⁸ Tillämpningsområdet är alltså likvärdigt i både förordningen och PUL.

En personuppgift är en sådan uppgift eller sådan information som, genom en hänvisning, kan identifiera en enskild person.⁴⁹ Vid bedömningen av vilka uppgifter som kan anses vara personuppgifter ska det beaktas om det finns fler uppgifter att tillgå om den enskilde som gemensamt kan identifiera den registrerade.⁵⁰ Dessa uppgifter behöver inte enbart innehas av den som ska genomföra behandlingen, utan de kan även finnas hos en annan person.⁵¹ Är så fallet ska uppgifterna bedömas såsom personuppgifter och omfattas av förordningen.⁵² Vid bedömningen ska hänsyn även tas till vilka rimliga hjälpmedel som kan användas för att direkt, eller indirekt, genom uppgiften identifiera en enskild person. Vilka rimliga hjälpmedel som kan användas ska bedömas utifrån vilken kostnad och tidsåtgång det skulle ta att använda dem, men även utifrån vilken tillgänglig teknik som finns att tillgå vid tidpunkten för behandlingen. Hänsyn ska även tas till den tekniska utvecklingen.⁵³

⁴⁴ Art. 2 och skäl 14 – 18 i allmän dataskyddsförordning (EU) 2016/679.

⁴⁵ NJA 2015 s. 180.

⁴⁶ Skäl 27 i allmän dataskyddsförordning (EU) 2016/679.

⁴⁷ Voigt, P. och von dem Bussche, A., *The EU General Data Protection Regulation (GDPR) – A practical guide*, Springer International Publishing, Switzerland, 2017, s. 11.

⁴⁸ Petersson och Reinholdsson s. 49 f.; Öman och Lindblom, personuppgiftslagen, kommentaren till 3 §, Zeteo, (besökt 2017-09-12).

⁴⁹ Skäl 26 i allmän dataskyddsförordning (EU) 2016/679.

⁵⁰ Voigt and von dem Bussche, s. 12.

⁵¹ C-582/14, *Patrick Breyer mot. Bundesrepublik Deutschland*, EU:C:2016:779, punkt 43.

⁵² Voigt and von dem Bussche, s. 12.

⁵³ Art. 4.1 och skäl 26 i allmän dataskyddsförordning (EU) 2016/679.

Uppgifter såsom namn, telefonnummer, fritidsintressen⁵⁴, lokaliseringssuppgifter, IP-nummer⁵⁵, foton⁵⁶ och videor har ansetts utgöra personuppgifter.⁵⁷ Vidare ska uppgifter som är specifika för den registrerade, såsom fysiska⁵⁸, genetiska, ekonomiska, kulturella eller psykiska, utgöra personuppgifter.⁵⁹ Anonymiserade uppgifter omfattas däremot inte av förordningen.⁶⁰ Med anonymiserade uppgifter avses sådana personuppgifter som inte har någon koppling till den enskilde individen, antingen för att uppgifterna inte går att koppla till en enskild individ eller för att uppgifterna gjorts omöjliga att koppla till en enskild individ.⁶¹ Anonymiseringen ska alltså göra det omöjligt att finna en enskild individ i ett material. Att enbart radera data är därmed inte alltid tillräckligt.⁶² Går uppgifterna att återskapa bedöms dessa alljämt som personuppgifter enligt förordningen.⁶³

Sammantaget kvarstår definitionen av personuppgifter såsom mycket bred och omfattande.⁶⁴

3.2.2 Känsliga personuppgifter

Känsliga personuppgifter är sådana uppgifter som vid en behandling kan innebära betydande risker för de grundläggande fri- och rättigheterna. Dessa ska alltså utifrån sin natur ges ett förstärkt skydd.⁶⁵ Vad som utgör känsliga personuppgifter anges i förordningens art. 9.1 och i artikeln anges att uppgifter som avslöjar ras⁶⁶ eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och behandling av genetiska eller biometriska uppgifter samt uppgifter om en fysisk persons hälsa, sexualliv eller sexuella läggning.⁶⁷ Vid tillämpningen av PUL har uppgifter om namn och språkkunskap tillsammans kunnat utgöra upplysningar om en persons etniska ursprung. Rörande politiska åsikter har själva avslöjandet av en åsikt ansetts vara känsligt, medan det rörande

⁵⁴ C-101/-01, *Lindqvist mot Åklagarkammaren i Jönköping*, EU:C:2003:596, p. 27.

⁵⁵ C-70/10, *Scarlet Extended SA mot Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, EU:C:2011:771, p. 50–51 (statiska IP-adresser); C-582/14, *Patrick Breyer mot. Bundesrepublik Deutschland*, EU:C:2016:779. 46–47 (dynamiska IP-adresser).

⁵⁶ Skäl 51 i allmän dataskyddsförordning (EU) 2016/679.

⁵⁷ Voigt och von dem Bussche, s. 11.

⁵⁸ Fingeravtryck har ansetts utgöra personuppgifter, se C-297/12, *Michael Schwarz mot Stadt Bochum*, EU:C:2013:670, p. 27.

⁵⁹ Art. 4.1 i allmän dataskyddsförordning (EU) 2016/679.

⁶⁰ Skäl 26 i allmän dataskyddsförordning (EU) 2016/679.

⁶¹ Voigt och von dem Bussche, s. 11.

⁶² Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN, WP216, s. 9.

⁶³ Voigt och von dem Bussche, s. 14.

⁶⁴ Koščik, M., *The Impact of General Data Protection Regulation on the grey literature*, Grey Journal (TGJ), s. 42-45, publicerad 2017-01-02, s. 42, <<http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/pdfviewer/pdfviewer?vid=2&sid=2409e5df-3839-43b2-bae6-c75f9be047a9@pdc-v-sessmgr01>>, (besökt 2017-12-07).

⁶⁵ Skäl 51 i allmän dataskyddsförordning (EU) 2016/679.

⁶⁶ Som anges i skäl 51 i allmän dataskyddsförordning (EU) 2016/679: "(...) användningen av termen ras (...) inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser."

⁶⁷ Art. 9.1 i allmän dataskyddsförordning (EU) 2016/679.

religiösa övertygelser har ansetts vara avslöjandet av själva övertygelsen. Genetisk information har inte omnämnts i 13 § PUL, men har ändå omfattats av lagen eftersom dessa uppgifter har ansetts kunna avslöja både hälsotillstånd och etnicitet.⁶⁸ Regeringsrätten framförde även i RÅ 2008 ref. 83 att biometriska uppgifter, som inte heller omnämns i 13 § PUL, ska omfattas av PUL såsom känsliga personuppgifter.

3.2.3 Personuppgiftsansvarig

Förordningen ska tillämpas och efterföljas av den som behandlar personuppgifter. Den som behandlar personuppgifter ansvarar för behandlingen och kallas för *personuppgiftsansvarig*. Den personuppgiftsansvarige kan vara både en fysisk eller juridisk person, men även en myndighet eller förening. Är den personuppgiftsansvarige ett företag ansvarar företaget för alla behandlingar som sker inom den egna verksamheten. Vidare är det den personuppgiftsansvarige som avgör syftet och medlen för behandlingen.⁶⁹ Den som utvecklat och tillhandahåller en hemsida där personuppgifter laddas upp och sedan överförs till en annan mottagare är exempelvis personuppgiftsansvarig för personuppgifterna eftersom denne bestämmer syftet med hemsidan och medlen för behandlingen.⁷⁰ Görs detta tillsammans med annan ska båda parterna gemensamt ses som personuppgiftsansvariga.⁷¹

I förordningen har den personuppgiftsansvariges ansvar utökats med ett nytt krav att denne ska ansvara för och kunna visa på att denne följer de principer som ställs i förordningen. Den personuppgiftsansvarige ska även kunna säkerställa att den registrerades rättigheter skyddas.⁷² Det är exempelvis den personuppgiftsansvarige som har bevisbördan för att ett giltigt samtycke har lämnats (art. 7.2) och det är den personuppgiftsansvarige som ska visa på att denne uppfyller kraven i art. 5.⁷³ Förordningen innehåller även, till skillnad från direktivet, en skyldighet för tillsynsmyndigheter att utdöma sanktionsavgifter på upp till 20 miljoner euro, eller 4 % av organisationens omsättning, när den personuppgiftsansvarige inte uppfyller kraven på behandlingar av personuppgifter. Motsvarande sanktioner har inte funnits i direktivet.⁷⁴ Förordningen uppmanar även till att sanktionerna ska vara effektiva, proportionerliga och avskräckande.⁷⁵

Förordningen är även tillämplig på *personuppgiftsbiträden*. Ett personuppgiftsbiträde är den som behandlar personuppgifter på uppdrag av

⁶⁸ Öman och Lindblom, personuppgiftslagen, kommentaren till 13 § PUL, Zeteo, (besökt: 2017-11-20); jfr. SOU 2017:39, s. 161.

⁶⁹ Voigt och von dem Bussche, s. 17 f.

⁷⁰ Datainspektionen, *Beslut efter tillsyn enligt personuppgiftslagen (1998:204) dnr. 706–2006*; jfr C-131/12, *Google Spain SL och Google Inc. mot Agencia Espanola de Protección de Datos (AEPD) och Mario Costeja González*, EU:C:2014:317.

⁷¹ Voigt och von dem Bussche, s. 17 f.

⁷² SOU 2017:52, *Så stärker vi den personliga integriteten*, s. 64.

⁷³ Jfr. art. 5 och art. 7.2 i allmän dataskyddsförordning (EU) 2016/679.

⁷⁴ SOU 2017:52, s. 72.

⁷⁵ Art. 83 i allmän dataskyddsförordning (EU) 2016/679.

en personuppgiftsansvarig.⁷⁶ Mellan personuppgiftsansvariga och personuppgiftsbiträden ska det finnas avtal som reglerar förhållandet mellan dem.⁷⁷

3.2.4 Behandling

En behandling definieras i förordningens i art. 4.2 såsom:

en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. överföring, lagring, användning, bearbetning eller ändring, begränsning eller radering av personuppgifter.

Definitionen ska ha en sådan extensiv tolkning att även en mindre mängd personuppgifter, som enbart behandlas under kort tid, ska omfattas av förordningen.⁷⁸

3.2.4.1 Automatisk behandling

En automatisk behandling avser alla former av behandlingar som genomförs med, eller med hjälp av, ett datasystem eller en annan form av tekniskt hjälpmedel såsom mobiltelefoner eller annan ”smart” teknik. Även en behandling som är *delvis automatiserad* omfattas av begreppet. Behandlingen är delvis automatiserad när personuppgifter samlas in manuellt med syftet att föra in och registrera uppgifterna i ett elektronisk format. Det kan även vara andra delar av behandlingen som utförs av manuellt.⁷⁹ I förhandsavgörandet C101/01, *Lindqvist*, fastslog EU-domstolen att handlingen att föra över och lägga ut personuppgifter på internet ska utgöra en delvis automatiserad behandling.⁸⁰ EU-domstolen har vidare fastslagit i mål C-131-12, *Google Spain*, att när en sökmotor sorterar, samlar ihop och delger personuppgifter ska detta anses utgöra en automatisk behandling av den som tillhandahåller sökmotorn, inte den som gör sökningen.⁸¹

⁷⁶ Voigt och von dem Bussche, s. 17.

⁷⁷ Gabel, D. och Hickman, T., *Unlocking the EU General Data Protection Regulation*, White & Case, 2016, s. 63-67.

⁷⁸ Voigt och von dem Bussche, s. 9 f; Gabel och Hickman, White & Case, s. 20; SOU 2017:39, s. 90.

⁷⁹ Voigt och von dem Bussche, s. 10; Petersson och Reinholdsson, s. 68.

⁸⁰ C101/01 *Lindqvist mot Åklagarkammaren Jönköping*, EU:C:2003:596, p. 23 – 27.

⁸¹ C-131/12, *Google Spain SL och Google Inc. mot Agencia Espanola de Protección de Datos (AEPD) och Mario Costeja González*, EU:C:2014:317, p. 41.

3.2.4.2 Manuell behandling

Till skillnad från automatiska behandlingar omfattas inte alla manuella behandlingar av förordningen. Endast en sådan manuell behandling där de personuppgifter som behandlas ingår i, eller är avsedda att ingå i, ett register faller inom tillämpningsområdet. Registret ska vara ordnat efter särskilda kriterier.⁸² Registret ska alltså vara systematiskt och organiserat i vissa särskilda kategorier utifrån specifika kriterier. Vad som avses med specifika kriterier framgår dock inte av förordningen.⁸³ Kravet på att registret ska vara ordnat utefter specifika krav är emellertid identiskt med motsvarande reglering i 5 § PUL. I PUL har kravet på ”specifika kriterier” tolkats, med stöd av direktivet, såsom att registret ska vara sökbart utifrån de personuppgifter som förvaras i registret. Det ska alltså gå att söka fram en enskild person genom att sökningen görs på dennes personuppgifter.⁸⁴ Voigt och von dem Bussche har ansett att de register som är kronologiska, alfabetiska eller kategoriserade utefter förbestämda kriterier ska kunna utgöra sådana specifika kriterier att de ska omfattas av förordningen.⁸⁵

I PUL har ett register, utöver att uppfylla kraven på att registret ska vara strukturerat, ansetts behöva ha någon form av varaktighet för att kunna omfattas av tillämpningsområdet. Lösa papper som tillfälligt förvarats i en strukturerad och sökbar hög på ett bord har därmed inte omfattas av PUL.⁸⁶ Eftersom förordningen ställer krav på att personuppgifterna ska finnas i ett register⁸⁷ torde detta gälla även framöver.

3.2.4.3 Missbruksregeln, 5 a § PUL

En förändring i svensk rätt blir att den så kallade missbruksregeln i 5 a § PUL, försvinner i och med införandet av förordningen.⁸⁸ Missbruksregeln infördes i PUL år 2007 för att, med hänsyn till den tekniska utvecklingen i samhället, underlätta den vardagliga behandlingen av personuppgifter. Missbrukregeln har varit uppbyggd på så sätt att de behandlingar som har fallit under dess tillämpningsområde inte har behövt uppfylla kraven i PUL på att, bland annat, en behandling enbart får ske med stöd av en rättslig grund⁸⁹. Istället har behandlingen fått genomföras så länge den personliga integriteten inte har kunnat kränkas genom behandlingen.⁹⁰

Missbruksregeln har varit tillämplig på behandlingar av sådana personuppgifter som inte har ingått i, eller varit avsedda att ingå i, en

⁸² Skäl 15 i allmän dataskyddsförordning (EU) 2016/679.

⁸³ Voigt och von dem Bussche, s. 10.

⁸⁴ Öman och Lindblom, s. 124 ff.

⁸⁵ Voigt och von dem Bussche, s. 10.

⁸⁶ Öman och Lindblom, s. 124 ff.

⁸⁷ jfr. skäl 15 i allmän dataskyddsförordning (EU) 2016/679.

⁸⁸ Dataskyddsinspektionen, *Missbruksregeln upphör*, uppdaterad 2017-02-23, <<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsförordningen/missbruksregeln-upphor/>>, (besökt: 2017-09-11).

⁸⁹ Bestämmelserna i §§ 9, 10, 13–19, 21–26, 28, 33, 34 och 42 PUL är alla undantagna då missbruksregeln är tillämplig.

⁹⁰ Öman och Lindblom, personuppgiftslagen, kommentaren till 5 a §, Zeteo, publicerad 2016-12-20, (besökt: 2017-09-12).

strukturerad samling med syftet att påtagligt underlätta sökningen av personuppgifterna. Genom sin natur har den därmed enbart omfattat ostrukturerade automatiska behandlingar eftersom ostrukturerade manuella behandlingar redan varit undantagna från PUL.⁹¹ Som huvudregel har personuppgifter i regelrätta register eller databaser inte ansetts omfattas av missbruksregelns undantag medan övriga automatiska behandlingar har omfattats.⁹² I de fall personuppgifterna har ingått i sökbara register eller databaser, men sökfunktionen inte varit kopplad till personuppgifterna utan annan information, har ändå missbruksregeln ansetts tillämplig på dessa register då personuppgifterna inte har ansetts varit tydligt markerade i registret.⁹³

Vidare har det ställts ytterligare krav på de strukturerade registren då de behövt uppnå en viss kvalité eller ha ett visst värde för att inte omfattas av missbruksregelns tillämpningsområde.⁹⁴ Ett ärende- eller dokumenthanteringssystem som påtagligt underlättat sökningen av personuppgifter har exempelvis ansetts uppnå detta krav, medan personuppgifter som funnits tillgängliga i en lista på en webbsida inte har ansetts uppnå sådan kvalité att listan har ansetts utgöra ett strukturerat register. Inte heller personuppgifter som har figurerat i e-postkonton eller i enskilda dokument sparade på lokala filer på en hårddisk har ansetts vara sådana strukturerade register att de inte omfattats av missbruksregeln.⁹⁵

I de fall behandlingar har undantagits enligt 5 a § PUL har den personuppgiftsansvarige inte behövt inhämta samtycke för en behandling eller lämna information till den registrerade om att en behandling har skett. Den personuppgiftsansvarige har inte heller omfattats av skyldigheten att på begäran av den registrerade rätta personuppgifter eller omfattats av förbudet att föra över personuppgifter till tredje land. Detta har gjort att den enskilde inte har kunnat motsätta sig en behandling av sina personuppgifter. I de fall en behandling har haft till syfte att falla under missbruksregeln, och därmed undvika de striktare reglerna i PUL, har denna alltid ansetts som kränkande för den enskilde och behandlingen har brutit mot gällande rätt. Vid bedömningen härvid, om en kränkning av den personliga integriteten har förekommit för den enskilde i samband med en behandling som fallit under missbruksregeln, har syftet med behandlingen, spridningen av den enskildes uppgifter och sammanhanget som behandlingen genomförts inom varit viktiga faktorer vid bedömningen. Som en regel har behandlingar som uppfyllt kraven på grundläggande behandling (9 §) och laglig grund (10 §) i PUL, fastän de varit undantagna från att uppfylla dessa krav, inte kunnat anses såsom kränkande för den enskilde.⁹⁶

⁹¹ Öman och Lindblom, s. 130 ff.

⁹² Petersson och Reinholdsson, s. 72 ff.

⁹³ SOU 2004:6 s. 128 f.

⁹⁴ Petersson och Reinholdsson, s. 72 ff.

⁹⁵ Petersson och Reinholdsson, s. 72 ff.

⁹⁶ Öman och Lindblom, s. 146 ff.

