Advokatfirman Kahn Pedersens skriftserie 2017:2

kahn pedersen

GDPR

– några tillämpningsfrågor

På Advokatfirman Kahn Pedersen ser vi det som en naturlig del av vår roll som specialistbyrå att delta i den offentliga diskussionen för att bidra till att föra fram och utveckla intressanta, och inte sällan svåra, rättsfrågor inom våra specialistområden. Ett led i detta arbete är denna skriftserie som kommer ut med ett till två nummer per år. Tanken med skriftserien är att lite mer djupgående utreda aktuella och mer komplicerade rättsfrågor, som vi märker är av intresse för våra klienter och samhället i stort.

Eftersom målsättningen är att vårt arbete inte bara ska komma våra klienter och samarbetspartners till del, utan även ska kunna bidra till utvecklingen av de rättsområden som är våra specialistområden, tillhandahålls alla nummer av skriftserien kostnadsfritt på vår webbplats under en Creative Commons Erkännande-Inga Bearbetningar 4.0 Internationell Licens, vilket möjliggör mångfaldigande och spridning av materialet förutsatt att inga ändringar görs och att källan anges. Innehållet i rapporten utgör inte juridisk rådgivning. Våra reflektioner och bedömningar i rapporten baseras på allmänna utgångspunkter och presenteras i syfte att bidra till en generell diskussion om de rätts- och tillämpningsfrågor som rapporten behandlar. Läsaren uppmanas att inte förlita sig enkom på rapporten vid juridisk analys eller tillämpning, utan att ha först konsulterat sakkunnig jurist för bedömning av de specifika omständigheterna i det enskilda fallet.

Ämnet för denna rapport, som har nummer 2017:2, är EU:s kommande allmänna dataskyddsförordning (GDPR) som ska tillämpas från och med den 25 maj 2018.

ISBN 978-91-983215-3-1

1. Inledning

Varför en rapport om GDPR?

Den 25 maj 2018 ska EU:s allmänna förordning om behandling av personuppgifter (GDPR)[1] börja tillämpas. Syftet med GDPR är bl.a. att skapa ett bättre och mer harmoniserat skydd för fysiska personers fri- och rättigheter vid behandling av deras personuppgifter. Senast den 25 maj 2018 ska således personuppgiftsansvariga ha säkerställt – och kunna visa – att GDPR:s bestämmelser följs, inte minst för att undvika de stora och mycket omdebatterade sanktionsavgifter som kan aktualiseras till följd av bristande efterlevnad av regelverket. Frågor kring GDPR är således högaktuella, särskilt under hösten 2017 och våren 2018, då många personuppgiftsansvariga kommer att genomföra s.k. GDPR-anpassningsprojekt för att identifiera brister i förhållande till GDPR:s krav och genomföra åtgärder i syfte att så långt som möjligt efterleva regelverket.

Vi har mot denna bakgrund valt att fokusera på GDPR i denna rapport. I vår rådgivning kring integritetsskydd har vi tacklat flera viktiga frågor kring tolkning och tillämpning av GDPR. Vid valet av de ämnen som rapporten avhandlar har vi utgått ifrån några av de frågor som är aktuella för våra klienter och som vi anser är intressanta ur ett rättsligt perspektiv och/eller ur ett praktiskt tillämpningsperspektiv. Rapporten innehåller således inte en heltäckande redogörelse över förordningens regelverk. Vi har istället gjort ett urval av ämnen och frågeställningar som vi finner särskilt intressanta och betydelsefulla för tolkningen och tillämpningen av GDPR.

Rapporten vänder sig till alla som arbetar med personuppgiftsfrågor. Vår målsättning med rapporten är att orientera läsaren i några av de utmaningar som GDPR medför, belysa olika frågeställningar som uppstår till följd av regelverket och förhoppningsvis bidra till en bättre förståelse av regelverket.

Disposition

Denna rapport är disponerad på följande sätt. I avsnitt 2 utreder vi roll- och ansvarsfördelning i de fall flera aktörer är inblandade i samma eller närliggande behandlingar av personuppgifter. Vi diskuterar även behovet av att i olika situationer förtydliga aktörers roll- och ansvarsfördelning genom avtalsregleringar. I avsnitt 3 redogör vi för de utökade skyldigheter som GDPR, i jämförelse med PuL, innebär i

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), hädanefter GDPR.

fråga om personuppgiftsbiträden och personuppgiftsbiträdesavtal. Vi kommenterar också kort de krav och åtaganden som den personuppgiftsansvarige enligt GDPR måste säkerställa att personuppgiftsbiträdet uppfyller. I avsnitt 4 avhandlar vi den upphandlingsrättsliga problematik som kan aktualiseras i samband med anpassning av personuppgiftsbiträdesavtal framtagna under PuL efter GDPR:s utökade krav. Avsnitt 5 handlar om frågor om laglig grund vid direktmarknadsföring. Vi resonerar i detta avsnitt även kring profilering och automatiserat beslutsfattande och dess eventuella betydelse för behandling som sker för direktmarknadsföringsändamål. I avsnitt 6 redogör vi för GDPR:s krav på risk- och konsekvensbedömning och hur dessa krav kan angripas med hjälp av en tvåstegsmodell. Slutligen, i avsnitt 7, presenterar vi några sammanfattande reflektioner om GDPR och de områden som rapporten avhandlar.

Förkortningar

FÖRKORTNING	BESKRIVNING
Dataskyddsdirektivet	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
CNIL	Commission nationale de l'informatique et des libertés (franska tillsynsmyndigheten för dataskydd)
DPIA	Data Protection Impact Assessment
GDPR	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)
ICO	Information Commissioner's Office (Storbritanniens tillsynsmyndighet för dataskydd)
LOU	Lag (2016:1145) om offentlig upphandling
LOU-direktivet	Europaparlamentets och Rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG
LUF	Lag (2016:1146) om upphandling inom försörjningssektorerna
LUF-direktivet	Europaparlamentets och Rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG
PuL	Personuppgiftslag (1998:204)
SOU	Statens offentliga utredningar
ÄLOU	Lag (2007:1091) om offentlig upphandling
ÄLUF	Lag (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster

2. Att fördela personuppgiftsansvar under GDPR – en enkel sak?

Inledning

Vi kommer i detta avsnitt att närmare analysera frågan om ansvars- och rollfördelning under GDPR när flera aktörer är involverade i samma eller närliggande behandlingar av personuppgifter.

Ett grundläggande krav i GDPR (liksom för den delen i PuL) är att det måste klargöras vem eller vilka som är personuppgiftsansvariga för en viss behandling av personuppgifter. En sådan fastställd ansvars- och rollfördelning är nödvändig för att kunna uppnå EU-lagstiftarens avsikt att genom GDPR stärka skyddet av de registrerades rättigheter och friheter och att effektivisera tillsynsmyndigheternas övervakning och åtgärder.[2] Detta ställer i sin tur krav på en noggrann analys av ansvars- och rollfördelningen mellan de aktörer som kan vara involverade i personuppgiftsbehandlingen.

Behovet av att tydligt fastställa ansvaret för viss behandling är principiellt lika viktigt under GDPR i fråga om behandlingar där en personuppgiftsansvarig anlitar en annan aktör för att utföra behandling för den ansvariges räkning (biträdesrelation)[3] som för behandlingar där flera personuppgiftsansvariga gemensamt fastställer ändamål och medel för viss eller vissa behandlingar (gemensamt personuppgiftsansvar)[4]. Som vi kommer att diskutera nedan menar vi att även överföring eller tillgängliggörande av personuppgifter från en personuppgiftsansvarig till en annan personuppgiftsansvarig (utlämnande) kräver särskilda överväganden.

Att fördela personuppgiftsansvar kan te sig enkelt i teorin men i praktiken är denna frågeställning ofta mer komplex än vad man kan tro. Vid tillhandahållandet av tjänster är det t.ex. vanligt att flera olika aktörer samverkar och har gemensam tillgång till information, inklusive personuppgifter, som många gånger dessutom flödar tämligen fritt mellan dessa aktörer. Att i en sådan situation avgöra när och av vem som beslut om ”ändamål och medel” för personuppgiftsbehandling i själva verket ska fattas är långt ifrån självklart.

En annan vanlig situation där det kan vara svårt att korrekt bedöma och fördela personuppgiftsansvar är den inom koncerner, medlems-

2 Skäl 79 GDPR.

3 Jfr Artikel 28 GDPR.

4 Jfr Artikel 26 GDPR.

organisationer eller kooperativ. Det är t.ex. relativt vanligt att flera koncernbolag har tillgång till en gemensam databas eller ett gemensamt register.

Personuppgiftsansvar bygger på bestämmanderätt

För varje behandling av personuppgifter i GDPR:s mening måste det alltid finnas en eller flera som är personuppgiftsansvariga. Legaldefinitionen av ”personuppgiftsansvarig” är i allt väsentligt densamma under PuL och GDPR. I GDPR uttrycks definitionen enligt följande:

”*personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter […]”.[5]

Enligt legaldefinitionen har personuppgiftsansvarig alltid bestämmanderätt över ändamålen och medlen för behandlingen i fråga.[6] Vem eller vilka som bestämmer över en viss behandling avgörs av de faktiska omständigheterna i varje enskilt fall. Detta innebär bl.a. att en aktör som de facto – rätt eller fel – bestämmer över ändamål eller medel för en behandling inte kan vara personuppgiftsbiträde för den behandlingen.

Med rätten att bestämma över ”ändamål” och ”medel” avses rätten att bestämma över ”varför” respektive ”hur” en behandling ska utföras. Viktiga frågor är ”varför behandlingen utförs” och ”vem som är initiativtagare till behandlingen”.[7]

När det gäller rätten att bestämma över **ändamål** är den aktör som har sådan bestämmanderätt alltid personuppgiftsansvarig för behandlingen, antingen ensamt eller tillsammans med annan. Beslut om **medel** för behandlingen kan dock delegeras i fråga om tekniska och organisatoriska frågor.[8] Det betyder att en aktör med viss bestämmanderätt över medlen inte nödvändigtvis är personuppgiftsansvarig, om bestämmanderätten har delegerats av en personuppgiftsansvarig eller om bestämmanderätten grundar sig på krav på personuppgiftsbiträden i GDPR eller annan lagstiftning. En personuppgiftsansvarig kan dock inte delegera beslut om medel i sådan utsträckning att den personuppgiftsansvarige inte längre kan utöva bestämmanderätt över medlen. I sådana fall upphör det tilltänkta personuppgiftsbiträdet att vara biträde och blir istället ansvarig för den faktiska

5 Artikel 4 GDPR.

6 Artikel 4 GDPR och 3 § PuL.

7 Artikel 29-gruppen, *Yttrande 1/2010 om begreppen registeransvarig och registerförare* s. 13. Se även Datainspektionens beslut 2010-07-02, dnr 686-2010, samt Förvaltningsrätten i Stockholms dom 2013-10-14 i mål nr 9987-12. Se vidare Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen: en kommentar,* 4 [rev.] uppl., Norstedts juridik, Stockholm, 2011, s. 93.

8 Artikel 29-gruppen, *Yttrande 1/2010,* s. 14. Se även artikel 28.3 c och 32 GDPR samt 30-31 §§ PuL.

behandlingen; sannolikt tillsammans med den aktör som ursprungligen ansågs vara ensamt ansvarig för behandlingen.[9]

Graden av självbestämmande och manöverutrymme i beslutsfattandet utgör således viktiga tolkningsdata för att avgöra bestämmanderätten.[10] Bestämmanderätten kan – med de begrepp som Artikel 29-gruppen[11] använder sig av – följa av (i) uttrycklig behörighet, (ii) underförstådd behörighet eller (iii) faktiskt inflytande.[12]

Med **uttrycklig behörighet** avses att bestämmanderätten framgår av lagtext eller är en direkt följd av lagtext. Myndighetsspecifika registerförfattningar är exempel på sådan lagstiftning där personuppgiftsansvaret ofta framgår av lagtext. I andra fall, då det saknas bestämmelse om uttrycklig behörighet, kan en aktör ha en **underförstådd behörighet** att bestämma över ändamål och medel. Med underförstådd behörighet avses att behörigheten härrör från rättsliga bestämmelser eller etablerad rättspraxis på området. Vissa roller brukar vanligtvis medföra en slags presumtion för personuppgiftsansvar; t.ex. arbetsgivare i förhållande till anställda, föreningar i förhållande till medlemmar och företag i förhållande till kunder. I dessa fall utgör rätten att bestämma en naturlig del av aktörens roll, och det är således rimligt att samma ansvarsfördelning även ska gälla i förhållande till personuppgiftsbehandlingen, förutsatt att en sådan ordning återspeglar de faktiska omständigheterna.[13]

Vidare kan bestämmanderätten grunda sig på **faktiskt inflytande** över behandlingen. Av de tre kategorierna för att avgöra bestämmanderätt är denna sannolikt den svåraste att tillämpa. Utifrån avtal och annan dokumentation kring parternas förhållanden är det ofta möjligt att utläsa om en aktör har bestämmanderätt, eller en dominerande roll, med avseende på behandlingen. Förutsatt att en sådan ordning återspeglar de faktiska omständigheterna vid behandlingen finns det inga hinder mot att godta den. I tveksamma fall, där det är oklart vilken part som bestämmer, kan även den grad av verkligt personuppgiftsansvar som en part utövar, trots att detta inte framgår av avtalet, de registrerades uppfattning i frågan samt de registrerades rimliga förväntningar påverka bedömningen.[14]

Datainspektionens syn på personuppgiftsansvar

Vi kan konstatera att Datainspektionen i sin tillsynspraxis under PuL sällan redovisar på vilka grunder som en aktör, t.ex. ett bolag som är

9 Artikel 28.10 GDPR. Se även särskilt om s.k. molntjänster nedan.

10 Artikel 29-gruppen, *Yttrande 1/2010*, s. 13.

11 Artikel 29-gruppen är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.

12 Artikel 29-gruppen, *Yttrande 1/2010*, s. 10-12.

13 Artikel 29-gruppen, *Yttrande 1/2010*, s. 10.

14 Artikel 29-gruppen, *Yttrande 1/2010*, s. 11-12.

föremål för tillsyn, har bestämmanderätt över viss behandling. Datainspektionen uttalar sig inte heller huruvida aktören bör anses som ensamt personuppgiftsansvarig, eller om flera aktörer kan vara gemensamt personuppgiftsansvariga för samma behandling.