När missbruksregeln försvinner kommer detta innebära att kravet på att det ska finnas en laglig grund för behandling bli tillämpligt för samtliga automatiserade behandlingar.⁹⁷ För myndigheter finns det emellertid ett förslag som har lagts fram i SOU 2017:39 som ska ge myndigheter möjligheten att fortsatt tillämpa en ny ”missbruksregel.” För myndigheter ska det vara rättsligt att hantera känsliga personuppgifter när detta är *absolut nödvändigt* så länge behandlingen inte utgör ett intrång i den personliges integritet och så länge personuppgifterna inte är sökbara.⁹⁸ Användandet av begreppet *absolut nödvändigt* har dock ifrågasatts av Datainspektionen och Kungliga Tekniska Högskolan. Detta eftersom denna nya missbruksregel bygger på art. 9.2 (g) i förordningen som ger rätten att hantera känsliga personuppgifter när det finns ett *viktigt allmänt intresse*. Valet att använda begreppet *absolut nödvändigt*, menar remissinstanserna, kan därför medföra att det blir oklart för personuppgiftsansvariga vad som krävs för att uppfylla kravet.⁹⁹

3.3 Territoriellt tillämpningsområde

PUL, i enlighet med datadirektivet, har byggt på *etableringsprincipen*. Definitionen av etablering är unionsgemensam och en verksamhet anses etablerad i en medlemsstat när den är en ”*effektiv och faktisk verksamhet med hjälp av en stabil struktur.*”¹⁰⁰ Förordningen bygger dock på två alternativa principer, *etableringsprincipen* och *effektlandsprincipen*. Effektlandsprincipen är nytillkommen och kommer att medföra att förordningen blir tillämplig för personuppgiftsansvariga även från länder utanför EU. Det krävs endast att en av principerna är uppfylld för att förordningen ska vara tillämplig.¹⁰¹

3.3.1 Etableringsprincipen

PUL har varit generellt tillämplig på behandlingar som utförs av en verksamhet som är etablerad i Sverige, oavsett om själva behandlingen utförts i Sverige eller i annan medlemsstat. I de fall verksamheten har varit etablerad inom flera medlemsstater har tillämplig lag varit den inom vilken medlemsstat som behandlingen har genomförts. Vilken lag som skulle ha varit tillämplig om samma behandling utförts av olika personuppgiftsansvariga i olika medlemsstater, men inom samma verksamhet som ansetts etablerad i båda medlemsstaterna, har dock varit oklart.¹⁰²

⁹⁷ Datakyddsinspektionen, *Missbruksregeln upphör*, <<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/>>, (besökt: 2017-09-12).

⁹⁸ SOU 2017:39, s. 42 och 177–182.

⁹⁹ Håkansson, Eva och Harnesk, Ulrika m.fl., Datainspektionen, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag*, 2017, s. 11 – 15; Karlsson, S., KTH, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag*, 2017.

¹⁰⁰ Öman och Lindblom, s. 166.

¹⁰¹ Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39), s. 3 f.

¹⁰² Öman och Lindblom, s. 117.

Förordningen kommer fortsatt vara tillämplig på de behandlingar som utförs av en personuppgiftsansvarig genom *etableringsprincipen* när verksamhetsstället är etablerat i unionen.¹⁰³ I den svenska språkversionen framgår det att detta ska gälla oavsett om behandlingen sker inom unionen eller inte. I den kompletterande promemorian till SOU 2017:39 framhålls emellertid att detta är en inkorrekt översättning i jämförelse med andra språkversioner¹⁰⁴. Förordningen är avsedd att enbart tillämpas på de behandlingar som sker inom en verksamhet som bedrivs i unionen och på de verksamhetsställen som är etablerade inom unionen. Är den personuppgiftsansvarige etablerad både inom unionen och i tredje land ska alltså behandling som utförs inom den verksamhet som bedrivs vid verksamhetsstället i tredje land inte omfattas av förordningen.¹⁰⁵

Begreppet etablering har i direktivet givits en extensiv tolkning av EU-domstolen vilket fortsatt bör vara gällande även i förordningen.¹⁰⁶ Utövande av all verklig, effektiv och faktiskt verksamhet, även om minimal och i vissa fall av en ensam representant, med hjälp av en stabil struktur uppfyller etableringskravet. Vad som är en stabil struktur och en bedriven verksamhet påverkas av verksamhetens och tjänstens specifika karaktär.¹⁰⁷ Voigt och von dem Bussche framhåller exempelvis att företag som exklusivt erbjuder sina tjänster online måste anses vara etablerade i de länder som företaget riktar sig emot och administrerar tjänsterna till.¹⁰⁸ En ensam representant som öppnar ett bankkonto, en postbox eller utgör kontaktperson för en verksamhets kunder har ansetts kunna utgöra stöd för en sådan stabil struktur som gör att verksamheten ska anses vara etablerad i ett visst land.¹⁰⁹ Verksamhetens ställets rättsliga form, oavsett om det är en filial eller ett dotterbolag, ska inte vara avgörande vid bedömningen av om det finns en stabil struktur.¹¹⁰ Inte heller ska det vara avgörande att verksamheten är registrerad i ett annat land.¹¹¹

Genom förordningen kommer medlemsstaternas nationella regler att få mindre inflytande även om vissa områden fortsatt kommer att vara reglerade på nationell nivå.¹¹² Personuppgiftsansvariga kommer nämligen i första hand, även i förhållande till kompletterande nationell lagstiftning, att behöva anpassa sig efter förordningen.¹¹³

¹⁰³ Skäl 22 i allmän dataskyddsförordning (EU) 2016/679; Voigt och von dem Bussche s. 22 f.; jfr, C-131/12, *Google Spain SL och Google Inc.*, EU:C:2014:317.

¹⁰⁴ En begäran om ändring av den svenska språkversionen har skickats in till Justitiedepartementet.

¹⁰⁵ Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39), s. 6 f.

¹⁰⁶ Gabel och Hickman, White & Case, s. 25.

¹⁰⁷ C-230/14, *Weltimmo s.r.o. mot Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639, p. 28–31; jfr. skäl 22 i allmän dataskyddsförordning (EU) 2016/679.

¹⁰⁸ Voigt och von dem Bussche s. 23.

¹⁰⁹ C-230/14, *Weltimmo*, EU:C:2015:639, p. 29 – 33.

¹¹⁰ Skäl 22 i allmän dataskyddsförordning (EU) 2016/679; jfr. C-131/12, *Google Spain SL och Google Inc.*, EU:C:2014:317, p. 48.

¹¹¹ Voigt och von dem Bussche, s. 23.

¹¹² Jfr. Gabel och Hickman, White & Case. s. 7.

¹¹³ Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39), s. 5.

3.3.2 Effektlandsprincipen

Till skillnad från direktivet kommer förordningen även att vara tillämplig för personuppgiftsansvariga som utför behandlingar på personuppgifter tillhörande en registrerad person inom unionen även om den personuppgiftsansvarige inte är etablerad inom unionen.¹¹⁴ I art. 3.2 i förordningen framgår det att om en behandling med anknytning till ett utbud av varor eller tjänster riktar sig till en enskild inom unionen, antingen kostnadsfritt eller till en avgift, eller om en behandling avser övervakning av en enskild inom unionen så ska dessa behandlingar falla under förordningens tillämpningsområde.¹¹⁵

Art. 3.2 i förordningen har tillkommit med syftet att utöka förordningens tillämpningsområde och försäkra att de som är berättigade till det skydd som förordningen ger omfattas av detta.¹¹⁶ Till skillnad från *etableringsprincipen* bygger art. 3.2 på principen *lex loci solutionis* vilket innebär att tillämplig lag blir den där erbjudandet om att ingå ett avtal uppstår. Bestämmelsen har till avsikt att omfatta alla erbjudanden som riktas mot unionens inre marknad och all profilering som sker av registrerade personer som befinner på den inre marknaden. Detta innebär att en registrerad person, oavsett nationalitet, kommer omfattas av förordningens skydd så länge denne befinner sig inom unionen.¹¹⁷ I förordningens skäl framgår det att det är den personuppgiftsansvariges, eller personuppgiftsbiträdets, avsikt bakom en tjänst som avgör om ett erbjudande är riktat till registrerade personer inom unionen. Att enbart ha åtkomst till en webbsida eller tillgång till en e-postadress är inte tillräckligt för att förordningen ska bli tillämplig. Erbjuds däremot webbsidan på ett eller flera av medlemsstaternas språk kan detta vara en faktor som talar för att erbjudandet riktar sig mot registrerade inom union.¹¹⁸

När en behandling genomförs för att profilera den enskildes beteende inom unionen är det den personuppgiftsansvariges avsikt med övervakningen som är avgörande för tillämpningsområdet. Om den enskilde spåras på internet och dennes uppgifter behandlas för att kunna kartlägga dennes beteende och preferenser för att kunna påverka den enskildes beslut torde denna avsikt ha funnits.¹¹⁹ Troligtvis kommer alla former av cookies¹²⁰ eller plugin-program att omfattas av förordningen.¹²¹

¹¹⁴ Díaz Díaz, s. 230,

<<https://doi.org/10.1080/23753234.2016.1240912>>, (besökt 2017-12-20).

¹¹⁵ Art. 3.2 i allmän dataskyddsförordning (EU) 2016/679.

¹¹⁶ Skäl 23 i allmän dataskyddsförordning (EU) 2016/679.

¹¹⁷ Voigt och von dem Bussche, s. 26 ff.

¹¹⁸ Skäl 23 i allmän dataskyddsförordning (EU) 2016/679.

¹¹⁹ Skäl 24 i allmän dataskyddsförordning (EU) 2016/679.

¹²⁰ En cookie är kortfattat varje dators unika användar-ID på en viss hemsida. Hemsidor som använder cookies sparar det unika ID:et och all aktivitet kopplad till detta ID varje gång datorn återvänder till hemsidan för att kunna analysera användarens beteende och spara information om denna.

¹²¹ Voigt och von dem Bussche, s. 27 f.

3.3.3 Förhållandet till tredje land och dataskyddslagen

I förordningens art. 3.3 framgår det att en sådan behandling som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men där behandlingen utförs i ett område där någon av medlemsstaternas nationella rätt är tillämplig enligt folkrätten, så ska behandlingen omfattas av förordningen.¹²² En liknande regel har funnits i 4 § 3 st. PUL.¹²³

I förordningen ges ingen vägledning om hur kompletterande nationell rätt ska förhålla sig till det territoriella tillämpningsområdet. I Sverige har det föreslagits att dataskyddslagen, som är tänkt att komplettera förordningen, som huvudregel ska tillämpa etableringsprincipen och inte effektlandsprincipen. Etableringsprincipen har enligt utredningen ansetts ligga närmare förordningens utgångspunkt och ge en högre kontinuitet i förhållande till vad som varit gällande i PUL. Utredningen framhöll även att flertalet medlemsländer uttalat att etableringsprincipen kommer vara huvudregeln i deras nationella lagstiftning vilket skulle öka harmoniseringen. Effektlandsprincipen kommer bli tillämplig i dataskyddslagen under samma omständigheter som i förordningen.¹²⁴

I förhållande till direktivet kommer förordningen i större utsträckning att bli tillämplig för aktörer i tredje land som bedriver verksamhet inom unionen. Förordningen kommer att behöva tillämpas i sin helhet av dessa aktörer i exempelvis sådana fall då de bedriver sin verksamhet över internet och riktar sina tjänster till enskilda i EU eller övervakar deras beteenden.¹²⁵ Vidare kommer även personuppgiftsbiträden i större utsträckning att påverkas även om de är etablerade i tredje land. Voigt och von dem Bussche framhåller att de personuppgiftsansvariga nämligen, för att själva uppfylla sina skyldigheter, kommer att upprätta avtal med sina personuppgiftsbiträden på så vis att avtalen ställer samma krav som förordningen gör.¹²⁶

¹²² Jfr. art. 3.3 i allmän dataskyddsförordning (EU) 2016/679.

¹²³ Öman och Lindblom s. 118 f.

¹²⁴ Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39), s. 6 ff.

¹²⁵ Gabel och Hickman, White & Case, s. 7 och 15; Voigt och von dem Bussche, s. 26 ff.

¹²⁶ Voigt och von dem Bussche, s. 25.

4 Laglig behandling

4.1 Allmänt om behandlingar

Alla behandlingar av personuppgifter måste, förutom att ske med stöd av någon av de lagliga grunderna i art. 6, även uppfylla de övriga allmänna villkor som ställs i förordningen för att kunna vara giltiga. Det är den personuppgiftsansvarige som ska uppfylla de krav som förordningen ställer, se art. 5.2, samt kunna visa på att dessa uppfylls. Skulle den personuppgiftsansvarige inte uppfylla villkoren som ställs kan denne drabbas av de rättsliga sanktionerna i art. 83.¹²⁷

4.1.1 Laglighet, korrekthet och öppenhet

De behandlingar som genomförs enligt förordningen ska vara lagliga, korrekta och öppna i förhållande till den registrerade personen. Kravet på *öppenhet* (eng. transparency) i art. 5.1 (a) utgör även en rättvis grund för att få behandla personuppgifter enligt art. 8 i EU-stadgan. Kravet på öppenhet har tillkommit i förordningen såsom ett uttryckligt villkor medan det i direktivet endast omnämndes i skälen. Genom sin nya position i förordningen påpekas emellertid registrerade personers rätt att veta och kontroll över sina personuppgifter så att de kan utöva sina rättigheter att, exempelvis, lämna eller återta samtycke.¹²⁸

Öppenhetsprincipen ska praktiseras mot registrerade personer. All information som den registrerade delges om behandlingen ska vara lättillgänglig, kortfattad och ges på ett klart, tydligt språk som den registrerade kan förstå.¹²⁹ Detta gäller särskilt om den registrerade är ett barn. Informationen får även lämnas genom visualisering eller via en webbsida.¹³⁰ Vidare är öppenhetsprincipen sammankopplad med den registrerades rätt till insyn och tillgång till de uppgifter som behandlas om denne. Den registrerade ska, bland annat, ha rätten att veta vem, hur, varför och i vilken omfattning dennes personuppgifter insamlats och behandlas.¹³¹ Vidare ska den registrerade personen få information om vilka risker, skyddsåtgärder och vilka rättigheter denne har genom förordningen rörande behandlingen för att den personuppgiftsansvarige ska försäkra sig om att öppenhetsprincipen uppfylls.¹³² Används uppgifterna till profilering ska den registrerade få information om detta och vad denna profilering leder till.¹³³

¹²⁷ Voigt och von dem Bussche, s. 87.

¹²⁸ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation, 2016/679* 17/EN, WP260, s. 5 f.

¹²⁹ Skäl 39 i allmän dataskyddsförordning (EU) 2016/679.

¹³⁰ Skäl 58 i allmän dataskyddsförordning (EU) 2016/679.

¹³¹ Art. 15 och skäl 39 i allmän dataskyddsförordning (EU) 2016/679.

¹³² Skäl 39, se även art. 13–14 för vidare krav i allmän dataskyddsförordning (EU) 2016/679.

¹³³ Skäl 39 och 58–61 i allmän dataskyddsförordning (EU) 2016/679.

Villkoret på *laglighet* har i PUL endast ansetts omfatta de lagliga grunderna i personuppgiftslagen.¹³⁴ I skälen till förordningen framgår det dock att begreppet häri även avser de laglighetsgrunder som fastställts i förordningen, annan unionsrätt eller medlemsstaternas nationella rätt enligt förordningen.¹³⁵ Kravet på laglighet är uppfyllt om behandlingen grundas på någon av de angivna grunderna art. 6 i förordningen.¹³⁶

Villkoret på *korrekthet* implementerades i PUL, även om den svenska lagstiftaren ansåg att villkoret hade en oklar betydelse och ifrågasatte dess nödvändighet i förhållande till laglighetskravet. Personuppgifter som insamlats på ett olagligt sätt, exempelvis genom telefonavlyssning, eller som behandlats ett sätt som varit oförenligt med det ändamål för vilka de samlades in har emellertid ansetts bryta mot villkoret på korrekthet i PUL.¹³⁷ Behandlingar som genomförs genom hemliga anordningar som samlar in personuppgifter utan samtycke har inte heller ansetts uppfylla kravet på korrekthet i PUL.¹³⁸ I SOU 2017:39 har förts en diskussion huruvida begreppet *korrekt* i den svenska språkversionen av förordningen framhåller det som egentligen avses med uttrycket. I utredningen påpekar de att begreppet i övriga språkversioner vanligen översätts till, och betyder, ”rimligt” snarare än korrekt. Utredningen kom fram till att en intresseavvägning bör göras vid bedömningen av vad som är *korrekt* enligt förordningen och att en behandling därmed kan komma att vara oskälig i vissa fall även om behandlingen grundas på en laglig grund.¹³⁹

4.1.2 Ändamålsbegränsning och uppgiftsminimering

I förordningens art. 5.1 (b-c) framgår vidare att personuppgifter endast får samlas in för *särskilda, uttryckligt angivna och berättigade ändamål*. De specifika ändamålen ska vara tydliga, legitima och bestämda vid tidpunkten för insamlingen och endast de personuppgifter som krävs för att uppfylla det ändamålet får samlas in. Personuppgifterna måste alltså även vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålet de behandlas för¹⁴⁰. Motsvarande artikel i direktivet, art. 6.1 (c), har haft direkt effekt i medlemsstaterna genom EU-domstolens dom i de förenade målen C-465/00 och C138/01 och 139/01 där domstolen uttalade att artikeln föreskrev

¹³⁴ HFD 2016 nr. 40.

¹³⁵ Skäl 40 i allmän dataskyddsförordning (EU) 2016/679.

¹³⁶ Voigt och von dem Bussche, s. 88.

¹³⁷ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt: 2017-10-03).

¹³⁸ Petersson och Reinholdsson, s. 97.

¹³⁹ SOU 2017:39, s. 106 f.

¹⁴⁰ Art. 5.1 (b och c) och skäl 30 i den allmänna dataskyddsförordningen (EU) 2016/679.

ovillkorliga skyldigheter.¹⁴¹ Syftet med kravet att personuppgifterna ska vara relevanta och adekvata är att så lite uppgifter som möjligt ska lagras.¹⁴²

I skälen till förordningen framgår att personuppgifter enbart bör behandlas när ändamålet med behandlingen inte kan uppnås på annat rimligt sätt. I synnerhet ska den tid personuppgifterna lagras hållas till ett minimum och den personuppgiftsansvarige ska säkerställa att uppgifterna inte sparas längre än vad som är nödvändigt för att fullgöra ändamålet. Strävan enligt förordningen är alltså att så få uppgifter som möjligt ska insamlas och behandlas.¹⁴³ Såsom uttalats i förhållande till PUL gör detta att det krävs att ändamålen är specifika och inte allmänna för att det ska kunna avgöras vilka personuppgifter som behöver samlas in.¹⁴⁴

Kravet på att de personuppgifter som samlas in ska vara adekvata och relevanta har, i förhållande till PUL, ansetts kunna påverka omfattningen av ändamålet.¹⁴⁵ Enligt Rosamund Jay ska det beaktas att kravet på uppgiftsminimering kommer ge tillämpningen av förordningen en striktare förhållning. Anledningen till detta är att mängden uppgifter som får samlas in kommer minska i jämförelse med direktivet. Skäl 39 i förordningen stipulerar nämligen att personuppgifter får samlas in endast om en behandling inte kan genomföras på något annat lämpligt sätt.¹⁴⁶ Detta är intressant att jämföra med den svenska utredningens inställning i SOU 2017:39 rörande nödvändighetskravet (se 4.2 nedan).