En viktig utgångspunkt för Datainspektionen synes hittills ha varit att någon aktör är personuppgiftsansvarig för en viss behandling och att fördelningen av personuppgiftsansvaret är rimlig och ändamålsenlig.[15] Detta är naturligtvis en bra utgångspunkt men som ovan framgått krävs många gånger en mer utförlig och komplex bedömning på behandlingsnivå. Det vore därför värdefullt om Datainspektionen gav ytterligare vägledning kring fördelning av personuppgiftsansvar. Detta tror vi skulle underlätta för många organisationer som nu förbereder sig för GDPR.

Särskilt om s.k. molntjänster

Frågan om i vilken utsträckning som en personuppgiftsansvarig kan delegera bestämmanderätt över medel är i vår mening särskilt intressant att belysa i förhållande till användning av standardiserade molntjänster (*cloud services*). Detta eftersom leverantörer av sådana tjänster ofta har stort – för att inte säga ensamt – inflytande över medlen, dvs. hur behandlingen ska utföras.

Datainspektionens syn på molntjänster synes vara att beställaren av molntjänsten ”alltid” är personuppgiftsansvarig och att molntjänstleverantören är personuppgiftsbiträde.[16] Detta utgör också en vedertagen uppfattning bland i vart fall svenska molntjänstleverantörer. Vissa utländska leverantörer (t.ex. Facebook) har helt motsatt uppfattning och anser sig vara personuppgiftsansvariga för alla personuppgifter som de behandlar. Enligt vår uppfattning finns ofta skäl att ifrågasätta, eller åtminstone komplettera, båda dessa slutsatser.

Om en beställare varken har uttrycklig behörighet, underförstådd behörighet eller faktiskt inflytande över den behandling som molntjänstleverantören utför kan beställaren – å ena sidan – inte rimligen anses vara ensamt personuppgiftsansvarig. Å andra sidan måste en beställare i normalfallet anses ha bestämmanderätt baserat på exempelvis underförstådd behörighet (t.ex. i rollen som arbetsgivare), en bestämmanderätt som inte rimligen kan anses upphöra när uppgifterna behandlas av molntjänstleverantören. Den franska dataskyddsmyndigheten (CNIL) har uttryckt en liknande uppfattning i frågan och anser att beställare av molntjänster i vissa fall, och för vissa behandlingar, bör anses som gemensamt personuppgiftsansvariga tillsammans med leverantören. Enligt CNIL beror det på att molntjänstleverantörer ofta erbjuder högst standardiserade tjänster till

15 Jfr Datainspektionens *Samrådsyttrande om fördelning av personuppgiftsansvar – E-delegationsprojektet Effektiv informationsförsörjning*, 2014-03-18, där Datainspektionen tämligen utförligt redogör för bedömningsgrunderna vid fördelning av personuppgiftsansvar.

16 Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*, 2016.

standardiserade villkor, dvs. tjänster som inte är anpassade till enskilda beställare och till villkor som inte kan förhandlas.[17] Såvitt vi känner till saknas dock vägledande praxis som talar för en sådan uppdelning av ansvar. En sådan uppdelning har heller inte godtagits inom branschen, sannolikt eftersom molntjänstleverantörer åtminstone hittills helt avvisat tanken på att de skulle åta sig det ansvar som åvilar en personuppgiftsansvarig.

Enligt vår mening bör Datainspektionens allmänna inställning rörande personuppgiftsansvar vid användning av molntjänster nyanseras, särskilt i förhållande till högst standardiserade molntjänster. Flera olika alternativ finns avseende fördelning av personuppgiftsansvar och det finns ingen modell som passar för alla tjänster. Vi förmodar t.ex. att beställaren och molntjänstleverantören ofta kan anses som gemensamt personuppgiftsansvariga för vissa behandlingar, t.ex. för lagring av personuppgifter i molntjänsten. För andra behandlingar bör molntjänstleverantören sannolikt betraktas som personuppgiftsbiträde och för ytterligare en kategori behandlingar kanske som ensamt personuppgiftsansvarig. En bedömning och analys behöver därför göras på behandlingsnivå. En sådan analys kan medföra att parterna inte kan nöja sig med ett traditionellt personuppgiftbiträdesavtal utan att ett mer omfattande avtal bör ingås, som täcker ansvarsfördelningen för flera olika behandlingstyper.

Vi kommer i nästa avsnitt att beskriva en generell modell för fördelning av personuppgiftsansvar.

Generell modell för fördelning av personuppgiftsansvar – en bedömning i flera steg

Som nämnts ovan är legaldefinitionen av personuppgiftsansvar i allt väsentligt densamma under PuL och GDPR. Detta talar starkt för att bedömningen av fördelningen av personuppgiftsansvar under GDPR bör utföras enligt samma principer som under PuL, åtminstone till dess att EU-organ, EU-domstol eller relevant tillsynsmyndighet meddelar annat.

Det innebär enligt vår mening också att Artikel 29-gruppens yttrande 1/2010, som med tanke på Artikel 29-gruppens ställning och oberoende roll bör utgöra det bästa tolkningsstödet på området, är aktuellt och relevant även under GDPR.

Baserat på Artikel 29-gruppens yttrande 1/2010 har vi tagit fram en schematisk modell för att underlätta bedömningen av fördelningen av personuppgiftsansvar. Denna modell knyter an till det för personuppgiftsansvaret avgörande kriteriet bestämmanderätt som beskrivits ovan.

17 CNIL, *Recommendations for companies planning to use cloud computing services*, s. 5-6.

Modellen för fördelning av personuppgiftsansvar innehåller fyra steg och kan illustreras enligt följande:

I **steg ett** identifieras och kartläggs en viss ”faktisk behandling”, dvs. en åtgärd eller en serie av åtgärder för samma ändamål.[18] För att kunna tillämpa modellen krävs information om i vart fall: a) varför behandlingen utförs (ändamålet), b) vilka personuppgifter som behandlas och c) vilka aktörer som är inblandade.

I **steg två** utreds vilka av de aktörer som identifierats i steg ett ovan som har bestämmanderätt över ändamål och medel för den faktiska behandlingen. Bedömningen bör genomföras per aktör. Bestämmanderätten kan, med Artikel 29-gruppens terminologi, grundas på uttrycklig behörighet, underförstådd behörighet och/eller faktiskt inflytande.

I **steg tre** delas behandlingen in i en av följande tre behandlingstyper:

a) egen behandling,
b) samordnad behandling, eller
c) biträdesrelation.

I den enklaste situationen identifieras endast en aktör med bestämmanderätt i steg två, vilket innebär att behandlingen i steg tre bör kategoriseras som en egen behandling. Om behandlingen involverar flera aktörer där endast en har bestämmanderätt kategoriseras behandlingen som en biträdesrelation. Om behandlingen involverar flera aktörer som har bestämmanderätt leder detta till vad vi kallar en ”samordnad behandling”. Vi kommer att beskriva sådana samordnade behandlingar närmare längre fram i detta avsnitt.