Specificeringen av ändamålet avgör dess omfattning och vilka personuppgifter som får behandlas inom ramen för detta. Vidare måste ändamålets omfattning bedömas utifrån vad den registrerade personen rimligen kunnat förvänta sig att samtycket omfattade. Detta är en inställning som antagits även av Datainspektionen i förhållande till PUL och art. 29-gruppen i förhållande till direktivet.¹⁴⁷ Skulle en behandling falla utanför ändamålet måste ett nytt samtycke eller annan laglig grund finnas för att behandlingen ska få genomföras.¹⁴⁸ Vid bedömningen av om behandlingen faller under det ursprungliga ändamålet ska den personuppgiftsansvarige

¹⁴¹ C-465/00, C138/01, 139/01, *Rechnungshof (C-465/00) och Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, och mellan Christa Neukomm (C-138/01), Joseph Lauerermann (C-139/01) och Österreichischer Rundfunk*, EU:C:2003:294, p. 99 – 101.

¹⁴² Voigt och von dem Bussche, s. 90.

¹⁴³ Skäl 39, jfr. art 5.1 (a) i allmän dataskyddsförordning (EU) 2016/679.

¹⁴⁴ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt 2017-10-15).

¹⁴⁵ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt 2017-10-15).

¹⁴⁶ Jay, R., *Guide to the General Data Protection Regulation – A companion to Data Protection Law and Practice 4th edition*, 1: a upplagan, Sweet and Maxwell, Great Britain, 2017, s. 87 f.

¹⁴⁷ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt 2017-10-15).

¹⁴⁸ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt 2017-10-15); Voigt och von dem Bussche, s. 89.

bland annat beakta vilken länk det finns mellan ändamålet och behandlingen, i vilket syfte insamlingen skedde för, relationen mellan den registrerade och den personuppgiftsansvarige, vilken typ av personuppgifter det rör sig om samt konsekvenserna av behandlingen.¹⁴⁹

I förordningen tillkommer inga större förändringar rörande hur ändamålet och dess omfattning ska tolkas.¹⁵⁰ Ändamålen ska även fortsatt vara särskilda, vilket kräver att de ska vara precisa. I PUL har, exempelvis, ändamålet ”Framtida forskning” ansetts vara för oprecist för att kunna accepteras som ett giltigt specifikt ändamål.¹⁵¹

4.1.3 Korrekthet, lagringsminimering, integritet och konfidentialitet

I förordningens art. 5.1 (d-f) ställs även krav på att de personuppgifter som behandlas av en personuppgiftsansvarig ska vara korrekta, uppdaterade och åtnjuta ett lämpligt skydd gentemot otillåten behandling, förlust eller skada¹⁵². Vidare får personuppgifterna inte lagras på ett sådant sätt som gör det möjligt att identifiera den registrerade eller lagras under längre tid än vad som är nödvändigt för att uppnå det ändamål vilket uppgifterna samlades in för.

De personuppgifter som behandlas om den registrerade ska vara *korrekta*. Detta innebär att den personuppgiftsansvarige utan dröjsmål ska vidta alla de rimliga åtgärder som krävs för att rätta eller radera felaktiga personuppgifter om en registrerad.¹⁵³ Den registrerade har rätt att själv begära rättelse av felaktiga uppgifter, komplettera ofullständiga uppgifter eller begära att de uppgifter som hanteras om denne ska begränsas. Den personuppgiftsansvarige ska tillgodose den registrerades begäran att utöva denna rätt. Om den registrerade personen begärt begränsning av de personuppgifter som behandlas måste dock någon av de fyra grunderna i förordningens art. 18 vara uppfyllda¹⁵⁴. När en begränsning av personuppgifter har gjorts kräver all annan behandling än lagring av dessa personuppgifter ett samtycke från den registrerade eller att det finns ett viktigt allmänintresse med behandlingen.¹⁵⁵

Den personuppgiftsansvarige ansvarar även för att personuppgifterna inte lagras för längre tid än nödvändigt i förhållande till de ändamål för vilka de samlades in. Bland annat uppmanas den personuppgiftsansvarige i skälen till förordningen att genomföra regelbundna rutiner för att kontrollera att detta

¹⁴⁹ Jay, s. 86 f.

¹⁵⁰ Art. 5.1 a och skäl 50 i allmän dataskyddsförordning (EU) 2016/679.

¹⁵¹ Öman och Lindblom, personuppgiftslagen, kommentaren till 9 §, Zeteo, (besökt 2017-10-15); Petersson och Reinholdsson, s. 98.

¹⁵² För mer information om vilka åtgärder som ska vidtas enligt förordningen för att uppnå lämpligt skydd, se art. 32–36 i allmän dataskyddsförordning (EU) 2016/679.

¹⁵³ Skäl 36 i allmän dataskyddsförordning (EU) 2016/679.

¹⁵⁴ Jfr. Art. 18.1 (a-d) i allmän dataskyddsförordning (EU) 2016/679.

¹⁵⁵ Art. 16 och art. 18 i allmän dataskyddsförordning (EU) 2016/679.

krav uppfylls.¹⁵⁶ Av både EU-domstolen, och i nationell praxis, har det dock ansetts att personuppgifter får sparas i ett par år efter att själva ändamålet upphört.¹⁵⁷ I C-553/07 ”Rijkeboer” uttalade EU-domstolen att detta är nödvändigt för att den registrerade ska kunna utöva sin rätt att exempelvis kunna få felaktiga eller ogiltiga personuppgifter rättade eller raderade. Lagring av personuppgifter ska alltså få ske med hänsyn till den registrerade personens rätt att kunna väcka talan i domstol.¹⁵⁸

Den personuppgiftsansvarige kan även bli skyldig att på begäran av den registrerade radera dennes personuppgifter redan innan ändamålet är uppnått. ”Rätten att bli bortglömd”, i förordningens art. 17, ger den registrerade rätten att få sina personuppgifter raderade, utan onödigt dröjsmål, under vissa omständigheter. Ett sådant exempel kan vara att den registrerade återkallar det samtycke denne har lämnat och det inte finns en annan rättslig grund för behandlingen eller om personuppgifterna hanterats på ett olagligt sätt.¹⁵⁹ En rätt till att få sina uppgifter ”utplånade” har även funnits i PUL.¹⁶⁰ I skälen till förordningen har det uttalats att den personuppgiftsansvariges ansvar ska utvidgas i förhållande till rätten att bli bortglömd. Den som offentliggjort personuppgifterna ska nämligen vidta rimliga åtgärder för att informera andra personuppgiftsansvariga som behandlar dessa uppgifter att den registrerade begärt radering av länkar, kopior eller reproduktioner av personuppgifterna.¹⁶¹

Det uttryckliga kravet på integritet och konfidentialitet i art. 5.1(f) har tillkommit i förordningen som en av de grundläggande principerna. Kravet fanns emellertid redan i direktivet och är i stort oförändrad.¹⁶² Den nya position i förordningen, likt kravet på öppenhet, ligger i linje med förordningens syfte att åter ge den registrerades kontroll över sina personuppgifter.¹⁶³ Kravet i art. 5.1 (f) ålägger den personuppgiftsansvarige att kunna försäkra att de personuppgifter som behandlas av denne omfattas av ett tillräckligt skydd.¹⁶⁴ Kravet på att tillräckliga tekniska och organisatoriska säkerhetsåtgärder ska tillämpas av den personuppgiftsansvarige har även funnits i både PUL och direktivet.¹⁶⁵

¹⁵⁶ Skäl 36 i allmän dataskyddsförordning (EU) 2016/679.

¹⁵⁷ Öman och Lindblom, personuppgiftslagen kommentaren till 9 §, Zeteo, (besökt: 2017-11-05).

¹⁵⁸ C-553/07, *College van burgemeester en wethouders van Rotterdam mot M.E.E. Rijkeboer*, EU:C:2009:293, p. 50 – 57.

¹⁵⁹ Art. 17 i allmän dataskyddsförordning (EU) 2016/679.

¹⁶⁰ Öman och Lindblom, Personuppgiftslagen, kommentar till 28 §, Zeteo (besökt 2017-12-20).

¹⁶¹ Skäl 66 i allmän dataskyddsförordning (EU) 2016/679.

¹⁶² Gabel och Hickman., *White & Case*, s. 26.

¹⁶³ Skäl 4 och 7 i allmän dataskyddsförordning (EU) 2016/679.

¹⁶⁴ Voigt och von dem Bussches, s. 92.

¹⁶⁵ C-342/12, *Worten – Equipamentos para o Lar SA mot Autoridade para as Condições de Trabalho (ACT)*, EU:C:2013:355, p. 24–29, se även 30–31 §§ PUL samt art. 17 i dir. 95/46/EG.

4.2 Lagliga grunder för behandling

Förordningen anger uttömmande i art. 6 på vilka lagliga grunder en behandling får genomföras. Utav de sex lagliga grunderna i art. 6 bygger enbart en av dem på samtycke. De övriga i art. 6.1 (b-f) bygger istället på ett nödvändighetskrav där samtycke inte är nödvändigt för att behandlingen genomförs.¹⁶⁶ Den registrerade ska dock alltid informeras om att en behandling sker och ha rätten att invända mot behandlingen, eller begära att dennes uppgifter ska raderas.¹⁶⁷ I de fall flera utav de lagliga grunderna kan vara tillämpliga på samma behandling bör den personuppgiftsansvarige överväga vilken rättslig grund som är mest lämplig. Fortsätter nämligen en behandling på en annan rättslig grund efter att ett samtycke återkallas, och ändamålet inte ändrats, kan nämligen en begäran om samtycke anses ha varit vilseledande och ogiltig.¹⁶⁸

Nödvändighetskriteriet ska tolkas utifrån unionsrätten. Till skillnad från den svenska definitionen, där nödvändighet uppstår när inga andra lösningar finns att tillgå, anses i SOU 2017:39 att nödvändighet härmed ska ges en vidare innebörd.¹⁶⁹ Om en behandling är nödvändig ska därmed bedömas utifrån ändamålet med behandlingen och ifall den personuppgiftsansvariges, eller tredje parts, intressen väger tyngre än den registrerades.¹⁷⁰ EU-domstolen har exempelvis bedömt att en behandling av personuppgifter kan vara nödvändig eftersom den bidrar med en klar effektivisering för den personuppgiftsansvarige.¹⁷¹ Rosamund Jay anser emellertid att förordningen kan få ett striktare tillämpningsområde med hänsyn till skäl 39 som anger att personuppgifter enbart ska samlas in om behandlingen inte kan ske på annat lämpligt sätt.¹⁷²

De lagliga grunder för behandling som anges i art. 6 är:

1. när den registrerade lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål (art. 6.1 (a)).
2. när en behandling är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade (art. 6.1 (b)),

¹⁶⁶ Art. 6.1 i allmän dataskyddsförordning (EU) 2016/679; SOU 2017:39 s. 103 f.

¹⁶⁷ Koščik, M., *The Impact of General Data Protection Regulation on the grey literature*, Grey Journal (TGJ), publicerad 2017-01-02, s. 42.

<<http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/pdfviewer/pdfviewer?vid=2&sid=2409e5df-3839-43b2-bae6-c75f9be047a9@pdc-v-sessmgr01>> (besökt: 2017-12-14).

¹⁶⁸ Article 29 Data Protection Working Party, 15/2011, *Opinion on the definition of consent*, 0119/11/EN, WP187, s. 13.

¹⁶⁹ SOU 2017:39, s. 105 f.

¹⁷⁰ Linder, A. (Editor), *European Data Protection Law – General Data Protection Regulation 2016*, 2016, s. 199; Koščik, M., s. 42 f.

<<http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/pdfviewer/pdfviewer?vid=2&sid=2409e5df-3839-43b2-bae6-c75f9be047a9@pdc-v-sessmgr01>>, (besökt 2017-12-14).

¹⁷¹ C-524/06, *Heinz Huber mot Bundesrepublik Deutschland*, EU:C:2008:724, p. 50–52.

¹⁷² Jay R., s. 87 f.

3. när behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åligger den personuppgiftsansvarige (art. 6.1.(c)),
4. när behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för registrerad eller annan fysisk person (art. 6.1 (d)),
5. när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (art. 6.1 (e)), eller
6. när behandlingen är nödvändig för sådana ändamål som rör den personuppgiftsansvariges eller tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn (art. 6.1 (f)).

Artikel 6.1 (f) får endast tillämpas av privata aktörer och inte av offentliga myndigheter.¹⁷³ Det är den personuppgiftsansvariges ansvar att välja den rättsliga grund som är mest passande i det enskilda fallet eftersom det är dennes ansvar att uppfylla de krav som ställs för att en behandling ska vara giltig.¹⁷⁴

4.2.1 Samtycke som laglig grund

Samtycke är den av de lagliga grunderna som ger den registrerade störst kontroll över behandlingen av sina personuppgifter. En av anledningarna är möjligheten för den registrerade att ta tillbaka sitt samtycke och på så sätt effektivt avsluta vidare behandling av de lämnade personuppgifterna.¹⁷⁵ Ett samtycke ska ha lämnats innan en behandling av den registrerades personuppgifter påbörjas.¹⁷⁶ Samtycken kan lämnas både skriftligt, muntligt eller elektroniskt.¹⁷⁷ Samtyckets placering som den första av de lagliga grunderna har ansetts visa på dess relevans i den gällande rätten. Samtycket är ett klart uttryck för enskildes grundläggande rättigheter, vilket även framgår av att samtycket uttryckligen omnämns i EU-stadgans art. 7 och 8.¹⁷⁸

Ett samtycke definieras i förordnings art. 4.11 såsom:

¹⁷³ Art. 6.1 (f) i allmän dataskyddsförordning (EU) 2016/679.

¹⁷⁴ Article 29 Data Protection Working Party (2011) WP187, s. 16; Article 29 Data Protection Working Party, *Guidelines on Consent under the Regulation 2016/679*, 17/EN, WP259, s. 4.

¹⁷⁵ Article 29 Data Protection Working Party (2011) WP187 s. 9; Article 29 Data Protection Working Party (2017) WP 259, s. 4; art. 17 (b) i allmän dataskyddsförordning (EU) 2016/679.

¹⁷⁶ Article 29 Data Protection Working Party (2011) WP187, s. 30 f.; Article 29 Data Protection Working Party (2017) WP259, s. 187; Article 29 Data Protection Working Party, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, 1676/13/EN, WP208, s. 4; Skäl 40 i allmän dataskyddsförordning (EU) 2016/679.

¹⁷⁷ Baker and McKenzie LLP, *Consent under the GDPR*, 2016, s. 3, <<http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Consent%20under%20the%20GDPR.pdf>>, (besökt: 2017-10-20)

¹⁷⁸ Article 29 Data Protection Working Party (2011) WP187, s. 5 ff.; Article 29 Data Protection Working Party (2017), WP259, s. 4.

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.

Definitionen är i stort sett densamma som den varit både i direktivet och i PUL, men den har förändrats något.¹⁷⁹ Kravet på att en otvetydig viljeyttring ska vara antingen ett uttalande eller en entydig bekräftande handling fanns inte i direktivet.¹⁸⁰ Kravet på den otvetydiga viljeyttringen ska vara en entydig bekräftande handling har inte heller funnits i PUL. Där har även kravet varit att samtycket ska vara särskilt istället för specifikt.¹⁸¹ Definitionen omfattar alla former av samtycke, detta innebär att kraven ska anpassas utifrån vem den registrerade är som ska lämna samtycket.¹⁸²

Utöver att samtycket måste uppfylla kraven som ställs genom dess definition i art. 4.11 måste det även finnas ett eller flera specifika ändamål för att detta ska vara giltigt. Vidare ska samtycket även uppfylla de villkor som ställs i förordningens art. 7. De behandlingar som grundas på samtycke ska vidare uppfylla de grundläggande villkor som ställs i art. 5 samt övriga krav som ställs i förordningen rörande den registrerades rättigheter.¹⁸³ Det är den personuppgiftsansvarige som ska visa att ett giltigt samtycke har lämnats.¹⁸⁴

4.2.1.1 Frivillighet

För att ett samtycke ska vara giltigt krävs det att detta är *frivilligt lämnat*. Den registrerade måste alltså haft möjligheten att göra, och sedan gjort, ett aktivt val att lämna sitt samtycke för ett visst ändamål. Om den registrerade inte har någon valmöjlighet eller känner sig tvingad till att lämna sitt samtycke, antingen genom hot eller för att den registrerade kommer lida negativa konsekvenser om den inte gör detta, är samtycket inte frivilligt lämnat.¹⁸⁵

Möjligheten att lämna ett frivilligt samtycke kan påverkas om den registrerade står i beroendeposition till den personuppgiftsansvarige och det finns en betydande ojämlikhet mellan parterna.¹⁸⁶ Så anses särskilt vara fallet när den personuppgiftsansvarige är en offentlig myndighet eller en

¹⁷⁹ Art. 2 (a) i dir. 95/46/EG; 3 § PUL.

¹⁸⁰ Article 29 Data Protection Working Party (2017) WP259, s. 5; Information Commissioners Office (ICO), *Consultation GDPR consent guidance*, 2017, s. 5, publicerad 2017-02-03, <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> (besökt: 2017-12-13).

¹⁸¹ 3 § PUL; art. 4.11 i allmän dataskyddsförordning (EU) 2016/679.

¹⁸² Ray, s. 90.

¹⁸³ Skäl 40 och 42 i allmän dataskyddsförordning (EU) 2016/679; Article 29 Data Protection Working Party (2017) WP259, s. 5 f.

¹⁸⁴ Datainspektionen, *Samtycke enligt personuppgiftslagen*, 2012, <<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsförordningen/rattslig-grund-for-personuppgiftsbehandling/samtycke/>> (besökt 2017-12-20).

¹⁸⁵ Article 29 Data Protection Working Party (2011) WP187, s. 12; jfr. Skäl 42 i allmän dataskyddsförordning (EU) 2016/679.

¹⁸⁶ Skäl 43 i allmän dataskyddsförordning (EU) 2016/679.

arbetsgivare.¹⁸⁷ Skatteverket efterlyste därför i sitt remissvar rörande SOU 2017:39 ett förtydligande kring när samtycke i denna situation kan lämnas.¹⁸⁸ Art. 29-gruppen har, som exempel, angivit att om myndigheten efterfrågar en enskilds e-postadress för att informera om ett specifikt bygge, och den registrerade personen kan få informationen även om denne inte lämnar sitt samtycke, skulle detta kunna vara en sådan situation då samtycke kan användas.¹⁸⁹

Art. 29-gruppen har även uttalat att en anställd generellt sett aldrig kan antas vara i den positionen att den kan avstå från att lämna ett giltigt samtycke om dennes arbetsgivare har bett om samtycket. Anledningen till detta är att den registrerade inte anses kunna neka till en sådan förfrågan utan att frukta för eventuella repressalier. Samtycken bör endast kunna lämnas frivilligt i anställningssituationer när det tydligt inte finns några konsekvenser av den registrerades val.¹⁹⁰ Art. 29-gruppen har framfört att detta exempelvis kan vara valet att inte delta i en reklamfilm för företaget.¹⁹¹ Att be sina anställda att lämna känsliga personuppgifter med syftet att förbättra likabehandling och mångfald inom ett företag har inte ansetts kunna utgöra ett frivilligt samtycke, även om den registrerade kunnat välja att inte lämna uppgifterna.¹⁹²

Problematik kring att lämna ett frivilligt samtycke kan även uppstå i, exempelvis, avtalssituationer.¹⁹³ I art. 7.4 framgår att det inte får finnas ett krav på att samtycke måste lämnas i en avtalssituation för att avtalet ska kunna fullgöras.¹⁹⁴

Samtycke presumeras att inte ha lämnats frivilligt när den registrerade inte kan ta del av ett avtal rörande en tjänst, om avtalet är beroende av att samtycket lämnas.¹⁹⁵ Samtycket kan alltså inte kunna utgöra en motprestation i en avtalssituation.¹⁹⁶ Frågan har diskuterats i förhållande till PUL. Öman och Lindblom har ansett att eftersom den registrerade kan välja mellan flera aktörer att ingå avtal med, varav vissa inte kräver samtycke för att fullgöra avtalet, så har den registrerade i slutändan gjort ett frivilligt val eftersom denne valt aktör. Undantaget ska vara om aktören har monopol på marknaden.¹⁹⁷ Voigt och von dem Bussche anser dock att det är en för snäv tolkning att enbart företag som innehar monopol ska kunna undantas

¹⁸⁷ Article 29 Data Protection Working Party (2017) WP259, s. 7 f.

¹⁸⁸ Skatteverket, *Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)*, 2017.

¹⁸⁹ Article 29 Data Protection Working Party (2017) WP259, s. 7 f.

¹⁹⁰ Article 29 Data Protection Working Party, 2/2017, *Opinion on data processing at work*, 17/EN, WP249, s. 6 f., 23; Article 29 Data Protection Working Party, *Opinion 8/2001, on the processing of personal data in the employment context*, 5062/01/EN, WP48, s. 23.

¹⁹¹ Article 29 Data Protection Working Party (2017) WP249, s. 6 f., 23.

¹⁹² Datainspektionen, *Tillsyn enligt personuppgiftslagen (1998:204) – registrering av känsliga personuppgifter om anställda*, dnr. 120–2017.

¹⁹³ Gabel och Hickman., *White & Case*, s. 37.

¹⁹⁴ Art. 7.4 i allmän dataskyddsförordning (EU) 2016/679.

¹⁹⁵ Skäl 43 i allmän dataskyddsförordning (EU) 2016/679.

¹⁹⁶ Article 29 Data Protection Working Party (2017), WP259, s. 9 f.

¹⁹⁷ Öman och Lindblom, *personuppgiftslagen*, kommentar till 3 §, Zeteo, (besökt: 2017-12-15).

bestämmelsen med beaktande av förordningens syfte att minska registrerades exploatering av personliga data.¹⁹⁸ Art. 29-gruppen har enbart uttalat sig om situationen där samma personuppgiftsansvarig erbjuder två likvärdiga tjänster. Så länge tjänsterna är helt likvärdiga har det ansetts att ett frivilligt samtycke kan lämnas i detta fall.¹⁹⁹ Vad som kommer att anses som ett frivilligt val då samma tjänst erbjuds av olika företag är därmed oklart.

För att samtycket ska vara frivilligt krävs det även, när samtycke ska lämnas för flera ändamål, att den registrerade separat kan välja vilka ändamål denne vill samtycka till.²⁰⁰ Den registrerade ska inte behöva lämna samtycke till direkt marknadsföring enbart för att denne öppnar ett medlemskap hos en butik.²⁰¹ Kan den registrerade inte separat välja mellan de olika ändamålen presumeras samtycket inte vara frivilligt lämnat.²⁰² Den registrerade måste även ha rätten att kunna återta sitt samtycke utan att detta ger några repressalier eller andra negativa konsekvenser från den personuppgiftsansvarige för att samtycket ska vara frivilligt.²⁰³ Rätten att återkalla samtycke finns i art. 7.3 i förordningen där det även stipuleras att det ska vara lika enkelt att återkalla samtycket som att lämna det.

4.2.1.2 Specifikt och informerat

Kravet på att samtycket ska vara *specifikt* angavs i PUL såsom att samtycket skulle vara särskilt. Orden är dock synonyma till varandra och har en liknande innebörd.²⁰⁴ Genom art. 6.1 (a) befästs att samtycket ska ges för ett specifikt ändamål, vilket därmed även styrker kraven på öppenhet/information och frivillighet. Regeln ska alltså läsas tillsammans med art. 5.1 (b) för att personuppgiftsansvariga ska veta vad som krävs för att ändamålet ska anses vara specifikt. I gemenskap försäkras artiklarna att de specifika ändamålen för vilka personuppgifter behandlas inte kan vidgas och att behandlingar som genomförs inte faller utanför det ursprungliga ändamålet.²⁰⁵ Så länge behandlingen faller inom det ändamål för vilket samtycket har lämnats är dock behandlingen laglig och vid en bedömning av ett ändamåls omfattning ska den personuppgiftsansvarige beakta vad den registrerade rimligen förväntade sig när denne lämnade samtycket.²⁰⁶ Exempelvis har EU-domstolen uttalat att om den registrerade är informerad om att dennes personuppgifter kan överföras till en bestämd tredje part ska inte ett nytt samtycke behöva inhämtas även om uppgifterna överlämnas till annan tredje part. Ändamålet med överföringen måste dock vara detsamma

¹⁹⁸ Voigt och von dem Bussche, s. 95; jfr. med Larsson, S. & Ledendal, J: *Personuppgifter som betalmedel*.

¹⁹⁹ Article 29 Data Protection Working Party (2017), WP259, s. 10.

²⁰⁰ Article 29 Data Protection Working Party (2017), WP259, s. 11.

²⁰¹ Jay, s. 90.

²⁰² Skäl 42 i allmän dataskyddsförordning (EU) 2016/679.

²⁰³ Article 29 Data Protection Working Party (2017), WP259, s. 11.

²⁰⁴ Jfr. 3 § PUL och art. 4.2 i allmän dataskyddsförordning (EU) 2016/679.

²⁰⁵ Article 29 Data Protection Working Party (2017) WP259, s. 12.

²⁰⁶ Öman och Lindblom, personuppgiftslagen, kommentar till 3 §, Zeteo, (besökt: 2017-12-16); Skäl 50 i allmän dataskyddsförordning (EU) 2016/679.

som samtycket lämnades för. Skulle överföringen falla utanför detta skulle överföringen vara ogiltig.²⁰⁷

Vidare ska den registrerade, för att samtycket ska uppfylla kravet på att vara specifikt, ha insyn i behandlingen och ha kontroll över de personuppgifter som behandlas.²⁰⁸ Ska samtycke lämnas för flera olika ändamål ska därför den registrerade, likt vad som gäller avseende kravet om frivillighet, kunna välja vilket, eller vilka, ändamål denne vill samtycka till.²⁰⁹ Information ska därmed lämnas i förhållande till varje ändamål så att den registrerade är medveten om vad varje ändamål innebär och på så vis kan lämna specifika samtycken.²¹⁰ Generella samtycken är därmed förbjudna enligt förordningen eftersom de saknar specifika ändamål.²¹¹ Ett förbud mot generella samtycken har även funnits i PUL.²¹²

Att samtycket ska vara *informerat* är starkt sammankopplat med kravet på öppenhet (eng. *transparency*) i art. 5.1 (a) och den registrerades rätt till information i art. 12.²¹³ Vikten av informationskravet för att enskilda ska kunna lämna informerade samtycken och nyttja sina rättigheter har särskilt påpekats av generaladvokaten i mål C-201/14, ”Bara-målet.”²¹⁴

För att samtycken ska vara informerade ska informationen ges innan den registrerade lämnar sitt samtycke till en behandling. Detta är för att den registrerade ska förstå vad denne samtycker till och konsekvenserna av detta.²¹⁵ Informationen ska lämnas på ett klart, tydligt och lättillgängligt sätt så att den som informationen är avsedd för kan ta till sig denna. Kan den avsedda mottagaren av informationen förändras över tid ska den personuppgiftsansvarige regelbundet kontrollera så att informationen är anpassad för mottagaren.²¹⁶ Detta gäller särskilt när informationen riktar sig till barn. Informationen ska då vara uttryckt på ett sådant sätt att barnen förstår att den riktar sig till dem.²¹⁷ Detta gäller även om samtycket lämnas av en person med nedsatt förmåga.²¹⁸

²⁰⁷ C-543/09 *Deutsche Telekom AG mot Bundesrepublik Deutschland*, EU:C:2011:279, p. 66–67.

²⁰⁸ Article 29 Data Protection Working Party (2017) WP259, s. 12.

²⁰⁹ Voigt and von dem Bussche, s. 96; Skäl 32 och 43 i allmän dataskyddsförordning (EU) 2016/679.

²¹⁰ Article 29 Data Protection Working Party (2017) WP259, s. 13.

²¹¹ Baker and McKenzie LLP, *Consent under the GDPR*, 2016, s. 2, <<http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Consent%20under%20the%20GDPR.pdf>> (besökt 2017-11-10).

²¹² Datainspektionens beslut, *Tillsyn enligt personuppgiftslagen*, dnr. 1938–2010.

²¹³ Article 29 Data Protection Working Party (2017) WP259, s. 13.

²¹⁴ C-201/14, *Smaranda Bara m.fl. mot Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, EU:C:2015:461.

²¹⁵ Article 29 Data Protection Working Party (2017) WP259, s. 13.

²¹⁶ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*, 17/EN, WP260, s. 6–10.

²¹⁷ Article 29 Data Protection Working Party, WP260, s. 6–10; Skäl 42 och 58 i allmän dataskyddsförordning (EU) 2016/679.

²¹⁸ Jay, s. 90.

Att informationen är lättillgänglig innebär att den registrerade inte ska behöva leta efter informationen för att ta del av den. Skulle informationen, eller en länk till denna, vara positionerad så att den är svår att uppfatta eller vara utformad i en färgskala som gör den svår att upptäcka menar art. 29-gruppen att kravet på lättillgänglighet inte ska vara uppfyllt.²¹⁹ Reglerna är därmed ett instrument för att ge registrerade en större säkerhet och trygghet, framförallt i förhållande till profilering och marknadsföring där det kan vara oklart om personuppgifter samlas in och vilka som i så fall tar del av dem. För att ett samtycke om cookies ska vara informerat enligt förordningen ska den registrerade få information om vart den data som samlas in sänds och i vilket syfte.²²⁰

En problematik med kravet på informerat samtycke har lyfts fram av Shara Monteleone, forskare i Nederländerna. Hon framför att majoriteten av alla företag idag använder sig av privacy policys för att delge registrerade den information som krävs enligt lag. Hon menar dock att det finns en ”privacy paradox”. Denna innebär att trots att individer är oroliga över sin personliga data läser de inte den givna informationen utan lämnar sitt samtycke trots att de inte blivit informerade om vad detta innebär. Shara Monteleone påpekar att detta beror på att den registrerade ofta möter informationsmättnad genom att dessa privacy policys är långa och komplicerat skrivna. Men även i de fall de är enklare och tillgängliga så läser inte den registrerade dessa. De har alltså ingen påverkan på användarens beteende. Hon menar vidare att även om kraven på att detaljerad, enkel och lättförståelig information ska lämnas kommer det inte påverka de registrerade i deras val.²²¹

Problematiken har även lyfts av Samson Esayas, Tobias Mahler och Kevin McGillivray. De hänvisar till studier som visar på att enbart en av fem läser privacy policys. De menar, likt Monteleone, att informationen som ges är för omfattande, komplicerad samt full av terminologi som ska förvirra de registrerade.²²² En studie som genomfördes i USA år 2007 visade även att om registrerade skulle ta del av den information som ges i de privacy policys som registrerade generellt ska läsa igenom under ett års tid, så skulle detta kräva cirka 201 timmar per registrerad person, eller utgöra en uppskattad kostnad på cirka 3 534 dollar²²³, i tidsförlust för den registrerade.²²⁴

²¹⁹ Article 29 Data Protection Working Party (2017), WP260, s. 7 f.

²²⁰ Monteleone, S., *Addressing the 'Failure' of informed consent in online data protection: Learning the lessons from behavioraware regulation*, in Macro Draft, publicerad: 2016-02-23, s. 72 ff. <<http://jilc.syr.edu/wp-content/uploads/2015/11/Monteleone-Macro-2-23.pdf>>, (besökt: 2017-11-19).

²²¹ Monteleone, s. 74 ff., 79 f., 87 ff., <<http://jilc.syr.edu/wp-content/uploads/2015/11/Monteleone-Macro-2-23.pdf>>, (besökt: 2017-11-19).

²²² Esayas, S., Mahler, T. och McGillivray K., *Is a Picture Worth a Thousand Terms? Visualising Contract terms and Data Protection Requirements for Cloud Computing Users*, in *Current trends in Web Engineering*, Springer International Publishing, 2016, s. 42 ff.

²²³ Drygt 29 500 kr enligt valutaräkning den 21 december 2017. För USA, där studien genomfördes, skulle detta resultera i en kostnad i tidsförlust på cirka 781 miljarder dollar årligen om detta efterföljdes av alla användare i landet.

²²⁴ McDonald, Aleecia M., Cranor Lorrie F.: *The cost of reading privacy policies*. In: *Proceedings of the Technology Policy Research Conference*, 26–28 September 2008, s. 549

Förordningen ställer nya krav på hur information ska lämnas som är avsedda att bemöta detta problem. I art. 7.2 i förordningen ställs kravet att då en begäran om samtycke lämnas i en skriftlig förklaring, som även rör andra frågor, ska en sådan begäran om samtycke klart och tydligt kunna särskiljas från de övriga frågorna. Art. 29-gruppen menar därmed att långa juridiska texter kommer vara förbjudna för att ”gömma” information rörande ändamålet och behandlingen som kan vara relevant för samtycket. Detta ska gälla särskilt i förhållande till samtycken som lämnas online.²²⁵ Information ska även lämnas på ett sätt som är passande för situationen.²²⁶ Shara Monteleone menar att förordningen härmed förespråkar en större användarvänlighet och personuppgiftsansvariga ska försöka finna nya vägar, utöver privacy policys, för att lämna information till registrerade.²²⁷

EU-domstolen har, rörande tydligheten och tillgängligheten av informationen, fastställt att enbart en hänvisning till information i, exempelvis, ett kollektivavtal inte uppfyller kravet om ett informerat samtycke.²²⁸ Art. 29-gruppen har dock ansett att en hänvisning bör vara tillräckligt om materialet överlämnas eller länkas till den registrerade.²²⁹ Det finns inga krav på vilken form informationen ska lämnas utan den kan vara skriftlig, elektronisk eller visuell.²³⁰

I skäl 42 till förordningen framgår att ett samtycke bör vara informerat så länge den personuppgiftsansvarige åtminstone lämnar information om ändamålet med behandlingen samt vem som genomför behandlingen (är personuppgiftsansvarig).²³¹ Art 29-gruppen har emellertid rekommenderat att personuppgiftsansvariga alltid bör, utöver detta, lämna information om vilka personuppgifter som kommer att behandlas, rätten att återta samtycket, om personuppgifterna kommer hanteras genom automatiska beslut såsom profilering samt, när det är relevant, riskerna att personuppgifterna kan överföras till tredje land där de inte kan få adekvat skydd.²³²

I direktivets art. 10 angavs vidare ytterligare krav på information när samtycket innebar att personuppgifterna även samlades in. Den personuppgiftsansvarige skulle då lämna information om att denne

– 568, <https://kb.osu.edu/dspace/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf> (besökt: 2017-11-19).

²²⁵ Article 29 Data Protection Working Party (2017) WP259, s. 14 f.

²²⁶ Article 29 Data Protection Working Party (2017), WP260, s. 11.

²²⁷ Monteleone, s. 92 f, <<http://jilc.syr.edu/wp-content/uploads/2015/11/Monteleone-Macro-2-23.pdf>>, (besökt: 2017-11-19).

²²⁸ C-397/01-C403/01, *Bernhard Pfeiffer (C-397/01)*, *Wilhelm Roith (C-398/01)*, *Albert Süß (C-399/01)*, *Michael Winter (C-400/01)*, *Klaus Nestvogel (C-401/01)*, *Roswitha Zeller (C-402/01)*, *Matthias Döbele (C-403/01)* Och *deutsches Rotes Kreuz, Kreisverband Waldshut eV, PFEIFFER M.FL. och Deutsches Rotes Kreuz, Kreisverband Waldshut eV*, EU:C:2004:584, p. 82–85.

²²⁹ Article 29 Data Protection Working Party (2017), WP260, s. 7 ff.

²³⁰ Skäl 58 i allmän dataskyddsförordning (EU) 2016/679.

²³¹ Skäl 42 i allmän dataskyddsförordning (EU) 2016/679; Article 29 Data Protection Working Party (2017), WP260, s. 10.

²³² Article 29 Data Protection Working Party (2017) WP259, s. 13.

behandlade uppgifterna, ändamålet med behandlingen, eventuella mottagare samt all ytterligare information såsom krävs för att den registrerade ska kunna utöva sina rättigheter.²³³ Detsamma har varit gällande i PUL.²³⁴ Informationskravet har dock här varit undantaget när missbruksregeln varit tillämplig.²³⁵ Den personuppgiftsansvarige har alltså enbart behövt lämna information i den omfattning som bedömts som nödvändig för den specifika behandlingen.²³⁶ I förordningens art. 13 specificeras vilken information som ska lämnas när personuppgifter insamlas från den registrerade och i art. 14 anges vad som krävs när personuppgifterna erhållits från annan än den registrerade. Informationen ska delges den registrerade, och får alltså inte lämnas som en del av allmänna villkor.²³⁷ Artiklarna anger att, utöver vad som angetts i stycket ovan av art. 29-gruppen, information även ska lämnas om vilken tidsperiod personuppgifterna kommer behandlas och rätten att inkomma med klagomål till tillsynsmyndigheten.²³⁸

4.2.1.3 Otvetydig viljeyttring

Ett samtycke ska vara en otvetydig viljeyttring vilket innebär att det inte ska finnas något tvivel om att den registrerade personen faktiskt samtycker till behandlingen.²³⁹ I direktivet har det inte funnits något krav på att en otvetydig viljeyttring ska ges genom ett visst uttalande eller en entydig bekräftande handling. Istället har varje indikation på att det varit den registrerades vilja att samtycka till en behandling varit giltig så länge indikationen varit tillräckligt tydlig. Detta har gett direktivet ett brett tillämpningsområde. Bland annat har konkludent handlande, passivitet och även inaktivitet kunnat utgöra indikationer på en otvetydig viljeyttring.²⁴⁰ Art. 29-gruppen framhöll dock, rörande direktivet, kritik gentemot att passivitet och inaktivitet kunde utgöra en otvetydig viljeyttring. Gruppen menade att det skulle vara tveksamt att det faktum att den registrerade inte ändrat på förinställningar som, exempelvis, tillåter vänners vänner på sociala medier att ta del av den registrerades information verkligen visat otvetydigt på den registrerade personens vilja.²⁴¹

Tolkningen av begreppet otvetydig viljeyttring har följt en liknande linje i PUL. För att det ska ha förelegat en otvetydig viljeyttring har det, i PUL, krävts att det inte förelegat några omständigheter som talat emot den registrerades avsikt med sitt handlande. Konkludent handlande har i PUL ansetts kunna ge uttryck för den registrerades vilja och har därmed kunnat utgöra giltigt samtycke. Varken Öman och Lindblom, Reinholdsson och

²³³ Art. 10 i dir. 95/46/EG.