18 Artikel 4 GDPR.

I **steg fyra** fastställs och dokumenteras personuppgiftsansvaret för den faktiska behandlingen, dvs. vilken eller vilka aktörer som är personuppgiftsansvariga. Även bedömningen som personuppgiftsansvaret grundar sig på, dvs. steg ett till tre ovan, bör dokumenteras. Beroende på om den undersökta behandlingen utgör en egen behandling, en samordnad behandling eller en biträdesrelation, kan det finnas behov av avtalsreglering mellan de involverade aktörerna. I en biträdesrelation krävs naturligtvis ett personuppgiftsbiträdesavtal.[19] För behov av avtalsreglering avseende samordnade behandlingar, se nedan.

Bedömningarna och resultaten enligt ovan bör slutligen kontrolleras så att fördelningen av personuppgiftsansvar är rimlig utifrån syftena med GDPR. Vid en sådan rimlighetsbedömning bör särskilt tas hänsyn till om fördelningen av ansvar gör det möjligt för den personuppgiftsansvarige och personuppgiftsbiträdet att uppfylla sina respektive skyldigheter samt för de registrerade att utöva sina rättigheter enligt GDPR.[20] Om tillämpningen av modellen leder till onödig komplexitet eller andra oönskade konsekvenser bör det finnas viss möjlighet att ”omfördela” ansvar mellan de inblandade aktörerna, t.ex. genom olika avtalskonstruktioner.[21] En sådan ”omfördelning” bör dock göras endast undantagsvis och får inte medföra ett kringgående av GDPR. Den valda fördelningen av personuppgiftsansvar måste återspegla de faktiska omständigheterna i det aktuella fallet.[22]

Ansvarsfördelning och behov av avtalsreglering vid samordnad behandling

Om två eller flera aktörer har bestämmanderätt över en viss behandling leder detta, med vår terminologi, till en samordnad behandling. Principiellt kan personuppgiftsansvar i samband med samordnade behandlingar beskrivas på i huvudsak följande två sätt:

a) gemensamt personuppgiftsansvar, eller
b) ”utlämnande” personuppgiftsansvarig till personuppgiftsansvarig.

Vad gäller gemensamt personuppgiftsansvar råder inga tvivel om att GDPR kräver ett ”*inbördes arrangemang*”. Av artikel 26 framgår nämligen att gemensamt personuppgiftsansvariga ”*under öppna former* [*ska*] *fastställa sitt respektive ansvar för att fullgöra skyldigheterna*” enligt GDPR genom ett ”*inbördes arrangemang*”. Arrangemanget ska särskilt avse former och ansvar för utövande av den registrerades rättigheter och skyldigheten att lämna information till registrerade. Vidare gäller att arrangemanget ”på lämpligt sätt ska återspegla

19 Artikel 28.3 GDPR. Det kan dock noteras att enligt sagda artikel ska biträdesrelationen regleras ”[…] *genom ett avtal eller annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet* […]”.

20 Jfr artikel 26 GDPR angående krav på arrangemang vid gemensamt personuppgiftsansvar.

21 Jfr Artikel 29-gruppen, *Yttrande 1/2010,* s. 23 samt liknande resonemang på s. 7 och 19. Se därutöver Datainspektionens *Samrådsyttrande* 2014-03-18.

22 Jfr Artikel 29-gruppen, *Yttrande 1/2010,* s. 23.

gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade" samt att "*det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade*". Kravet på inbördes arrangemang är sanktionerat med administrativ sanktionsavgift.[23]

Om en samordnad behandling istället beskrivs som ett "utlämnande" från en personuppgiftsansvarig till en annan personuppgiftsansvarig står det klart att den aktör som samlar in och initialt lagrar personuppgifterna är ansvarig för dessa behandlingar. Vidare är den aktör som mottar uppgifterna ansvarig för alla behandlingar som denne utför efter överföringen. Vad gäller ansvaret för själva överföringen (vilket är en behandling i sig) är situationen mer komplicerad. I vissa fall kan det vara lämpligt att betrakta utlämnande och mottagande aktör som gemensamt personuppgiftsansvariga för själva överföringen, förutsatt såklart att de tillsammans bestämmer ändamålen och medlen för överföringen. I andra fall kan endast en av aktörerna utöva bestämmanderätt över ändamålen och medlen för själva överföringen. Så kan t.ex. vara fallet när en myndighet bestämmer att samt hur och varför ett bolag ska lämna ut vissa personuppgifter till myndigheten.

Som ovan framgått krävs ett inbördes arrangemang för det fall flera aktörer är gemensamt personuppgiftsansvariga för själva överföringen. Vi menar dock att personuppgiftsansvarig även bör överväga om någon form av "arrangemang" eller avtalsreglering är lämpligt i varje fall av utlämnande. Behovet av ett sådant arrangemang får såklart bedömas från fall till fall och utifrån aktuella omständigheter. Normalt sett bör den utlämnande aktören i vart fall försäkra sig om att personuppgifterna inte behandlas i strid med GDPR av den mottagande aktören. Den mottagande aktören bör i sin tur i vart fall försäkra sig om att de registrerade fått korrekt information om utlämnandet och att insamlandet i övrigt var lagligt. Detta kan i förlängningen innebära ett behov av koordinerad informationslämning, hantering av registrerades rättigheter, reglering avseende säkerhetsåtgärder osv. Skillnaden jämfört med ett inbördes arrangemang enligt artikel 26 förefaller därmed inte som särskilt stora.

Kravet i GDPR på ett arrangemang för gemensamt personuppgiftsansvariga bör sannolikt inte förstås som ett uttryckligt krav på avtal aktörerna sinsemellan. Enligt vår bedömning är det dock klart att ett sådant "arrangemang" bör dokumenteras och regleras inom ramen för ett avtal.

Enligt vår uppfattning bör åtminstone följande dokumenteras och regleras för varje samordnad behandling: (i) klargörande av de olika aktörerna och deras roller, (ii) varför data behandlas (ändamålet), (iii) vilken typ av data som ska/får omfattas, (iv) hur de registrerade kan utöva sina rättigheter, (v) hur de registrerade ska få tillräcklig

23 Artikel 83.4 a GDPR.

information om behandlingen, (vi) hur de grundläggande principerna för behandling av personuppgifter uppfylls, (vii) laglig grund för behandlingen och (viii) om någon av de ansvariga ska utgöra en gemensam kontaktpunkt för de registrerade m.m.[24] Andra viktiga frågor som kan vara lämpliga att adressera är gallring, säkerhet i behandlingen, sekretess och möjligheterna till kontroll av den andre partens avtalsefterlevnad.

Vi menar mot ovanstående bakgrund att det, beroende på omständigheterna, kan finnas behov av avtalsreglering vid de flesta former av samordnade behandlingar, oavsett om behandlingen kategoriseras som ett ”utlämnande” från en personuppgiftsansvarig till en annan personuppgiftsansvarig eller som en behandling med gemensamt personuppgiftsansvar. Vi tror dock att sådan avtalsreglering i dag snarare är undantag än regel, och att det finns ett stort behov av tillkommande analys och avtalsreglering för att korrekt reglera och formalisera samordnade behandlingar under GDPR.