²³⁴ Petersson och Reinholdsson, s. 173; Datainspektionen, *Beslut efter tillsyn enligt personuppgiftslagen (1998:204)*, dnr. 998–2006.

²³⁵ 5 a § i PUL.

²³⁶ Article 29 Data Protection Working Party (2011) WP187, s. 19 f.; Petersson och Reinholdsson, s. 173.

²³⁷ Article 29 Data Protection Working Party (2017), WP260, s.14 ff.

²³⁸ Art. 13 och art. 14 i allmän dataskyddsförordning (EU) 2016/679.

²³⁹ Skäl 31 i allmän dataskyddsförordning (EU) 2016/679; Annereau, S., *Understanding consent under the GDPR*, TaylorWessing, publicerad: November 2016, <www.taylorwessing.com/globaldatahub/article-understanding-consent-under-the-gdpr.html>, (besökt: 2017-12-02).

²⁴⁰ Article 29 Data Protection Working Party (2011) WP187, s. 11 f.

²⁴¹ Article 29 Data Protection Working Party (2011) WP187, s. 11, 21 ff.

Petersson eller Datainspektionen har emellertid ansett att passivitet eller inaktivitet kunnat utgöra en otvetydig viljeyttring från den registrerade.²⁴² Datainspektionen har vidare framhållit att konkludent handlande generellt inte har ansetts tillräckligt för att utgöra en tillräckligt stark viljeyttring för att lämna ett samtycke i förhållande till känsliga personuppgifter i PUL.²⁴³

I och med klargörandet att en otvetydig viljeyttring ska bestå av ett visst uttalande eller vara en entydig bekräftande handling kommer det enligt förordningen krävas någon form av medveten handling från registrerade personer som gör det uppenbart att de har lämnat sitt samtycke. Detta blir således en förutsättning för att handlingen ska kunna ses som otvetydig.²⁴⁴ Det finns emellertid inget formkrav i förordningen på hur samtycket ska lämnas. En otvetydig viljeyttring kan därmed vara både skriftlig, muntlig, elektronisk eller i någon annan form.²⁴⁵ I direktivet har det inte heller funnits något formkrav på hur samtycke ska lämnas. Art. 29-gruppen har framhållit att syftet med detta har varit att samtycken ska kunna vara flexibla.²⁴⁶

En entydig bekräftande handling har i skälen till förordningen ansetts kunna vara att den registrerade kryssar i en ruta vid besök på en internetsida, gör val av inställningsalternativ på en internetsida eller annat beteende som i sammanhanget tydligt visar på att den registrerade godkänner behandlingen.²⁴⁷ Att den registrerade personen skriver i ett e-post i vilken omfattning denne samtycker till en viss behandling är en entydig handling. Art. 29-gruppen har även framfört att fysiska rörelser, såsom att svepa över en skärm, ska kunna utgöra en otvetydig viljeyttring så länge det är klart för den registrerade personen att handlingen innebär att ett samtycke lämnas.²⁴⁸

Genom förordningens krav på en entydig bekräftande handling har det ansetts att tystnad, inaktivitet eller användandet av redan ikryssade rutor inte kommer utgöra giltiga samtycken.²⁴⁹ Rosamund Jay har dock lyft frågan om huruvida ett samtycke fortsatt kommer kunna vara giltigt genom att den registrerade endast fortsätter att ta del av en tjänst såsom är vanligt på internetsidor.²⁵⁰ Cookies får exempelvis inte läsas in och sparas på den registrerade personens dator om inte denne har lämnat sitt samtycke till behandlingen genom en sådan aktiv handling att det är tydligt för den personuppgiftsansvarige att den registrerade har lämnat sitt samtycke. Skulle den registrerade personen enbart stanna på startsidan menar art. 29-gruppen att det är svårt att argumentera för

²⁴² Öman och Lindblom, personuppgiftslagen, kommentaren till 3 §, Zeteo, (besökt 2017-12-20); Reinholdsson och Petersson s. 115 f.; Datainspektionen informationsblad, *Samtycke enligt personuppgiftslagen*, 2015, s. 7 f.

²⁴³ Datainspektionen informationsblad, *Samtycke enligt personuppgiftslagen*, 2015, s. 9.

²⁴⁴ Article 29 Data Protection Working Party (2017) WP259, s. 16; Skäl 32 i allmän dataskyddsförordning (EU) 2016/679.

²⁴⁵ Skäl 31 i allmän dataskyddsförordning (EU) 2016/679.

²⁴⁶ Article 29 Data Protection Working Party (2011) WP187, s. 11.

²⁴⁷ Skäl 32 i allmän dataskyddsförordning (EU) 2016/679.

²⁴⁸ Article 29 Data Protection Working Party (2017) WP259, s. 17.

²⁴⁹ Article 29 Data Protection Working Party (2017) WP259, s. 16 f.; Voigt and von dem Bussche, s. 95,

²⁵⁰ Jay, s. 90.

att ett otvetydigt samtycke lämnats. Att den registrerade klickar på en länk för att få mer information om cookies ska inte heller ses som ett samtycke trots att detta är en aktiv handling i sig, eftersom den aktiva handlingen enbart visat på att den registrerade begärt mer information och inte att denne samtyckt till behandlingen.²⁵¹ Hur förhållandet till just cookies kommer att bli genom förordningen kommer dock troligtvis att preciseras i e-skyddsförordningen.

4.2.2 Barns samtycke

Barn har, enligt förordningen, rätt till ett särskilt skyddsvärde.²⁵² Detta skydd gäller särskilt mot profilering och direkt marknadsföring.²⁵³ Barn har i skälen till förordningen ansetts vara mindre medvetna om konsekvenserna och riskerna med att lämna ett samtycke, samt mindre medvetna om vilka rättigheter de har gentemot personuppgiftsansvariga.²⁵⁴ Förordningen kommer därför att ställa högre krav på den information som lämnas till barn, barns rätt att radera sina uppgifter och den kommer öka skyddet gentemot profilering och direkt marknadsföring.²⁵⁵ Förordningen inför även nya krav för när barn ska lämna samtycke genom art. 8.

4.2.2.1 Barns samtycke i PUL och direktivet

I PUL har samtliga fysiska personer kunnat lämna samtycke så länge de har förstått innebörden av samtycket. Även barn har därmed kunna lämna giltiga samtycken så länge de har uppnått sådan mognad och förståelse att de varit medvetna om och förstått konsekvenserna av samtycket. Ett barn har enligt PUL varit den som är under 18 år. Oförmåga att lämna giltiga samtycken har emellertid även omfattat vuxna som inte haft förmåga att förstå innebörden av ett lämnat samtycke. I PUL har det inte funnits någon angiven ålder för när barn generellt har ansetts mogna nog att lämna ett giltigt samtycke. Datainspektionen har gjort bedömningen att denna ålder generellt ska vara 15 år.²⁵⁶ För barn under 15 år, eller barn som trots sin ålder inte har uppnått sådan mognad att ett giltigt samtycke kunnat lämnas, har som regel vårdnadshavarna varit de som kunnat lämna ett giltigt samtycke i barnets ställe.²⁵⁷

Direktivet har inte heller haft några specifika regler rörande barns möjligheter att lämna ett giltigt samtycke till behandling. Även här har en bedömning av

²⁵¹ WP29, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, 1676/13/EN, WP208, s. 4 f.

²⁵² Skäl 38, i allmän dataskyddsförordning (EU) 2016/679; SOU 2017:39 s. 140; Voigt and von dem Bussche, s. 98; Macenaite, & Kosta, s.149, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-16).

²⁵³ Skäl 38 i allmän dataskyddsförordning (EU) 2016/679; SOU 2017:39, s. 141.

²⁵⁴ Skäl 38 i allmän dataskyddsförordning (EU) 2016/679; Macenaite & Kosta, 2017, s. 149, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-16); Article 29 Data Protection Working Party, (2017), WP259, s. 23; SOU 2017:39, s. 141.

²⁵⁵ Macenaite & Kosta, 2017, s. 149, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-16).

²⁵⁶ Datainspektionen informationsblad, *Samtycke enligt personuppgiftslagen*, 2015, s. 10 f.

²⁵⁷ Öman och Lindblom, personuppgiftslagen, kommentaren till 3 §, Zeteo, (besökt 2017-12-16).

barnets mognad fått göras i förhållande till barnets förmåga att själv bestämma över sina intressen.²⁵⁸ I de fall ett barn inte ansetts kunna ge ett giltigt samtycke enligt direktivet har detta kunnat lämnas, eller godkännas i efterhand, av barnets rättsliga företrädare såsom barnets vårdnadshavare. Art. 29-gruppen har i förhållande till direktivet belyst att vårdnadshavarna alltid ska fatta ett beslut om samtycke å barnets vägnar med hänsyn till barnets bästa och dess särskilda skyddsvärde. Art-29-gruppen har även framfört att barnet ska, i förhållande till sin mognad och ålder, konsulteras i frågan och att barnets vilja ska beaktas.²⁵⁹

4.2.2.2 Förordningens art. 8

Ett generellt ökat intresse för barns skyddsvärde inom olika frågor inom EU har gjort att behovet av särskilda regler som reglerar barns skydd av personuppgifter ansetts nödvändiga i unionen, detta menar Milda Macenaite & Eleni Kosta i sin artikel ”*Consent for processing childrens’ personal data in the EU: following in the US footsteps*”. De framför vidare att empiriska studier visat att alltför många internet-sidor och applikationer (härefter ”appar”) riktar sig till barn i allt lägre åldrar, samtidigt som barn mellan 11–16 år har svårt att rapportera felaktiga behandlingar av deras personuppgifter och att genomföra nödvändiga inställningar för att skydda dessa.²⁶⁰ Genom införandet av förordningens art. 8, som reglerar barns möjlighet att lämna giltiga samtycken, ska ett starkare skydd vid behandlingar av barns personuppgifter uppnås.²⁶¹ Bland annat är ambitionen att barn inte ska kunna bli pressade till att lämna samtycken i situationer när de inte förstår innebörden eller konsekvenserna av att göra detta.²⁶²

Art. 8 stipulerar att barn under 16 år inte kan lämna giltiga samtycken till de av informationssamhällets tjänster som direkt riktar sig till barn. För barn under 16 år kan endast giltigt samtycke lämnas, eller i efterhand godkännas, av den, eller de som har föräldraansvaret för barnet.²⁶³ Det är den som har vårdnaden om barnet, eller ett liknande förhållande med detta, som även har

²⁵⁸ Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of childrens personal data (General Guidelines and special case of schools)*, 398/09/EN, WP160, s. 9.

²⁵⁹ Article 29 Data Protection Working Party, (2009), WP160, s. 6 ff.

²⁶⁰ Macenaite & Kosta, s. 149, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-16).

²⁶¹ Article 29 Data Protection Working Party (2017) WP259, s. 23; Macenaite, M., *From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation*, in *new media and society*, vol. 19(5), 765-779, publicerad den 16 januari 2017, s. 772,

<<http://journals.sagepub.com/ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>, (besökt 2017-12-16).

²⁶² Macenaite, s. 772,

<<http://journals.sagepub.com/ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>, (besökt 2017-12-16).

²⁶³ Article 29 Data Protection Working Party (2017) WP259, s. 23; Macenaite & Kosta, s. 160; <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-18), Verdoodt, V. & Lievens, E., *Data protection and Privacy under Pressure – Targeting Children with Personalised advertising*, s. 323, <<https://biblio.ugent.be/publication/8541057/file/8541058>> (besökt 2017-12-18); SOU 2017:39 s. 144 ff.

föräldraansvaret för barnet. Föräldraansvaret regleras i föräldrabalken (FB) i svensk rätt och i FB framgår det att det är vårdnadshavarna som innehar denna roll.²⁶⁴ Detta gäller även i förhållande till unionsrätten.²⁶⁵ Art. 8.1 ska *inte* påverka tillämpningen av avtalsrättsliga bestämmelser rörande giltighet eller effekt rörande barn.²⁶⁶

Med informationssamhällets tjänster avses sådana tjänster som vanligen utförs elektroniskt, på distans och på individuell begäran av en tjänstemottagare mot ersättning.²⁶⁷ Milda Macenaite & Eleni Kosta har framfört att EU-domstolen tolkat begreppet brett och att även annonsbaserade tjänster som erbjuds utan ersättning²⁶⁸ ska omfattas av begreppet.²⁶⁹ Det är ännu oklart om tjänster som erbjuds från s.k. ”non-profit” organisationer, alltså rena välgörenhetsorganisationer, kommer att undantas från begreppet.²⁷⁰ I flera fall har begreppet informationssamhällets tjänster tolkats såsom att det ska omfatta alla tjänster som erbjuds online.²⁷¹ I SOU 2017:39 har utredningen ansett att begreppet ska omfatta alla onlinetjänster som erbjuder försäljning av varor, tillhandahåller en sökmotor, utgör sociala medier, tillhandahåller videoklipp eller utgör appar.²⁷² Art. 8 i förordningen är avsedd att omfatta sociala medier vilket har framförts av Kommissionen.²⁷³

²⁶⁴ SOU 2017:39 s. 148.

²⁶⁵ Article 29 Data Protection Working Party, (2009), WP160, s. 5.

²⁶⁶ Art. 8.3 i allmän dataskyddsförordning (EU) 2016/679.

²⁶⁷ Art. 4.25 i allmän dataskyddsförordning (EU) 2016/679; Art. 1.1 (b) i Europaparlamentets och rådets (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (kodifiering).

²⁶⁸ Detta har även framförts vid Roundtable on the GDPR and children’s rights, Session 6, Geary Patrick, s. 19,

<<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-20).

²⁶⁹ Macenaite & Kosta, s. 171, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-17).

²⁷⁰ Detta har även framförts vid Roundtable on the GDPR and children’s rights, Session 6, Geary Patrick, 23 June 2017, s. 19,

<<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-20).

²⁷¹ Macenaite & Kosta, s. 171, <https://doi.org/10.1080/13600834.2017.1321096>, (besökt: 2017-12-17); van der Hof, S. & Lievens, E., *The General Data Protection Regulation and children’s rights: questions and answers for legislators, DPA:s, industry, education, stakeholders and civil society*, Roundtable report, Brussels, 23 June 2017, – Session 2: *Identification of children’s rights issues in the implementation of the GDPR*, s. 11, <<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-21).

Baker and McKenzie LLP, *Consent under the GDPR*, 2016, s. 4, <<http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Consent%20under%20the%20GDPR.pdf>> (besökt 2017-12-01);

Bird & Bird, *Bird & Bird & guide to the General Data Protection Regulation*, Maj 2017, s. 16, <<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>>, (besökt 2017-12-01).

²⁷² SOU 2017:39 s. 144 ff.; Baker and McKenzie LLP, *Consent under the GDPR*, 2016, <<http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Consent%20under%20the%20GDPR.pdf>>, (besökt: 2017-12-09).

²⁷³ Council of the European Union, *Note from Presidency to Working Party on Information Exchange and Data Protection*, 11028/14, Brussels, 30 June 2014, fotnot 86, s. 87.

Skulle en tjänst vara förebyggande eller rådgivande ska den inte omfattas av förordningens art. 8. Vad som avses med en förebyggande eller rådgivande tjänst framgår emellertid inte av förordningen.²⁷⁴ Detta har inte heller diskuterats i SOU 2017:39. BRIS har kritiserat utredningen på denna punkt och begärt att det ska förtydligas vad som avses med undantaget även om de är positiva till detta.²⁷⁵ Art. 29-gruppen har enbart kortfattat framfört att en socialtjänst eller annat skydd för barn som erbjuds genom, exempelvis, en online-chatt ska omfattas av begreppet.²⁷⁶

Kravet på att tjänsten ska vara direkt riktad till barn har tolkats i SOU 2017:39 som att både tjänster som direkt marknadsförs till barn och tjänster som på grund av sin utformning, sitt innehåll eller sin funktion, ska omfattas av begreppet. Utredningen hänvisar dock till vidare vägledning av art. 29-gruppen.²⁷⁷ I art. 29-gruppens riktlinjer, som publicerades i början av december 2017, framförs det att när det för potentiella användare av en tjänst tydligt framgår utifrån sidans innehåll och marknadsföring att tjänsten är avsedd för personer över 18 år så ska tjänsten inte vara direkt riktad till barn.²⁷⁸ Milda Macenaite & Eleni Kosta påpekar dock problematiken kring att barn kan ha åtkomst till och nyttja sidor som visserligen inte är riktade sig till dem, men däremot en generell publik. Som exempel belyser de att YouTube, Facebook och Google inte riktar sig direkt till barn men att många av användarna är barn under 16 år.²⁷⁹ Frågan har även lyfts av BIK²⁸⁰ som belyser att personuppgiftsansvariga i princip kommer behöva veta exakt vilka deras användare/kunder verkligen är för att kunna uppfylla ansvarskraven som ställs på dem enligt förordningen.²⁸¹ Att ha vetskap om sin kundkrets kan därmed bli ett krav för alla som erbjuder tjänster för informationssamhället. Endast ett uttalande från den personuppgiftsansvarige att denne inte direkt riktar sina tjänster till barn kommer troligtvis inte heller vara tillräckligt, utan den personuppgiftsansvarige kommer behöva visa att så inte är fallet.²⁸²

Enligt art. 29-gruppen kommer art. 8 i förordningen ställa ytterligare krav på den personuppgiftsansvarige i förhållande till samtycket. Gruppen har framfört att personuppgiftsansvariga ska återkoppla till barn som använder deras tjänster när de uppnår sådan ålder att de får lämna giltiga samtycken.

²⁷⁴ Skäl 38 i allmän dataskyddsförordning (EU) 2016/679.

²⁷⁵ Jägerskog, Magnus, Bris, *Bris yttrande på betänkande Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*, SOU 2017:39, 2017, s. 3 – 4.

²⁷⁶ Article 29 Data Protection Working Party (2017) WP259, s. 27.

²⁷⁷ SOU 2017:39, s. 147.

²⁷⁸ Article 29 Data Protection Working Party (2017) WP259, s. 24.

²⁷⁹ Macenaite & Kosta, s. 172 ff, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-20).

²⁸⁰ Se beskrivning av BIK ovan i stycke 1.5.

²⁸¹ Geary, Patrick, The General Data Protection Regulation and children's rights: questions and answers for legislators, DPA:s, industry, education, stakeholders and civil society, Roundtable report, Brussels, 23 June 2017: *Session 6: Article 8, parental consent and codes of conduct*, s. 19, <<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-20)

²⁸² Geary, Patrick, s. 19, <<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-20)

Den personuppgiftsansvarige ska då även begära in nya samtycken från barnet själv eftersom tidigare samtycken lämnats av barnets vårdnadshavare. Anledningen till detta är att samtycket, till sin natur, är personligt.²⁸³

En annan problematik som har belysts rörande art. 8 i förordningen är hur vårdnadshavares samtycke rent faktiskt ska inhämtas.²⁸⁴ Enligt förordningens art. 8.2 är det den personuppgiftsansvarige som är ansvarig för att ha vidtagit rimliga ansträngningar för att försäkra sig om att ett giltigt samtycke har lämnats, eller godkänts, av den som har föräldraansvaret för barnet i förhållande till den teknik som finns tillgänglig. Kan den personuppgiftsansvarige alltså visa att rimliga åtgärder har vidtagits har de uppfyllt sin skyldighet enligt art. 8. En verifikation ska ske innan ett barns personuppgifter insamlas. Milda Macenaite & Eleni Kosta påpekar emellertid att vad som avses med ”rimliga ansträngningar” i förordningen är oklart.²⁸⁵

Art. 29-gruppen har vidare i sina riktlinjer för hur samtycket ska tolkas i förordningen föreslagit att personuppgiftsansvariga ska beakta dataminimeringskravet i art. 5.1 (c) för att verifiera att ett samtycke är lämnat av rätt person. Som regel ska alltså verifikationen i sig genomföras med användning av så få personuppgifter som möjligt. En proportionerlig mängd personuppgifter skulle, enligt art. 29-gruppen, kunna vara att enbart samla in kontaktinformation till den/de som har föräldraansvaret. För behandlingar med låga risker för registrerade kan det emellertid vara proportionerligt att enbart samla in uppgifter så att en e-postbekräftelse kan skickas till den föräldraansvarige. För behandlingar med höga risker kan fler personuppgifter behövas för en verifiering. Art. 29-gruppen har framfört att hur komplicerat det är verifiera vem som lämnat samtycke i det enskilda fallet kan påverka vad som ska anses vara rimliga åtgärder för att försäkra sig om detta. Som exempel har art. 29-gruppen beskrivit situationen att en webbsida för onlinespel frågar efter användarens ålder. Om användaren anger att denne är under 16 år ska tjänsten upplysa användaren om att ett föräldrasamtycke krävs för att den ska få användas. Barnet ska då ange vårdnadshavarens e-postadress. Tjänsten ska sedan kontakta och ta ”lämpliga steg” för att verifiera vårdnadshavarens samtycke.²⁸⁶ Som Milda Macenaite framhåller i artikeln *From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation* kan det emellertid uppstå stora problem att verifiera barns ålder eftersom det generellt saknas säkra verktyg för att göra detta. Barn kommer även, med största

²⁸³ Article 29 Data Protection Working Party (2017) WP259, s. 26 f.

²⁸⁴ van der Hof & Lievens, s. 11,

<<https://biblio.ugent.be/publication/8528975/file/8528976>> (besökt: 2017-12-20); Macenaite & Kosta s. 175; <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-20); Article 29 Data Protection Working Party (2017) WP259, s. 25.

²⁸⁵ Macenaite & Kosta, s. 177, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-22).

²⁸⁶ Article 29 Data Protection Working Party (2017) WP259, s. 25 f.

sannolikhet, hitta nya vägar runt verifieringssystemen för att själva kunna lämna samtycke.²⁸⁷

Vidare ska det särskilt belysas att art. 8 i förordningen inte är harmoniserande för medlemsstaterna inom EU. Istället har förordningen gett medlemsstaterna möjligheten att i nationell rätt sänka åldern för barns möjlighet att lämna giltiga samtycken till minst 13 år. Som art. 29-gruppen har belyst kommer detta att medföra att personuppgiftsansvariga som erbjuder tjänster till flera medlemsstater kommer behöva följa ålderskravet i respektive medlemsstat.²⁸⁸

I det svenska lagförslaget har det föreslagits att sänka åldern för giltiga samtycken lämnade av barn till 13 år. Förslaget motiveras i SOU 2017:39 med, bland annat, att barn i Sverige är välinsatta i informationssamhällets medium och att denna plattform utgör en stor del av deras vardagliga liv. En hög åldersspärr skulle därmed kunna utgöra en begränsning av barns informationsfrihet.²⁸⁹ Detta är ett argument som delats av Milda Macenaite samt organisationen BIK. Både Milda Macenaite och BIK har även framfört vikten av att barn måste få verka på och uppleva för internet för att kunna utvecklas och lära sig förstå användandet av plattformen.²⁹⁰

I SOU 2017:39 framhålls att det för närvarande saknas säkra åldersspärrar som kan garantera att den angivna åldersgränsen kommer efterföljas. I utredningen framförs även att en problematik med att bestämma åldersgränsen i svensk rätt är att en liknande åldersreglering inte har funnits på detta område. Det har därmed saknats vägledning i frågan. Samtidigt har utredningen påpekat att barn i svensk rätt vanligen bedöms ha uppnått sådan mognad och förståelse att de kan fatta rättsliga beslut från 15 eller 16 års ålder. I utredningen antogs att en lägre ålder troligtvis kommer att införas i övriga medlemsstater inom unionen. Utredningen menar därmed att detta är ett incitament för att sänka åldern i svensk rätt. Sammantaget ansåg utredningen att oklarheten kring hur föräldrars samtycken ska kunna verifieras och att en hög åldersgräns kommer begränsa barns informations- och yttrandefrihet, samt deras självbestämmanderätt, motiverade förslaget på att sänka åldersgränsen till 13 år.²⁹¹

Det svenska förslaget att sänka åldersgränsen till 13 år har mött både kritik och medhåll från vissa av remissinstanserna. Det har bland annat framhållits

²⁸⁷ Macenaite, 775 f,
<<http://journals.sagepub.com/ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>,
(besökt 2017-12-22).

²⁸⁸ Article 29 Data Protection Working Party (2017) WP259, s. 25.

²⁸⁹ SOU 2017:39, s. 157 f.

²⁹⁰ Macenaite, s. 767 - 772,
<<http://journals.sagepub.com/ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>,
(besökt 2017-12-22), Livingstone, Sonia, *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPA:s, industry, education, stakeholders and civil society*, Roundtable report, Brussels, 23 June 2017, – *Session 3: Do children understand the commercial nature of the internet*, 2017, s. 14 f.
<<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-22).

²⁹¹ SOU 2017:39, s. 150 – 158; Skäl 38 i allmän dataskyddsförordning (EU) 2016/679.

i flertalet yttranden att de konsekvenser som en hög, respektive låg, åldersgräns medför inte är tillräckligt väl underbyggda i utredningen för att i ett första skede kunna avvika från den standardålder på 16 år som angetts i förordningen. Vidare har det ansetts nödvändigt och av stor vikt att barn ska ha uppnått sådan ålder att de förstår konsekvenserna av ett samtycke för att kunna lämna detta. Denna ålder har generellt bland instanserna ansetts uppnådd runt 15 års ålder, vilket ligger i linjen med Datainspektionens praxis. Vissa av remissinstanserna har även varit skeptiska till att träda ifrån förordningens åldersgräns på 16 år med argumentet, som gjordes i utredningen, att andra medlemsstater eventuellt kan komma sänka åldersgränsen. Remissinstanserna har istället ansett att det vore att föredra, med beaktande av barns särskilda skyddsvärde, att utgå från den högre åldern och vid behov sänka denna i ett senare skede.²⁹²

Några av de remissinstanser som har yttrat att de tillstryker förslaget har i sin tur framfört, likt utredningen, att internet och sociala medier idag används i princip av samtliga ungdomar i Sverige redan från en mycket ung ålder och att detta användande är en stor del av deras vardagliga liv.²⁹³ Remissinstansen Surfa lugnt.se har till och med uttryckt en djup oro över att begränsa barns frihet till internet genom att införa en hög åldersgräns. Anledningen var att de menade att det inte går att utgå ifrån att unga kommer få sina föräldrars samtycke.²⁹⁴ BRIS framförde att de visserligen efterlyser en djupare utredning kring hur åldersgränsen kan påverka barns integritet, men att de anser att en hög åldersgräns mycket kraftigt kan begränsa barns liv. BRIS belyste även den eventuella problematiken som kan uppstå om barnets relation med den som har föräldraansvaret är dålig. De menade att en hög åldersgräns för att lämna samtycke i sådana fall snarare kan skapa en falsk trygghet rörande barnets personliga integritet.²⁹⁵ Denna problematik har även tagits upp av både Milda Macenaite och organisationen BIK. Båda lyfter fram

²⁹² Riksdagens ombudsman, *Yttrande över betänkandet Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)*, 2017 s. 2; Datainspektionen, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag*, 2017, s. 9 f.;

Socialpedagogiska skolmyndigheten, *Svar på remiss gällande Ny dataskyddslag – kompletterande bestämmelser till EU:s dataskyddsförordning*, SOU 2017:39, 2017; Länsstyrelsen Skåne, *Ny dataskyddslag (SOU 2017:39) Kompletterande bestämmelser till EU:s dataskyddsförordning*, 2017; Skolverket, *Yttrande över SOU 2017:39: Betänkande av dataskyddsutredningen*, 2017; Skolinspektionen, *Yttrande över betänkandet Ny dataskyddslag (SOU 2017:39)*, 2017; Uppsala universitet, *Remiss av betänkandet Ny dataskyddslag*, SOU 2017:39, 2017, s. 6; Umeå universitet, *Yttrande över betänkandet Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning*, SOU 2017:39, 2017, s. 1 f.; Sveriges konsumenter, *Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning*, 2017, s. 2.

²⁹³ Socialstyrelsen, *Socialstyrelsens yttrande över betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)*, 2017; Centrala studiestödsnämnden, *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)*, 2017; Surfa lugnt.se, *Yttrande: Ny dataskyddslag SOU 2017:39*, 2017; Sveriges Television Ab, *Yttrande över SOU 2017:39, Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning*, 2017, s. 1 f.; Bris, *Bris yttrande på betänkande Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*, SOU 2017:39, 2017, 1 f.

²⁹⁴ Surfa lugnt.se, remissyttrande.

²⁹⁵ Bris, remissyttrande, s. 1 f.

att föräldrar inte alltid fattar de bästa besluten för sina barn och att de kan sakna insyn i vikten för barn att kunna röra sig på internet.²⁹⁶ Milda Macenaite och Eleni Kosta menar även att föräldrar kan komma att begränsa barns rättigheter samt drabbas av ”informationströtthet” av att behöva ständigt lämna nya samtycken.²⁹⁷

Art. 29-gruppen har uppmanat medlemsstaterna att försöka harmonisera området²⁹⁸. I skrivande stund ser det däremot ut som att det kommer bli ett delat landskap inom EU. Eva Lievens och Ingrida Milkaité har fört en kontinuerlig kartläggning av lagstiftningsarbetet inom Europa. Första publikationen av deras kartläggning gjordes den 19 juni 2017 och denna uppdaterades senast den 12 oktober 2017. I den senast uppdaterade kartläggningen framgår att Tyskland, Litauen och Luxemburg har bestämt åldersgränsen till 16 år, medan Ungern och Nederländerna har lagt fram denna ålder som förslag till nationell lag men ännu inte antagit dessa. Österrike har bestämt åldersgränsen för samtycke till 14 år, medan Irland och Storbritannien bestämt den till 13 år. Spanien, Polen, Danmark, Tjeckien och Finland har, förutom Sverige, lagt fram som förslag att sänka åldern för barns giltiga samtycke till 13 år.²⁹⁹

Huruvida förslaget på att sänka åldersgränsen i svensk rätt består eller inte får tiden utvisa. Skulle åldersgränsen sänkas i svensk rätt har det dock lämnats förslag på att dataskyddslagen ska kompletteras på sådant sätt att lagen ska vara tillämplig enligt effektlanssprincipen i förhållande till behandlingen av personuppgifter av barn. Detta för att garantera att alla barn som befinner sig i Sverige ska omfattas av samma rättigheter.³⁰⁰

4.2.3 Uttryckligt samtycke

Som huvudregel är det förbjudet att hantera känsliga personuppgifter i förordningen, se art. 9.1. Detsamma har varit gällande i PUL, se 13 § PUL. Enligt 15 § PUL har det varit möjligt att hantera känsliga personuppgifter om den registrerade lämnat sitt uttryckliga samtycke³⁰¹. Med uttryckligt

²⁹⁶ Macenaite, s. 772 f.,

<<http://journals.sagepub.com/ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>, (besökt 2017-12-22); De Geest, C., Parola, A. m.fl., *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPA:s, industry, education, stakeholders and civil society, Roundtable report, Brussels, 23 June 2017, Session 5: Challenges for DPAs, industry, parents and children*, <<https://biblio.ugent.be/publication/8528975/file/8528976>>, (besökt: 2017-12-29).

²⁹⁷ Macenaite & Kosta, s. 171, <<https://doi.org/10.1080/13600834.2017.1321096>>, (besökt: 2017-12-30).

²⁹⁸ Article 29 Data Protection Working Party (2017) WP259, s. 25.

²⁹⁹ Lievens, E. och Milkaité, I., *Age of consent in the GDPR: updated mapping*, <<https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355>>, (besökt 2017-12-20).

³⁰⁰ Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39), s. 8.

³⁰¹ Petersson och Reinholdsson, s. 125.

samtycke menas att samtycket ska ha kommit till uttryck på ett särskilt tydligt sätt³⁰².

Vad som definieras som känsliga personuppgifter har beskrivits ovan i avsnitt 3.2.2. I förordningen framgår av art. 9.2 (a) att ett uttryckligt samtycke från den registrerade även fortsatt kommer att vara ett giltigt undantag för att hantera känsliga personuppgifter.³⁰³ För att behandlingen av känsliga personuppgifter ska vara giltig krävs det, utöver uttryckligt samtycke enligt art. 9.2, att behandlingen uppfyller villkoren i art. 5 samt någon av de lagliga grunderna i art. 6.³⁰⁴

I förordnings art. 9.2 (a) ges det möjlighet att i nationell rätt, eller i unionsrätten, föreskriva undantag gällande enskildas befogenhet att lämna giltiga samtycken och därmed upphäva det generella förbudet mot att behandla känsliga personuppgifter.³⁰⁵ Denna möjlighet fanns även i direktivet, men i PUL infördes ingen sådan begränsning.³⁰⁶ I prop. 1997/98:44 ansågs det nämligen att när en registrerad lämnat ett frivilligt samtycke för en behandling saknas det ett integritetsskyddande intresse som gör det proportionerligt att förbjuda behandlingen.³⁰⁷ Motivet i propositionen följde därmed datalagskommitténs linje i SOU 1997:39. Den menade att den enskildes självbestämmanderätt över vilka personuppgifter denne vill lämna ut och bedömer är känsliga inte ska begränsas med hänsyn till självbestämmanderätten.³⁰⁸ I SOU 2017:39 hänvisar utredningen till datalagskommitténs motivering i SOU 1997:39 som grund för bedömningen att någon begränsning av den registrerades befogenhet att lämna samtycke för behandlingar av känsliga personuppgifter inte ska införas i den nya kompletterande dataskyddslagen.³⁰⁹

Uttryckligt samtycke krävs även när den personuppgiftsansvarige vill genomföra automatiserad behandling och profilering, se art. 22.2 (c), eller när denne vill överföra den registrerades uppgifter till ett tredje land som saknar adekvat³¹⁰ skydd för personuppgifterna, se art. 49.1 (a). Profilering definieras i förordnings art. 4.4 såsom alla former av automatiska behandlingar som har till syfte att tillstyrka den registrerade vissa personliga egenskaper och i synnerhet analysera och förutsäga dennes beteenden eller preferenser. Att klassificera personer utifrån ålder eller kön skulle därmed kunna falla under begreppet enligt art. 29-gruppen. Vanligen sker profilering från data som

³⁰² Datainspektionens beslut, *Tillsyn enligt personuppgiftslagen (1998:204)*, dnr. 1938–2010.

³⁰³ Art. 9 i allmän dataskyddsförordning (EU) 2016/679.

³⁰⁴ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN, WP251, s. 22.

³⁰⁵ Art. 9.2 (a) i allmän dataskyddsförordning (EU) 2016/679.

³⁰⁶ Öman och Lindqvist, personuppgiftslagen, kommentaren till 15 §, Zeteo, (2017-12-06),

³⁰⁷ Prop. 1997:98: 44, s. 68.

³⁰⁸ SOU 1997:39, *Integritet, Offentlighet, Informationsteknik* s. 372 f.

³⁰⁹ SOU 2017:39, s. 166.

³¹⁰ Personuppgifterna ska ha ett likvärdigt skydd i tredje land med det skydd som finns i förordningen för att uppfylla kravet på adekvat skydd.

kommer från tredje part och inte direkt från den registrerade. Vid profilering ska den personuppgiftsansvarige, för att uppfylla informationskravet och öppenhetsprincipen, lämna information till den registrerade om att dennes uppgifter behandlas. Den personuppgiftsansvarige ska även förklara syftet samt konsekvenserna med behandlingen.³¹¹

Vid överföring av personuppgifter till tredje land ska uttryckligt samtycke lämnas för de specifika överföringarna. Ett generellt samtycke om överföringar kommer därmed inte vara giltigt även om det är uttryckligt (jfr. kraven på samtycke ovan). För att informationskravet ska vara uppfyllt måste den registrerade vara informerad om riskerna med överföringen och att samma säkerhet som erhålls under förordningen inte kan garanteras. Registrerade ska även delges vem som ska motta uppgifterna samt var de ska överföras.³¹²

Vad som ska avses med *uttryckligt samtycke* i förordningen framgår inte.³¹³ Art. 29-gruppen har framhållit att eftersom begreppet *samtycke* fått en striktare innebörd i förordningen bör det klargöras vilka krav som behöver uppfyllas för att det ska röra sig om ett *uttryckligt samtycke*. Kravet på uttrycklighet är kopplat till hur samtycket lämnas av den registrerade. Det finns inget formkrav för hur uttryckligt samtycke ska lämnas, men det skulle exempelvis kunna lämnas genom ett undertecknat skriftligt yttrande. Då kan även den personuppgiftsansvarige tydligt visa att ett samtycke har lämnats. Uttryckliga samtycken kan även lämnas muntligt, genom att samtycket spelas in, eller elektroniskt genom en elektronisk signatur. Art. 29-gruppen föreslår att s.k. tvåstegsverifiering kan användas för att säkerställa att uttryckligt samtycke har lämnats, exempelvis genom att den registrerade uttrycker sitt samtycke och sedan bekräftar detta genom ytterligare en handling, såsom en e-postbekräftelse med en länk.³¹⁴ Intresset för den personuppgiftsansvarige att kunna tydligt visa att ett uttryckligt samtycke har lämnats är av stor vikt om denne vill undvika rättsliga sanktioner. Detta kommer troligtvis bidra med att främst skriftliga samtycken kommer inhämtas eftersom de ska anses vara uttryckliga.³¹⁵

³¹¹ Article 29 Data Protection Working Party (2017) WP251, s. 6 – 9, 13, 20.

³¹² Voigt och von dem Bussche, s. 118 f.

³¹³ Article 29 Data Protection Working Party (2017) WP251, s. 12.

³¹⁴ Article 29 Data Protection Working Party (2017) WP259, s. 18 f.

³¹⁵ Article 29 Data Protection Working Party (2011) WP187, s. 25 ff., Jay s. 101.

5 Analys

Samtycke ska vara den rättsliga grund som ger den registrerade störst möjlighet att reglera och bibehålla kontrollen över sina personuppgifter. För den personuppgiftsansvarige är *samtycket*, med beaktande av den registrerades möjlighet att när som helst återta detta, det mest osäkra av de lagliga grunderna som anges i förordningens art. 6. Kraven på hur ett giltigt samtycke ska lämnas i förordningen efterliknar till stor del de krav som ställts i PUL, men genom striktare ska-krav, nya begränsningar och framförallt ett förtydligt personuppgiftsansvar kommer förordningen ändå att medföra en hel del förändringar för den personuppgiftsansvarige som vill använda sig av samtycke.