Avslutande kommentarer

Ett mer nyanserat sätt att betrakta och fördela personuppgiftsansvar är, enligt vår mening, nödvändigt för att korrekt tillämpa och efterleva GDPR. Att – såsom under PuL – närmast slentrianmässigt utse en part (t.ex. en beställare) till personuppgiftsansvarig och en annan part (leverantören) till biträde är otillräckligt. En analys på behandlingsnivå är nödvändig, varvid flera olika alternativ måste övervägas. Allt oftare torde detta leda till att samordnade behandlingar aktualiseras, dvs. behandlingar av personuppgifter där flera aktörer har någon form av rättsligt relevant bestämmanderätt.

GDPR ställer krav på att aktörer som deltar i en samordnad behandling hanterar och reglerar ansvars- och rollfördelningen sinsemellan. Detta följer av GDPR:s sanktionerade krav på inbördes arrangemang mellan gemensamt ansvariga och personuppgiftsbiträdesavtal mellan ansvarig och biträde, men också av det faktum att ett effektivt ansvarsutkrävande enligt GDPR synes bygga på ett solidariskt ansvar gentemot den registrerade.[25]

Aktörer som använder eller annars deltar i komplexa tjänster/samarbeten bör således först reda ut (och dokumentera) vilka personuppgiftsbehandlingar som aktualiseras och därefter – i den mån samordnade behandlingar identifieras – sinsemellan reda ut hur personuppgiftsansvaret ska delas och utövas i praktiken. Till stöd för en sådan inbördes ansvarsfördelning, som speglar ansvarsfördelningen enligt GDPR, anser vi att berörda aktörer först och främst bör utgå ifrån vad Artikel 29-gruppen uttalat till vägledning i fråga om personuppgiftsansvar och ansvarets eventuella fördelning på flera personuppgifts-

24 Se ICO, *Data sharing code of practice*, särskilt s. 41-43.

25 Artikel 82.1-82.2 GDPR.

ansvariga, liksom gränsdragningen mot rollen som personuppgifts-biträde.

Vi menar att den modell och det synsätt som uttrycks i nämnda vägledning, och som vi utvecklat närmre i detta avsnitt, är central för att kunna uppfylla de krav som följer av GDPR.

3. Behöver befintliga personuppgiftsbiträdes-avtal ändras?

Inledning

Vi kommer i detta avsnitt att redogöra för de förändringsbehov som GDPR innebär för sådana personuppgiftsbiträdesavtal som upprättats under och varit anpassade till PuL:s regelverk. Frågeställningen är intressant av flera anledningar, inte minst av praktiska skäl eftersom det för många verksamheter skulle vara mycket arbetskrävande och betungande att behöva ingå nya biträdesavtal med alla befintliga personuppgiftsbiträden.

För offentliga kontrakt finns ytterligare en dimension på frågeställningen, eftersom eventuella ändringar i sådana kontrakt kan ge upphov till en upphandlingsrättslig problematik. Denna upphandlingsrättsliga aspekt diskuteras närmare i avsnitt 4 nedan.

Kort om personuppgiftsbiträdets förändrade roll under GDPR

GDPR innebär att personuppgiftsbiträdets roll – och delvis också ansvar – förändras, på så sätt att biträden får nya skyldigheter och ett, såsom Datainspektionen uttrycker det, utökat eget ansvar för behandlingar. Genom GDPR ställs också mer utförliga krav på utformningen av personuppgiftsbiträdesavtal i förhållande till PuL.[26]

En viktig skillnad mot PuL är att biträdet under GDPR får ett självständigt ansvar i förhållande till registrerade och tillsynsmyndigheter. GDPR innebär således att även biträden ytterst kan dömas till administrativ sanktionsavgift samt bli skadeståndsskyldiga gentemot de registrerade.[27] Detta ska jämföras med sanktionsbestämmelserna i PuL om förbud vid vite och skadestånd, som endast avser personuppgiftsansvariga.[28]

Det utökade ansvaret för biträden i GDPR kan vidare exemplifieras genom att GDPR medför ett eget ansvar för biträden att bedöma lämpligheten avseende nödvändiga tekniska och organisatoriska säkerhetsåtgärder, samt ansvar för att underrätta den personuppgiftsansvarige vid personuppgiftsincidenter, föra register över de

26 Datainspektionens informationsblad, *Vägledning för personuppgiftsbiträden*, 2016.

27 Artikel 82-83 GDPR.

28 45 och 48 §§ PuL.

behandlingar som biträdet utför samt i vissa fall utse ett dataskyddsombud.[29] Personuppgiftsbiträdet ska också informera den personuppgiftsansvarige om biträdet anser att den ansvariges instruktioner strider mot GDPR eller annan dataskyddsbestämmelse. Biträdet är därutöver skyldigt att bistå den ansvarige när denne ska fullgöra vissa skyldigheter enligt GDPR.[30]

Således innebär GDPR att ansvarsfördelningen mellan personuppgiftsansvarig och biträden förändras, så att biträdets ansvar utökas vad gäller uppfyllandet av förordningens krav, samt i relationen till de registrerade och tillsynsmyndigheterna. Detta är, enligt vår mening, betydelsefulla förändringar som på flera olika sätt kan komma att ändra dynamiken mellan parterna.

29 Artikel 32, 33.2, 30.2 och 37 GDPR.

30 Artikel 28.3 GDPR.

Hur skiljer sig GDPR:s krav på personuppgiftsbiträdesavtal från PuL?

Som ovan antytts skiljer sig de explicita lagkraven på personuppgiftsbiträdesavtal åt mellan PuL och GDPR. Dessa skillnader kan sammanfattas enligt följande:

<table>
<tr><th colspan="2">FORMELLA KRAV PÅ INNEHÅLL I PERSONUPPGIFTSBITRÄDESAVTAL</th></tr>
<tr><th>PuL</th><th>GDPR</th></tr>
<tr><td rowspan="2">• Krav på skriftligt avtal (30 § 1 st. PuL).
• Föreskrift om att biträdet får behandla personuppgifterna endast i enlighet med instruktioner från den personuppgiftsansvarige (30 § 2 st. PuL).
• Föreskrift om att biträdet ska vidta säkerhetsåtgärder (30 § 2 st. samt 31 § 1 st. PuL).</td><td>• Krav på skriftligt avtal (art. 28.3 och 28.9 GDPR).[31]
• Föreskrift om att biträdet endast får behandla personuppgifter på dokumenterade[32] instruktioner från den personuppgiftsansvarige (art. 28.3 a GDPR).
• Föreskrift om att biträdet ska vidta lämpliga säkerhetsåtgärder m.m.[33], vilket enligt GDPR inkluderar:
- Säkerhetsåtgärder enligt artikel 32 GDPR (art. 28.3 c GDPR),
- Att uppfylla sina skyldigheter samt bistå den personuppgiftsansvarige vid den senares uppfyllande av skyldigheter enligt artikel 32-36 GDPR (art. 28.3 f GDPR).</td></tr>
<tr><td>• Konfidentialitetsåtagande (art. 28.3 b GDPR).
• Beskrivning som specificerar vilka behandlingar som omfattas (art. 28.3 GDPR).
• Föreskrift om att ålägga s.k. underbiträden samma skyldigheter som gäller för biträdet (art. 28.3 d, 28.2 och 28.4 GDPR).
• Föreskrift om att bistå den personuppgiftsansvarige vid begäran från de registrerade (art. 28.3 e GDPR).
• Åtagande om att enligt instruktion återlämna eller radera personuppgifter och radera befintliga kopior (art. 28.3 g GDPR).
• Åtagande om att ge den personuppgiftsansvarige tillgång till information och bidra till granskning och inspektioner (art. 28.3 h GDPR).</td></tr>
</table>

31 Notera att det i artikel 28.3 GDPR anges att personuppgiftsbiträdesrelationen ska regleras ”[...] *genom ett avtal eller annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet* [...]”.