5.1 Villkor, rättigheter och ansvar

Något som framförallt har förtydligats och kodifierats i förordningen är informationskravet. Informationskravet har stärkts genom att kravet på öppenhet har förtydligats i förordningen. Det är emellertid sannolikt att kravet på öppenhet kommer att stärkas ytterligare framöver. Detta kommer enligt min bedömning, mot bakgrund av förordningens syfte, att ge registrerade personer ökad kontroll över sina personuppgifter, att ske genom prejudicerande avgöranden eller vägledande riktlinjer från EU-domstolen och unionsgemensamma organ samt nationella domstolar och tillsynsmyndigheter efter att dessa har tolkat förordningen och dess innebörd.

Som bland andra Shara Monteleone har anfört att användandet av privacy policys i form av långa juridiska texter ett vanligt sätt för många personuppgiftsansvariga att lämna information till registrerade. Att information lämnas på detta sätt kommer, som art. 29-gruppen har anfört, inte vara förenligt med förordningen. Detta framkommer tydligt av art. 7.2 i förordningen som ställer ett uttryckligt krav på att information om en behandling som kräver samtycke ska lyftas ut och tydliggöras i förhållande till övriga delar av ett avtal eller andra skriftliga förklaringar. Kravet i art. 7.2 kommer omfatta alla avtal, från anställningsavtal till allmänna villkor. För att uppfylla art. 7.2 kommer personuppgiftsansvariga behöva lämna all information om samtycke och behandling separat eller på annat sätt tydligt separera den ifrågasvarande informationen i förhållande till annan text.

I förordningen ställs även tydligare krav på vilken information som ska lämnas vid insamlandet av personuppgifter. I såväl direktivet som i PUL har kravet på vilken information som ska lämnas i stort sett varit likvärdigt med kravet i förordningen. Kravet i direktivet och PUL har emellertid kunnat tillämpas i olika utsträckning utifrån vilken behandling som har genomförts och vad ändamålet med behandlingen har varit. I förordningen kommer det dock, vid insamling av personuppgifter, att vara ett krav på att all information som anges i art. 13 ska lämnas. Den tidigare, enligt direktivet och PUL,

gällande ordningen kommer efter förordningens ikraftträdande därmed endast vara tillämplig i situationer när personuppgifter inte insamlas utan endast ytterligare behandlingar av uppgifterna sker. Personuppgiftsansvariga behöver därför se över vilken information de lämnar till registrerade när de samlar in personuppgifter genom samtycke.

Det är författarens uppfattning att omfattningen av den information som ska lämnas vid insamlandet av personuppgifter kommer bidra till att registrerade blir mer medvetna om sina rättigheter i förhållande till personuppgiftsansvariga. Informationen kommer även göra de registrerade mer medvetna om hur de kan utöva sin rätt. Denna förändring kommer främst bli märkbar i förhållande till de personuppgifter som har behandlats med stöd av missbruksregeln eftersom skyldigheten för personuppgiftsansvariga att lämna information varit undantaget sådan behandling. Vidare kommer registrerade personer i större omfattning kunna motsätta sig sådana behandlingar eftersom de, om behandlingen bygger på samtycke, kommer kunna återta samtycket vilket inte varit möjligt tidigare. Detta bidrar till att registrerade får en ökad medvetenhet och kontroll över sina personuppgifter.

Att den personuppgiftsansvarige enbart behöver lämna information om sin identitet och hur denne kan kontaktas har i skäl 42 i förordningen ansetts kunna vara tillräckligt för att en behandling ska vara informerad. Med beaktande av de krav som ställs i art. 7 i förordningen anser jag att detta enbart torde vara tillämpligt i de fall en ytterligare behandling sker och personuppgifter inte behöver insamlas.³¹⁶

Kravet på att information om den registrerades rätt att återta sitt samtycke ska lämnas är nytt, men rätten att återta ett samtycke har funnits både i PUL och i direktivet. Rätten för enskilda att återta ett lämnat samtycke är en förutsättning för den enskildes självbestämmanderätt. Den nya framträdande plats denna rättighet har i förordningen genom art. 7.3 visar på ambitionen att öka registrerades kontroll över sina personuppgifter och vikten av självbestämmanderätten för den registrerade. Den personuppgiftsansvariges ansvarsskyldighet kommer även att bli mer omfattande i förordningen. Personuppgiftsansvariga kommer inte, till skillnad från i direktivet och PUL, vara skyldiga att inte enbart avsluta de behandlingar denne genomför. Om den registrerade begär att uppgifterna raderas ska den personuppgiftsansvarige även informera andra personuppgiftsansvariga som behandlar uppgifterna om att denna begäran har gjorts. Enligt min mening kan denna skyldighet bli mycket betungande för personuppgiftsansvariga med beaktande av dagens globaliserade samhälle. Det är emellertid för närvarande oklart hur betungande denna skyldighet kommer att bli för den personuppgiftsansvarige.

Det är den personuppgiftsansvarige som ska visa att ett giltigt samtycke har lämnats. Detta innebär att den personuppgiftsansvarige även ska kunna visa att den registrerade har lämnat en entydig bekräftande handling eller tydligt

³¹⁶ Jfr. art. 29-gruppens inställning i WP259, 2017.

uttryckt att den registrerade samtycker till en behandling av dennes personuppgifter. I förordningen förtydligas och begränsas därmed vad som kan utgöra en otvetydig viljeyttring. Passivitet och inaktivitet kommer inte att kunna utgöra giltiga samtycken, vilket begränsar hur en personuppgiftsansvarig kan inhämta sådana i förhållande till direktivet. Detta ligger däremot i linje med vad som har varit gällande i PUL. Det kan diskuteras huruvida ett konkludent handlande kommer att kunna ses som en entydig bekräftande handling enligt förordningen. Ett konkludent handlande utgör dock ett realhandlande som gör det osannolikt att sådant handlande inte ska ses som en entydig bekräftande handling. Personuppgiftsansvariga bör ändå finna och utveckla nya sätt för att inhämta samtycken som de kan använda för att visa att de tydligt uppfyller kraven som ställs enligt förordningen. I förordningen har det exemplifierande uttryckts att markerandet av en kryssruta utgör en otvetydig viljeyttring. Det är mot denna bakgrund, enligt min mening, sannolikt att det kommer att bli fler kryssrutor för registrerade att kryssa i eftersom en registrerad härmed, på ett enkelt sätt, avger en otvetydig viljeyttring. En registrerad kan samtidigt på ett tydligt, lättöverskådligt och enkelt sätt välja vilka specifika ändamål denne vill samtycka till.

Det kan dock, enligt min uppfattning, ifrågasättas huruvida det skärpta informationskravet och det skärpta kravet på vad som utgör en otvetydig viljeyttring kommer att medföra någon större förändring av hur registrerade väljer att ta del av den information som lämnats av personuppgiftsansvariga. Det har framförts av, bland andra, art. 29-gruppen, BIK och Milda Macenaite att många registrerade idag lider av en informationströtthet och därför inte tar del av den information som lämnas. Det är, enligt min mening, därmed tveksamt om de nya kraven kommer att få registrerade att börja ta till sig den lämnade informationen och inte bara vanemässigt lämna sitt samtycke utan att veta vad behandlingen innefattar. Rättsläget är således oklart avseende vilka åtgärder som kommer att krävas av den personuppgiftsansvarige för att kunna säkerställa att informationskravet är uppfyllt.

Det har påtalats av art. 29-gruppen att det är viktigt att en personuppgiftsansvarig har kännedom om vilka som använder dennes tjänster. Anledningen till detta är att den personuppgiftsansvarige ska utforma den information som lämnas på ett korrekt sätt i förhållande till en användares ålder och förståelse. Det är för närvarande oklart vilka åtgärder en personuppgiftsansvarig kommer att behöva vidta, och i vilken omfattning, för att inhämta den kunskapen.

Generella samtycken har varit otillåtna i PUL och kommer alltså vara det i förordningen som emellertid förtydligar kravet på att den enskilde endast kan samtycka till specifika ändamål. Det framgår i skälen till förordningen att det kommer presumeras att ett lämnat samtycke inte är giltigt om den registrerade inte kan välja vilka specifika ändamål den registrerade vill samtycka till. Detta framgår även särskilt rörande skriftliga avtal eller villkor i art 7.4 i förordningen. Det är därmed sannolikt, enligt min uppfattning, att denna rätt kommer få en striktare tillämpning i förordningen än i PUL. Det även min

uppfattning att detta kan påverka den tolkning av rätten till valfrihet som tidigare gjorts av Öman och Lindblom i PUL. De har framfört att om den registrerade kan välja mellan en likvärdig tjänst som erbjuds av två olika personuppgiftsansvariga, varav endast en personuppgiftsansvariga kräver att den registrerade samtycker till att denne får behandla den registrerades uppgifter, så kan den registrerade göra ett frivilligt val och därmed lämna ett giltigt samtyck. Mot bakgrund av art. 7.4 och art. 29-gruppens tolkning av frågan är det dock min uppfattning att en enskild personuppgiftsansvarig inte kommer kunna ställa ett sådant krav. Den registrerade ska ha friheten att kunna välja om den registrerade vill att dennes uppgifter ska behandlas eller inte utan att behöva välja en annan aktör.

Rosemary Jay har gjort bedömningen att det förstärkta kravet på specifika ändamål och det förstärkta frivillighetskravet kommer att medföra att den registrerades samtycke att lämna personuppgifter för att skapa ett konto på en hemsida eller bli medlem i en butik inte kommer innebära att den registrerade har samtyckt till ändamålet att uppgifterna används för att skicka ut reklam eller nyhetsbrev. Rosemary Jays bedömning är, enligt min mening, överensstämmande med förordningens tillämpning. Särskilt med beaktande av att nyhetsbrev vanligen kan avregistreras utan att detta påverkar den registrerades medlemskap. Detta ska därför även vara fallet avseende köp som genomförs via internet. Samtycke från den registrerade att lämna sina personuppgifter för att kunna genomföra ett köp ska inte betyda att den registrerade även samtyckt till att motta reklam eller nyhetsbrev.

En problematik som, enligt min uppfattning, skulle kunna uppstå när medlemskap ingås i butiker är möjligheten för den personuppgiftsansvarige att visa att ett giltigt samtycke har lämnats. Om butiksbiträdet inte delger den registrerade information på ett sådant sätt att denne förstår vilka specifika ändamål uppgifterna ska användas till och att den registrerade har möjligheten att återta sitt samtycke har inte ett giltigt samtycke lämnats enligt förordningen. Eftersom informationen vanligen i dessa fall lämnas muntligt kan det vara mycket svårt för den personuppgiftsansvarige att visa att den registrerade fått tillräcklig information om den registrerade påstår att tillräcklig information inte har lämnats. Det är därmed sannolikt att personuppgiftsansvariga kommer att behöva ha tydliga instruktioner för sina anställda om vilken information som ska lämnas vid dessa tillfällen. Vidare kommer personuppgiftsansvariga även vara tvungna att se över vilken information de delger registrerade när de samlar in deras personuppgifter så att denna information överensstämmer med den information som ska lämnas enligt art. 13 och art. 14 i förordningen.

Det är svårt att bedöma i vilken omfattning missbruksregeln har använts för att behandla personuppgifter av personuppgiftsansvariga. Med beaktande av att missbruksregeln har undantagit nästintill alla vardagliga automatiserade behandlingar gör jag bedömningen att tillämpningsområdet troligtvis har varit omfattande. Att missbruksregeln upphör kommer därför kräva att samtliga personuppgiftsansvariga i Sverige granskar vilka personuppgifter som har behandlats med stöd av missbruksregeln och, för att dessa ska få

fortsätta behandlas efter den 25 maj 2018, finna en laglig grund i art. 6 i förordningen som tillåter behandling av de ifrågavarande personuppgifterna. Detta innebär att om behandlingen kräver att den personuppgiftsansvarige inhämtar ett samtycke från den registrerade så ska detta samtycke uppfylla samtliga krav som ställs i förordningen. Eftersom missbruksregeln även har varit tillämplig på känsliga personuppgifter krävs det att personuppgiftsansvariga inhämtar giltiga uttryckliga samtycken i de fall ett samtycke krävs för att uppgifterna fortsatt ska kunna behandlas.

Att missbruksregeln upphör kommer, enligt min uppfattning, främst att påverka privata företag. Anledningen till detta är förslaget i SOU 2017:39 om att en ny form av missbruksregeln ska införas i nationell rätt som enbart kommer vara tillämplig för offentliga myndigheter. Den nya regeln kommer emellertid att vara mer inskränkt än missbruksregeln i 5 a § PUL eftersom den endast kommer få tillämpas, utifrån nuvarande förslag, när det är absolut nödvändigt. Även offentliga myndigheter kommer därmed att påverkas av att missbruksregeln försvinner och kommer att behöva se över sina rutiner för hur de har behandlat personuppgifter med stöd av 5 a § PUL.

5.2 När barns samtycke ska lämnas

Giltiga samtycken i direktivet och i PUL har kunnat lämnas av barn oavsett deras ålder så länge de har uppnått sådan mognad och förståelse att de har förstått konsekvenserna av ett samtycke. I förordningen kommer behovet av sådana bedömningar att kraftigt begränsas eftersom en åldersgräns införs genom art. 8. Barn från 16 års ålder kommer kunna lämna giltiga samtycken till informationssamhällets tjänster. I dessa fall kommer den personuppgiftsansvarige därför inte behöva göra någon bedömning i varje enskilt fall av barnets mognad och förståelse. Informationssamhällets tjänster kommer, med beaktande av de tolkningar som gjorts av bland andra art. 29-gruppen samt Milda Macenaite och Eleni Kosta, med stor sannolikhet att omfatta samtliga tjänster som erbjuds via internet.

Art. 8 har införts i förordningen för att särskilt skydda barns personliga integritet eftersom barn generellt har ansetts sakna den mognad som krävs för att förstå konsekvenserna av att lämna ett samtycke. Eftersom åldersgränsen för barn i förordningen är reglerad till 16 år får det antas att det är vid denna ålder som EU-kommissionen gjort bedömningen att ett barn generellt har uppnått den mognad och förståelse som krävs för att lämna ett giltigt samtycke. Art. 8 i förordningen är emellertid inte harmoniserande utan medlemsstaterna har givits möjligheten att sänka ålderskravet i nationell rätt till 13 år. Det är, enligt min uppfattning, ändå oklart huruvida ett barn har uppnått den mognad och förståelse som krävs för att förstå innebörden av ett samtycke vid 13 års ålder.

Som har framförts både av flera remissinstanser och BIK, använder barn idag internet, appar och sociala medier i mycket stor omfattning och de är en integrerad del av barnens vardagliga liv. Barnen är därför vana att navigera sig i dessa digitala miljöer. Frågan är dock när det går att säkerställa att ett

barn generellt har uppnått sådan mognad och förståelse som krävs för att kunna lämna giltiga samtycken.

Trots att informationskravet i förordningen innebär att all information som lämnas till barn ska vara utformad på ett sådant att barnet ska kunna förstå informationen, är det min uppfattning att en låg ålder på 13 år ändå kan komma att försvaga barns personliga skydd. Bakgrunden till denna uppfattning är att Datainspektionen har, i förhållande till PUL, gjort bedömningen att ett barn generellt inte har uppnått en sådan mognad som krävs för att lämna ett informerat samtycke före 15 års ålder. Detta är en bedömning som även baseras på att barn i svensk rätt vanligen har bedömts kunna fatta vissa rättsliga beslut från 15 eller 16 års ålder.

En hög åldersgräns kan emellertid medföra andra risker som kan försvaga barns tilltänka skydd enligt förordningen och utgöra intrång i barns personliga integritet. I de fall den som har föräldraansvaret för barnet vägrar att lämna, eller godkänna, ett samtycke å barnets vägnar kan barnet bli ytterst begränsad i sina möjligheter att ha kontakt med vänner via sociala nätverk eller ta del av information som erbjuds på internet. Genom en hög åldersgräns får den med föräldraansvar även en relativt omfattande insyn i barnets liv vilket i sig kan utgöra en kränkning av barnets privatliv och personliga integritet. Risken för att den med föräldraansvaret ska drabbas av informationströtthet får även anses öka om denne behöver samtycka till ett stort antal tjänster å barnets vägnar i många år. Det föreligger en risk att den med föräldraansvaret inte tar del av den information som lämnas före en behandling utan enbart samtycker till denna å barnets vägnar.

För personuppgiftsansvariga kommer art. 8 till en början medföra ett antal oklarheter kring den personuppgiftsansvariges ansvar och vilka åtgärder denne ska vidta för att uppfylla kraven i förordningen. Exempelvis ska den personuppgiftsansvarige kunna visa att denne har vidtagit alla rimliga åtgärder, med hänsyn till den teknik som finns tillgänglig, för att verifiera att samtycket har lämnats av den som har föräldraansvaret och därmed är giltigt. Ansvar är genom formuleringen i art. 8.2 i förordningen begränsat till att den personuppgiftsansvarige kan visa på att denne vidtagit tillräckliga åtgärder, men det är oklart hur omfattande den personuppgiftsansvariges ansvar är. Speciellt i förhållande till det faktum att barn, med stor sannolikhet, kommer att finna sätt att kringgå de säkerhets- och verifieringssystem som den personuppgiftsansvarige använder sig av. Ansvar för den personuppgiftsansvarige är dock, utifrån min tolkning, utformat så att den personuppgiftsansvarige ska följa den tekniska utvecklingen och kontinuerligt utveckla sina system och rutiner för att kunna uppfylla sitt ansvar och motverka detta.

Art. 8 i förordningen kommer även, enligt min bedömning, ha en påverkan utanför sitt tillämpningsområde på informationssamhällets tjänster. I de fall art. 8 inte är tillämplig får det antas att, med beaktande av att förordningen bygger på direktivet, en bedömning av barnets mognad och förståelse ska ske i varje enskilt fall för att bedöma om barnet kan lämna ett giltigt samtycke.

Genom Datainspektionens praxis har ett barn antagits ha uppnått sådan mognad från 15 års ålder. För det fall åldersgränsen för ett barn att lämna ett giltigt samtycke skulle bestämmas till 13 års ålder i den svenska nationella lagstiftningen, kommer denna ålder med stor sannolikhet, istället för vad som nu är gällande, att bli utgångspunkten vid sådana bedömningar som ska ske i varje enskilt fall.

Huruvida vilken åldersgräns som bör införas i nationell rätt är medlemsstaterna i Europa uppenbarligen delade i sin uppfattning eftersom den nuvarande kartläggningen visar på att medlemsstaterna antingen kommer välja 13 eller 16 år såsom nationell åldersgräns. Det återstår att se hur fördelningen inom Europa kommer att bli innan den 25 maj 2018.

Vilken åldersgräns Sverige bör tillämpa är en svår fråga där olika intressen ställs mot varandra. Vikten av att barn förstår innebörden och konsekvenserna av ett samtycke har varit ett av skälen till att art. 8 har införts i förordningen. Samtidigt har barn rätt till ett ökat självbestämmande utifrån sin mognad och ålder. Enligt min bedömning är det dock mycket viktigt att ta hänsyn till att barn utvecklas olika. Med en högre åldersgräns ökar mognaden och förståelsen bland barn generellt. Risken för att barn ska kunna bli lurade eller samtycka till något de inte förstår minskar därmed genom en högre åldersgräns och barn skulle i större omfattning omfattas av det som är syftet bakom art. 8. Visserligen saknas det i dagsläget säkra verifieringsmetoder för att garantera att barn inte kan kringgå reglerna, men en högre åldersgräns i nationell rätt hade ändå förtydligat barns rätt till skydd enligt förordningen. Min bedömning är därmed att åldersgränsen i nationell rätt bör vara från 15 år såsom har föreslagits av, bland andra Datainspektionen i deras remissvar.

Att art. 8 i förordningen inte är harmoniserande kommer ställa högre krav på personuppgiftsansvariga eftersom de kommer behöva beakta den nationella rätten i alla medlemsstater för att inte drabbas av sanktioner. Den personuppgiftsansvarige kommer även behöva vara medveten om vilka territoriella bestämmelser respektive land tillämpar, så att den personuppgiftsansvarige är medveten om när den nationella rätten blir tillämplig.

Genom att utöka det generella tillämpningsområdet för förordningen gentemot tredje land genom effektlanssprincipen, kommer förordningen att stärka skyddet för de som befinner sig i unionen även på en global skala.

6 Slutsats

Rent juridiskt är rättsläget mellan direktivet, PUL och den allmänna dataskyddsförordningen i förhållande till samtycket vid en första anblick i stort sett detsamma. Men när reglerna granskas närmre framgår det att de förändringar som har skett har förtydligat vad som ska utgöra ett giltigt samtycke. Kraven för att inhämta ett giltigt samtycke har även förstärks och prejudicerande domar såsom C 131/12, *Google Spain*, har kodifierats och givits en mer central roll i förordningen genom bland annat art. 7 och art. 13.

Förordningens inverkan på hur personuppgiftsansvariga ska fullgöra sina skyldigheter och uppfylla de krav som ställs på samtycket är, vid närmare granskning, en betydlig skillnad. Genom att det i förordningen har kodifierats vad som är en otvetydig viljeyttring, att det har tillkommit nya krav på vilken information som *ska* lämnas till registrerade personer och att striktare krav på *hur* information ska lämnas måste personuppgiftsansvariga granska och utveckla sina organisationer eller verksamheter. Personuppgiftsansvarigas skyldigheter har utökats även i förhållande till, bland annat, rätten att återta ett samtycke och därigenom rätten att bli bortglömd eftersom den personuppgiftsansvarige ska kontakta och informera andra personuppgiftsbiträden att denna begäran har lämnats. För personuppgiftsansvariga i Sverige kommer med största sannolikhet en av de största förändringarna vara att 5 a § PUL, missbruksregeln, försvinner i förordningen. Personuppgiftsansvariga kommer behöva granska sina organisationer för att identifiera alla behandlingar som har genomförts med stöd av undantaget, granska dessa och finna lagliga grunder att behandla dessa på. Samtycken kommer behöva inhämtas i tillämpliga fall och när förordningen har trätt i kraft kommer dessa behandlingar att omfattas av samtliga regler i förordningen. En fördel med detta är att personuppgifter, enligt min mening, troligtvis kommer behandlas i en mer begränsad omfattning under förordningen.

Genom den nya regleringen om barns möjligheter att lämna giltiga samtycken kommer personuppgiftsansvariga att, initialt, verka på ett osäkert rättsområde. Det krävs prejudicerande domar som kan ge tydligare riktlinjer om vad som avses med informationssamhällets tjänster, förebyggande och rådgivande tjänster, vad som krävs för att en tjänst ska vara direkt riktad till barn och vilka åtgärder personuppgiftsansvariga ska behöva vidta för att kunna visa att de vidtagit rimliga åtgärder för att verifiera att den som har föräldraansvaret lämnat samtycke å ett barns vägnar. Det är med andra ord i nuläget oklart vilken effekt artikel 8 i förordningen kommer att få i praktiken och om det avsedda syftet kommer kunna uppnås. Det återstår även att se vilken åldersgräns som kommer bli gällande i den nya svenska lagstiftningen.

Förordningen har för registrerade till syfte att öka den personliga integriteten samt stärka den registrerades kontroll över sina personuppgifter. Förordningen har genom att införa striktare krav rörande samtycket givit

registrerade fler möjligheter att uppnå detta syfte. Det nya kravet på att information ska lämnas på ett klart, lättillgängligt och enkelt sätt och att denna information inte får gömmas i långa juridiska avtal kommer göra det enklare för registrerade att ta del av informationen. Kravet på att registrerade ska informeras om sina rättigheter och hur de kan använda dessa kommer öka medvetenheten om vilken kontroll och bestämmanderätt samtycket ger de registrerade. Vidare kommer, enligt min uppfattning, det bli vanligare med skriftliga samtycken för att den personuppgiftsansvarige ska kunna visa att ett giltigt samtycke har lämnats. Detta kommer även förtydliga för registrerade när ett samtycke faktiskt har lämnats. Registrerade kommer med största sannolikhet få en ökad möjlighet att endast samtycka till de behandlingar den registrerade vill samtycka till. Framförallt kommer de få en ökad vetskap om vilka personuppgifter som har hanterats om dem under missbruksregeln.

Förordningen kommer, i förhållande till samtycket, utöka kraven och ansvaret för den personuppgiftsansvarige. Den personuppgiftsansvarige kommer även, enligt min uppfattning, med stor säkerhet att följa de nya reglerna och utveckla sina rutiner. Anledningen till detta är de höga sanktionsavgifter som personuppgiftsansvariga kan bli tvingade att betala om de skulle bryta mot sitt ansvar eller sina skyldigheter enligt förordningen. Eftersom samtycket är ett uttryck för registrerades självbestämmanderätt över sina personuppgifter, och har en särställning såsom den enda lagliga grunden som omnämns både i EKMR och EU-stadgan, kan det antas att brister vid inhämtandet av giltiga samtycken motiverar höga sanktionsavgifter. Personuppgiftsansvariga har mot denna bakgrund ett starkt incitament för att följa förordningens regler rörande samtycke.

Förordningen kommer även genom sina striktare regler ge registrerade, både barn och vuxna, möjligheten att utöka kontrollen över sina personuppgifter och utöva de rättsliga rättigheter som samtycket och förordningen ger dem. För att förordningen ska ge önskad effekt kommer det emellertid krävas att registrerade använder de verktyg som tillhandahålls genom förordningen och intar en aktiv roll när de ska lämna ett samtycke för en behandling. Om en registrerad enbart lämnar ett samtycke utan att ta del av den information som en personuppgiftsansvarig delger kommer de registrerade även fortsatt sakna kontroll över sina personuppgifter. Förordningen kommer att stärka samtycket och utöka personuppgiftsansvarigas ansvarsskyldighet. I slutändan kommer enskilda behöva återta kontrollen över sina personuppgifter och utöva de rättigheter som samtycket ger dem för att en verklig förändring ska kunna ske.

Källförteckning

Tryckta källor

Datainspektionen, *Samtycke enligt personuppgiftslagen*, 2012.

Dr. Gabel, Detlev. och Hickman, Tim., *Unlocking the EU General Data Protection Regulation*, White & Case, 2016.

Larsson, S. & Ledendal, J: *Personuppgifter som betalmedel*, Konsumentverkets rapport 2017:4.

(finns via

<<https://www.konsumentverket.se/globalassets/publikationer/produkter-och-tjanster/gemensamt/rapport-2017-4-personuppgifter-som-betalmedel-konsumentverket.pdf>>)

Sandgren, Clas, *Är rättsdogmatiken dogmatisk?*, Ingår i Tidsskrift for Rettsvitenskap, TfR, Vol. 118, nr 4-5, ; 2005, s. 648-656.

Offentligt tryck

Europeiska unionen

Council of the European Union, *Note from Presidency to Working Party on Information Exchange and Data Protection*, 11028/14, Brussels, 30 June 2014. (finns via <<http://www.statewatch.org/news/2014/jul/eu-council-dp-reg-11028-14.pdf>>).

Sverige

Utredningsbetänkanden

Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39).

SOU 2017:52, Så stärker vi den personliga integriteten.

SOU 2017:39, Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning.

SOU 2016:41, Hur står det till med den personliga integriteten.

SOU 2004:6, Översyn av personuppgiftslagen.

SOU 1997:39, Integritet, Offentlighet, Informationsteknik.

SOU 1999:109, Personuppgiftslag.

Propositioner

Prop. 1997/98:44, Personuppgiftslag.

Remissyttranden

(Samtliga remissyttranden finns på www.regeringen.se.)

Länsstyrelsen Skåne, *Ny dataskyddslag (SOU 2017:39) Kompletterande bestämmelser till EU:s dataskyddsförordning, 2017.*

Surfa lugnt.se, *Yttrande: Ny dataskyddslag SOU 2017:39, 2017.*

Skolverket, *Yttrande över SOU 2017:39: Betänkande av dataskyddsutredningen, 2017.*

Skatteverket, *Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39), 2017.*

Sveriges konsumenter, *Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning, 2017.*

Ulrika m.fl., Datainspektionen, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag, 2017.*

Bris yttrande på betänkande Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning, SOU 2017:39, 2017.

KTH, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag, 2017.*

Riksdagens ombudsman, *Yttrande över betänkandet Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39), 2017.*

Socialpedagogiska skolmyndigheten, *Svar på remiss gällande Ny dataskyddslag – kompletterande bestämmelser till EU:s dataskyddsförordning, SOU 2017:39, 2017.*

Umeå universitet, *Yttrande över betänkandet Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning, SOU 2017:39, 2017.*

Socialstyrelsen, *Socialstyrelsens yttrande över betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39), 2017.*

Sveriges Television Ab, *Yttrande över SOU 2017:39, Ny dataskyddslag, Kompletterande bestämmelser till EU:s dataskyddsförordning, 2017.*

Centrala studiestödsnämnden, *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)*, 2017.

Uppsala universitet, *Remiss av betänkandet Ny dataskyddslag, SOU 2017:39*, 2017.

Skolinspektionen, *Yttrande över betänkandet Ny dataskyddslag (SOU 2017:39)*, 2017.

Elektroniska källor

Annereau, Sally, *Understanding consent under the GDPR*, TaylorWessing, publicerad: November 2016, www.taylorwessing.com/globaldatahub/article-understanding-consent-under-the-gdpr.html.

Baker and McKenzie LLP, *Consent under the GDPR*, 2016, <<http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Consent%20under%20the%20GDPR.pdf>>.

Better Internet for Kids, <<https://www.betterinternetforkids.eu/web/portal/about>>.

Bird & Bird, *Bird & Bird & guide to the General Data Protection Regulation*, Maj 2017, <<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>>.

Datainspektionen, *Missbruksregeln upphör*, <<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/>>.

Datainspektionen, *Samtycke*, <<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/samtycke/>>.

Díaz Díaz, Efren, *The new European Union General Regulation on Data Protection and the legal consequences for institutions*, in Church, Communication and Culture, 1:1, 206-239, Informa UK Limited, Taylor & Francis Group, publicerad 2016-10-27, <<https://doi.org/10.1080/23753234.2016.1240912>>.

Europeiska kommissionen, Article 29 Data Protection Working Party, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=59485>.

Information Commissioners Office (ICO), *Consultation GDPR consent guidance*, 2017, publicerad 2017-02-03, <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>>.

Koščík, Michal, *The Impact of General Data Protection Regulation on the grey literature*, in Grey Journal (TGJ), s.42-45, publicerad 2017-01-02, <<http://eds.b.ebscohost.com.ludwig.lub.lu.se/eds/pdfviewer/pdfviewer?vid=2&sid=2409e5df-3839-43b2-bae6-c75f9be047a9@pdc-v-sessmgr01>>.

Lievens, E. och Milkaité, I., *Age of consent in the GDPR: updated mapping*, <<https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355>>.

Macenaite, Milda, & Kosta, Eleni, *Consent for processing children's personal data in the EU: following in the US footsteps?* in Information & Communications Technology Law, 26:2, 146-197 Informa UK Limited, Taylor & Francis Group, publicerad: 2017-05-10, <<https://doi.org/10.1080/13600834.2017.1321096>>.

Macenaite, Milda, *From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU general Data Protection Regulation*, in new media and society, vol. 19(5), 765-779, publicerad den 16 januari 2017. <<http://journals.sagepub.com.ludwig.lub.lu.se/doi/pdf/10.1177/1461444816686327>>

McDonald, Aleecia M., och Cranor, Lorrie F.: *The cost of reading privacy policies*. In: Proceedings of the Technology Policy Research Conference, 26–28 September 2008. <https://kb.osu.edu/dspace/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf>.

Monteleone, Shara, *Addressing the 'Failure' of informed consent in online data protection: Learning the lessons from behavioraware regulation*, in Macro Draft, publicerad 2016-02-23, <<http://jilc.syr.edu/wp-content/uploads/2015/11/Monteleone-Macro-2-23.pdf>>.

The General Data Protection Regulation and children's rights: questions and answers for legislators, DPA:s, industry, education, stakeholders and civil society, Roundtable report, Brussels, 23 June 2017:

De Geest, Caroline, Parola, Andrea m.fl., *Session 5: Challenges for DPAs, industry, parents and children*. <<https://biblio.ugent.be/publication/8528975/file/8528976>>,

Geary, Patrick, *Session 6: Article 8, parental consent and codes of conduct*. <<https://biblio.ugent.be/publication/8528975/file/8528976>>,

Livingstone, Sonia, *Session 3: Do children understand the commercial nature of the internet*.

<<https://biblio.ugent.be/publication/8528975/file/8528976>>,

van der Hof, Simone & Lievens, Eva, *Session 2: Identification of children's rights issues in the implementation of the GDPR*.

<<https://biblio.ugent.be/publication/8528975/file/8528976>>.

Verdoodt, Valerie & Lievens, Eva, *Data protection and Privacy under Pressure – Targeting Children with Personalised advertising*, s. 323, <<https://biblio.ugent.be/publication/8541057/file/8541058>>.

Article 29 Data Protection Working Party

(Samtliga yttranden och riktlinjer finns på http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 och http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936)

Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation, 2016/679* 17/EN, WP260.

Article 29 Data Protection Working Party, *Guidelines on Consent under the Regulation 2016/679*, 17/EN, WP259, antagen den 28 november 2017.

Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN, WP251, antagen den 3 oktober 2017.

Article 29 Data Protection Working Party, 2/2017, *Opinion on data processing at work*, 17/EN, WP249, antagen den 8 juni 2017.

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN, WP216, antagen den 10 april 2014.

Article 29 Data Protection Working Party, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, 1676/13/EN, WP208, antagen den 2 oktober 2013.

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 0119/11/EN, WP187, antagen den 13 juli 2011.

Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and special case of schools)*, 398/09/EN, WP160, antagen den 11 februari 2009.

Article 29 Data Protection Working Party, *Opinion 8/2001, on the processing of personal data in the employment context*, 5062/01/EN, WP48, antagen den 13 september 2001.

Litteratur

Esayas, Samson, Mahler, Tobias och McGillivray, Kevin, *Is a Picture Worth a Thousand Terms? Visualising Contract terms and Data Protection Requirements for Cloud Computing Users*, in *Current trends in Web Engineering*, Springer International Publishing, 2016.

Holmberg, Erik mfl. Regeringsformen, 2 kap. 6 §, Zeteo, lagkommentar, publicerad 2016-05-13.

Jay, Rosemary, *Guide to the General Data Protection Regulation – A companion to Data Protection Law and Practice 4th edition*, 1: a upplagan, Sweet and Maxwell, Great Britain, 2017.

Linder, Andreas, (Ed.), *European Data Protection Law – General Data Protection Regulation*, 2016.

Peczenik, Alexander, *Juridikens metodproblem: Rättskällelära och lagtolkning*, 2: a upplagan, Almqvist och Wikson, Stockholm, 1980.

Petersson, Roger och Reinholdsson, Klas, *Personuppgiftslagen i praktiken*, 5:e upplagan, Norstedts juridik, Vällingby, 2012.

Voigt, Paul och von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) – A practical guide*, Springer International Publishing, Switzerland, 2017.

Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – en kommentar*, 4:e upplagan, Vällingby, 2011.

Öman, Sören och Lindblom, Hans-Olof, *personuppgiftslagen*, Zeteo, lagkommentar, publicerad 2016-12-20.

Rättsfallsförteckning

EU-domstolen

C-582/14, *Patrick Breyer mot. Bundesrepublik Deutschland*, EU:C:2016:779.

C-230/14, *Weltimmo s.r.o. mot Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639.

C-201/14, *Smaranda Bara m.fl. mot Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, EU:C:2015:461.

C-131/12, *Google Spain SL och Google Inc. mot Agencia Espanola de Protección de Datos (AEPD) och Mario Costeja González*, EU:C:2014:317.

C-297/12, *Michael Schwarz mot Stadt Bochum*, EU:C:2013:670.

C-342/12, *Worten – Equipamentos para o Lar SA mot Autoridade para as Condições de Trabalho (ACT)*, EU:C:2013:355.

C-70/10, *Scarlet Extended SA mot Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, EU:C:2011:771.

C-543/09 *Deutsche Telekom AG mot Bundesrepublik Deutschland*, EU:C:2011:279.

C-553/07, *College van burgemeester en wethouders van Rotterdam mot M.E.E. Rijkeboer*, EU:C:2009:293.

C-524/06, *Heinz Huber mot Bundesrepublik Deutschland*, EU:C:2008:724.

C-397/01-C403/01, *Bernhard Pfeiffer (C-397/01), Wilhelm Roith (C-398/01), Albert Süß (C-399/01), Michael Winter (C-400/01), Klaus Nestvogel (C-401/01), Roswitha Zeller (C-402/01), Matthias Döbele (C-403/01) Och deutsches Rotes Kreuz, Kreisverband Waldshut eV, PFEIFFER M.FL. och Deutsches Rotes Kreuz, Kreisverband Waldshut eV*, EU:C: 2004:584.

C101/01, *Lindqvist mot Åklagarkammaren Jönköping*, EU:C:2003:596.

C-465/00, C138, 139/01, *Rechnungshof (C-465/00) och Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, och mellan Christa Neukomm (C-138/01), Joseph Lauer mann (C-139/01) och Österreichischer Rundfunk*, EU:C:2003:294.

Svenska rättsfall

HFD 2016 nr. 40.

NJA 2015 s. 180.

RÅ 2008 ref. 83.

Datainspektionens beslut

Datainspektionen, *Tillsyn enligt personuppgiftslagen (1998:204) – registrering av känsliga personuppgifter om anställda*, dnr. 120–2017.

Datainspektionens beslut, *Tillsyn enligt personuppgiftslagen*, dnr. 1938–2010.

Datainspektionen, *Beslut efter tillsyn enligt personuppgiftslagen (1998:204)*, dnr. 998–2006.

Datainspektionen, *Beslut efter tillsyn enligt personuppgiftslagen (1998:204)* dnr. 706–2006.