32 Genom GDPR införs således ett formkrav i fråga om att den personuppgiftsansvariges instruktioner till personuppgiftsbiträdet ska vara ”dokumenterade”.

33 Som ovan angetts får biträden under GDPR har ett eget ansvar för att bedöma och vidta lämpliga säkerhetsåtgärder. Biträdets eget ansvar innebär dock inte att personuppgiftsansvariges ansvar minskar i motsvarande mån i relation till registrerade eller tillsynsmyndigheter, men kan däremot få betydelse för parternas inbördes ansvar. Ansvar kan riktas gentemot såväl personuppgiftsbiträdet som den personuppgiftsansvarige, se artikel 83.4 a samt artikel 82 GDPR. Se även Datainspektionens informationsblad, *Förberedelser för Personuppgiftsansvariga*, 2017.

Rättsutveckling under PuL

Vid en första anblick kan det förefalla som om GDPR medför en lång rad helt nya krav på innehållet i ett personuppgiftsbiträdesavtal. Detta är dock en sanning med modifikation. I själva verket utgör GDPR:s mer omfattande krav i stor utsträckning en kodifiering av den rättsutveckling som ägt rum inom EU de senaste åren.

I Sverige har rättsutvecklingen avseende innehåll i biträdesavtal framförallt drivits av Datainspektionens tillsyn över molntjänster. En stor och bred tillsyn utfördes på detta område mellan 2010-2012, vilket utmynnande i flera tillsynsbeslut och allmänna regler för vad ett biträdesavtal ska innehålla för att möta kraven i PuL och Dataskyddsdirektivet.[34]

Exempel på redan gällande krav på biträdesavtal enligt praxis i Datainspektionens ovannämnda tillsynsärenden är:[35]

- Att personuppgiftsansvarig ska kunna utföra revision av biträdets, och eventuella underbiträdens, behandling av personuppgifter (jfr artikel 28.3 h GDPR).

- Att biträden på personuppgiftsansvariges anmodan och vid behandlingens upphörande antingen ska radera eller återlämna de behandlade personuppgifterna (jfr artikel 28.3 g GDPR).

- Att ett biträde kan ges ”mandat” att ingå biträdesavtal för den ansvariges räkning om biträdet anlitar ett underbiträde, under förutsättning att biträdets avtal med underbiträdet innehåller krav som motsvarar personuppgiftsbiträdesavtalet mellan den personuppgiftsansvarige och biträdet (jfr artikel 28.4 GDPR).

Det ovan sagda torde innebära att i de fall Datainspektionens senare praxis rörande biträdesavtal har beaktats, är förändringsbehovet tämligen litet för sådana biträdesavtal. Enligt vår erfarenhet uppfyller dock en större andel av personuppgiftsbiträdesavtalen framtagna för PuL endast PuL:s explicita lagkrav, se vidare i detta avsnitt under ”Avslutande kommentarer” nedan.

34 Datainspektionens beslut (*Salems kommun*) 2011-09-28, dnr 263-2011, uppföljt genom beslut 2013-04-31, dnr 1351-2012, samt Förvaltningsrätten i Stockholms dom 2014-07-01, mål nr 15410-13, och Datainspektionens beslut (*Brevo*) 2011-09-28, dnr 574-2011, (*Enköpings kommun*) 2011-09-28, dnr 256-2011 samt Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*, 2016.

35 Ibid.

Närmare om vissa av personuppgifts-biträdets åtaganden under GDPR

BESKRIVNING AV BEHANDLINGEN

Som ovan framgått ska personuppgiftsbiträdesavtal enligt GDPR innehålla en beskrivning av de behandlingar som kommer att ske under avtalet. En sådan specifikation ska närmare bestämt beskriva:

- föremålet för de behandlingar som biträdet utför,
- behandlingarnas varaktighet, art och ändamål,
- typen av personuppgifter (t.ex. namn och kontaktuppgifter),
- kategorier av registrerade vars uppgifter omfattas (t.ex. anställda eller kunder), samt
- den personuppgiftsansvariges skyldigheter och rättigheter.[36]

Syftet med specifikationen är att tydliggöra vilka behandlingar och vilka personuppgifter som omfattas av biträdesavtalet i fråga. Biträdet får naturligtvis endast behandla personuppgifterna å personuppgiftsansvariges vägnar på så vis och för de ändamål som anges i en sådan specifikation.

KONFIDENTIALITETSÅTAGANDE

Personuppgiftsbiträdesavtalet ska föreskriva krav på att biträdet säkerställer att personer med behörighet att behandla personuppgifterna åtar sig att iaktta konfidentialitet eller att de annars omfattas av en lämplig lagstadgad tystnadsplikt.[37]

ANLITANDE AV ANNAT PERSONUPPGIFTSBITRÄDE

Personuppgiftsbiträdesavtalet ska föreskriva att biträdet inte får anlita ett annat personuppgiftsbiträde (s.k. underbiträde) utan att på förhand ha inhämtat ett särskilt eller allmänt skriftligt tillstånd av den personuppgiftsansvarige. Om den personuppgiftsansvarige har gett biträdet ett allmänt tillstånd att anlita underbiträden måste biträdet fortfarande informera den personuppgiftsansvarige om eventuella planer på att anlita nya eller ersätta befintliga underbiträden, så att den personuppgiftsansvarige kan framställa eventuella invändningar mot detta i förekommande fall.[38]

Personuppgiftsbiträdesavtalet ska särskilt föreskriva att underbiträden genom avtal ska åläggas samma skyldigheter i fråga om dataskydd som de som fastställts i biträdesavtalet mellan den personupp-

36 Artikel 28.3 GDPR. Se även skäl 81 GDPR.

37 Artikel 28.3 b GDPR.

38 Artikel 28.2 och 28.3 d GDPR.

giftsansvarige och biträdet, särskilt vad gäller tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder. Med andra ord ska biträdesavtalet innehålla en skyldighet för biträdet att ingå ett eget personuppgiftsbiträdesavtal med underbiträdet, förutsatt att tillstånd enligt ovan föreligger. I de fall som underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska biträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för underbiträdets skyldigheter.[39]

Det kan diskuteras hur avtalet mellan biträdet och underbiträdet egentligen bör kategoriseras från ett rättsligt perspektiv. Den traditionella synen under PUL var att ett s.k. underbiträdesavtal i själva verket är ett direktavtal mellan den ansvarige och underbiträdet, låt vara att avtalet ingås av biträdet med stöd av fullmakt från den personuppgiftsansvarige. Ska artikel 28.2 GDPR förstås som en förändring härav, såtillvida att ett obligationsrättsligt bindande avtal uppkommer mellan biträdet och underbiträdet? Kanske finns ledning i artikel 28.4, som föreskriver att ”[o]*m det andra personuppgiftsbiträdet* [dvs. underbiträdet, vår anm.] *inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter*”. Detta kan (möjligen) tolkas, läst motsatsvis, så att under förutsättning att underbiträdet fullgör sina skyldigheter så ansvarar underbiträdet endast mot personuppgiftsbiträdet och inte mot den ansvarige. Om detta är en korrekt tolkning får man anta att GDPR faktiskt medför en förändring av rättsläget i detta avseende; en personuppgiftsansvarig har som utgångspunkt att framställa krav och utkräva ansvar mot sitt personuppgiftsbiträde och inte direkt gentemot underbiträdet. Med detta synsätt får alltså en form av obligationsrättsligt bindande avtal anses uppkomma mellan personuppgiftsbiträdena. Vi är inte övertygade om att detta är en lämplig – eller ens avsedd – lösning och betraktar detta som en frågeställning som bör klargöras av Datainspektionen eller Artikel 29-gruppen.

ASSISTANS TILL PERSONUPPGIFTSANSVARIG

Personuppgiftsbiträdesavtalet ska föreskriva att biträdet ska hjälpa den personuppgiftsansvarige att fullgöra sina skyldigheter i samband med att de registrerade utövar sina rättigheter enligt artikel 16–22 GDPR. De rättigheter som avses är bl.a. rätt till registerutdrag, rätt till en kopia av personuppgifter som är under behandling, rätt till rättelse, radering (”rätten att bli bortglömd”), begränsning av behandling och dataportabilitet (rätten att flytta personuppgifter till en annan personuppgiftsansvarig).

Biträdesavtalet ska vidare föreskriva att biträdet ska bistå den personuppgiftsansvarige att fullgöra skyldigheterna i GDPR vad avser säkerhet i samband med behandlingen, anmälan av och information om

39 Artikel 28.4 GDPR. Se även skäl 81 GDPR.

personuppgiftsincidenter, konsekvensbedömning avseende dataskydd samt förhandssamråd.[40]

RADERA ELLER FÖRSTÖRA PERSONUPPGIFTER

Personuppgiftsbiträdesavtal ska särskilt föreskriva att biträdet, efter det att behandlingen har avslutats, och enligt den personuppgiftsansvariges val, antingen ska återlämna alla personuppgifter till den personuppgiftsansvarige eller radera dessa. Även eventuella kopior ska raderas, såvida inte lagring krävs enligt unionsrätten eller svensk rätt.[41] Det är således viktigt att förse biträdesavtal med tydliga instruktioner om radering och destruering av personuppgifter.

INFORMATIONSSKYLDIGHET

Personuppgiftsbiträdesavtalet ska föreskriva att biträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som anges i artikel 28 GDPR har fullgjorts, samt att biträdet ska möjliggöra och bidra till revision (audit) (se vidare nedan).[42]

Biträdesavtalet ska även föreskriva att biträdet omedelbart måste informera den personuppgiftsansvarige för det fall biträdet anser att en instruktion som denne fått av en personuppgiftsansvarig strider mot GDPR eller mot andra dataskyddsbestämmelser.[43] Vi anser att bestämmelsen är särskilt intressant i de situationer där biträdet har ett självständigt ansvar för den behandling som utförs inom ramen för biträdesrelationen. Detta eftersom biträdet i sådana situationer har ett eget ansvar att ta ställning till innebörden av GDPR eller annan lagstiftning som kan vara tillämplig i fråga om dataskydd.

REVISION

Personuppgiftsbiträdesavtalet ska föreskriva att biträdet ska möjliggöra och bidra till granskningar och inspektioner som genomförs av antingen den personuppgiftsansvarige eller av tredje man som den personuppgiftsansvarige utsett.[44]

SÄRSKILT OM GARANTIER ENLIGT ARTIKEL 28.1 GDPR

I tillägg till vad som angetts ovan får personuppgiftsansvarig endast anlita personuppgiftsbiträden som ger ”tillräckliga garantier” om att

40 Artikel 28.3 f som hänvisar till artikel 32-36 GDPR.

41 Artikel 28.3 g GDPR.

42 Artikel 28.3 h GDPR.

43 Artikel 28.3 h, andra stycket GDPR.

44 Artikel 28.3 h GDPR.

genomföra lämpliga tekniska och organisatoriska åtgärder på sådant sätt att behandlingen uppfyller kraven i GDPR och säkerställer att den registrerades rättigheter skyddas.[45] Detta gäller i synnerhet biträdets sakkunskap, tillförlitlighet och resurser.[46] Det är den personuppgiftsansvarige som måste kunna visa att biträdet gett sådana tillräckliga garantier. Om biträdet är anslutet till en godkänd uppförandekod eller certifieringsmekanism, när sådana väl finns på plats, kan dessa användas av den personuppgiftsansvarige för att visa att denne har uppfyllt sina skyldigheter.[47] I övriga fall kan det vara svårt för den personuppgiftsansvarige att visa att biträdet har gett tillräckliga garantier utan att först ha genomfört en s.k. *due diligence* av biträdets behandling av personuppgifter.

Avslutande kommentarer

Enligt vår bedömning utgör de ”nya” kraven i GDPR till stor del en kodifiering av den praxis som utvecklats under PuL. Detta innebär att många befintliga biträdesavtal kan anses uppfylla GDPR:s krav – om de har upprättats av parter som har följt rättsutvecklingen. Vår erfarenhet är dock att biträdesavtal under PuL många gånger har ingåtts närmast slentrianmässigt och utan större diskussion eller förhandling mellan parterna. Dessutom är det mycket sällan ett biträdesavtal under PuL tydligt har specificerat vilka uppgifter och vilken behandling som omfattas av avtalet.

Ändringsbehovet i befintliga biträdesavtal beror således på kvaliteten och noggrannheten i det befintliga avtalet. ”Bra” biträdesavtal kan många gånger leva vidare även under GDPR med mindre justeringar, medan ”sämre” avtal kräver omförhandling. Det enda sättet för en verksamhet att göra en sådan bedömning är naturligtvis att gå igenom samtliga befintliga biträdesavtal och analysera avtalsinnehållet utifrån de krav som GDPR numera ställer.

Det ska också sägas att biträdets nya roll under GDPR, med utökat ansvar och skärpta sanktioner, kan medföra att befintliga personuppgiftsbiträdesavtal under alla omständigheter kan behöva omförhandlas. GDPR saknar övergångsregler, vilket innebär att eventuella nya biträdesavtal – om sådant bedöms nödvändigt enligt ovan – behöver vara ingångna före den 25 maj 2018.

Som nämnts ovan kan anpassningen av befintliga personuppgiftsbiträdesavtal till GDPR utlösa en potentiell konflikt med reglerna om offentlig upphandling. Vi utreder närmare denna utmaning för upphandlande myndigheter och enheter i avsnitt 4 nedan.

---

45 Artikel 28.1 GDPR.

46 Skäl 81 GDPR.

47 Ibid.

4. GDPR vs LOU; särskilt om ”väsentlig ändring” i offentliga kontrakt

Inledning

Som redovisats i avsnitt 3 ovan kommer befintliga biträdesavtal i vissa fall att behöva justeras för att uppfylla kraven i det nya regelverket. Det förhållandet att personuppgiftsbiträdet får direkta åtaganden under GDPR i kombination med ett skärpt sanktionssystem kommer i sin tur att medföra en större riskexponering för leverantören, med den potentiella följden att leverantören (i den utsträckning avtalsvillkoren medger) kan vilja förhandla till sig högre priser och/eller utökade ansvarsbegränsningar för att kompensera för denna förhöjda risknivå och eventuella merkostnader. Ett förändringsbehov, i den mån ett sådant finns, föranleder en särskild problematik i upphandlingsrättsligt hänseende, eftersom upphandlande myndigheter/enheter har begränsade möjligheter att företa ändringar i ett befintligt kontrakt enligt LOU och LUF.

Vi kommer mot denna bakgrund nedan att belysa vilka utmaningar, men också möjligheter, den upphandlande myndigheten/enheten har när det föreligger ett *materiellt* förändringsbehov. Med *materiellt* förändringsbehov åsyftas ändringar som medför en kostnadsökning eller en förändring av den ekonomiska jämvikten i avtalsförhållandet, vilket delvis är en annan situation än den som behandlas i avsnitt 3 ovan i de delar som avser rent formella ändringar.

De nya upphandlingslagarna

Genom EU-domstolens praxis är det sedan länge klarlagt att ett upphandlat kontrakt som ändras alltför mycket i förhållande till de ursprungliga villkoren (s.k. ”väsentliga förändringar”) ska betraktas som ett nytt tilldelat kontrakt som måste föregås av annonsering i enlighet med bestämmelserna i LOU och LUF. EU-domstolen konstaterade redan år 2000 att betydande skillnader som ”[...] *visar på en önskan från parternas sida att omförhandla de väsentliga villkoren i avtalet* [...]” kan medföra att upphandlingsreglerna blir tillämpliga.[48] Om den upphandlande myndigheten/enheten därvid underlåter att annonsera, riskerar ändringen att betraktas som en otillåten direktupphandling i strid med upphandlingslagarna. Den närmare tolkningen av begreppet väsentliga förändringar har varit föremål för EU-domstolens prövning i flera omdiskuterade avgöranden, däribland mål C-454/06, *Pressetext* och mål C-549/14, *Finn Frogne*.

48 Se EU-domstolens dom i mål C-337/98, *Kommissionen mot Frankrike*, EU.

Artiklarna 72 respektive 89 i LOU- och LUF-direktiven utgör i stora drag en kodifiering av denna praxis.[49] Till skillnad mot 2007 års upphandlingslagar reglerar LOU och LUF således uttryckligen vilka ändringar som är tillåtna respektive otillåtna för den upphandlande myndigheten/enheten att göra i befintliga kontrakt och ramavtal utan föregående annonsering.[50] De nya bestämmelserna om ändring av kontrakt och ramavtal har tillerkänts retroaktiv verkan, såtillvida att de är tillämpliga även på ändringar av befintliga kontrakt och ramavtal vilka ingåtts före lagarnas ikraftträdande den 1 januari 2017.[51] Huvudregeln är, som tidigare, att bestämmelserna i ett kontrakt eller ett ramavtal inte får ändras utan att det genomförs en ny annonserad upphandling. Av 17 kap. 8–16 §§ LOU respektive 16 kap. 8–16 §§ LUF följer dock en rad uttryckliga undantagsbestämmelser, som innebär att ett befintligt kontrakt eller ramavtal får ändras utan en ny upphandling, om ändringen görs med stöd av någon av bestämmelserna i 9–14 §§. Härvid ska dock noteras att den upphandlande myndigheten/enheten ändå har en skyldighet att, rent upplysningsvis, annonsera ändringar som föranletts av oförutsebara omständigheter respektive kompletterande beställningar, se vidare nedan.

Ändringar av mindre värde

Det första undantaget i 16 kap. 9 § LUF respektive 17 kap. 9 § LOU, beträffande ändringar av mindre värde, innebär att ett kontrakt eller ett ramavtal får ändras utan en ny upphandling, under förutsättning att kontraktets eller ramavtalets övergripande karaktär inte ändras och *ökningen eller minskningen* av kontraktets eller ramavtalets värde är lägre än (1) det tröskelvärde som genom beslut eller meddelande fastställts av EU-kommissionen, och (2) 10 respektive 15 procent av kontraktets eller ramavtalets värde.[52]

Vid beräkningen av värdet av ändringen ska samma principer tillämpas som vid tröskelvärdeberäkningen enligt 5 kap. LOU respektive LUF.[53] Vidare gäller att det samlade nettovärdet av ändringarna ska jämföras med de värden som anges ovan, om flera ändringar görs efter varandra.

Det ovanstående innebär att den upphandlande myndigheten/enheten har ett förhållandevis stort utrymme att genomföra olika typer av

49 Jfr skälen 107–111 i LOU-direktivet och skälen 113–117 i LUF-direktivet.

50 Regleringen är således en nyhet i förhållande ÄLOU och ÄLUF där lagstiftaren helt utelämnat frågan om ändring av kontrakt. Däremot har man av möjligheterna till förhandlat förfarande utan föregående annonsering kunnat sluta sig till att vissa ändringar av ett kontrakt kan göras utan att en ny konkurrensutsättning behöver ske (jfr 4 kap. 7 och 8 §§ ÄLOU och 4 kap. 2 § ÄLUF). Frågan om väsentliga ändringar regleras även implicit genom de begränsningar som uppställs av de grundläggande principerna i 1 kap. 9 § ÄLOU respektive 1 kap. 24 § ÄLUF.

51 Se prop. 2015/16:195, s. 851.

52 Varvid det förra gäller för upphandling av vara eller tjänst och det senare för upphandling av byggentreprenad.

53 Se närmare JP Infonet och lagkommentaren till 5 kap. LOU som författats av Advokatfirman Kahn Pedersen.

ändringar, under förutsättning att myndigheten/enheten håller sig under de aktuella tröskelvärdena. Exempelvis är det möjligt att justera priset i såväl höjande som sänkande riktning på de varor eller tjänster som ursprungligen upphandlats.[54]

För biträdesavtalens vidkommande medför detta att rena formaliajusteringar i biträdesavtalet (exempelvis förtydliganden avseende vilka behandlingar och personuppgifter som omfattas eller utökade sekretessförbindelser), liksom mindre prisjusteringar för att kompensera ett motsvarande utökat åtagande från leverantören, kan anses vara tillåtna i den mån värdet av dessa inte överstiger nämnda belopp. I många fall torde emellertid de åtgärder som krävs av leverantören för att efterleva GDPR (och då särskilt att på eget ansvar säkerställa att de åtgärder som vidtagits garanterar en tillräcklig säkerhetsnivå) föranleda högre merkostnader och därmed större prisökning, än vad som medges inom ramen för 16 kap. 9 § LUF respektive 17 kap. 9 § LOU. Eftersom ändringarnas värde enligt den aktuella undantagsbestämmelsen beräknas med utgångspunkt i det belopp som, enligt den upphandlande myndighetens uppskattning, ska betalas enligt kontraktet, saknas vid denna bedömning utrymme att ta hänsyn till de merkostnader leverantören drabbas av (till skillnad från den ekonomiska jämvikten enligt 16 kap. 14 § LUF respektive 17 kap. 14 § LOU).

Ändringsklausuler

Enligt 16 kap. 10 § LUF respektive 17 kap. 10 § LOU får ett kontrakt eller ett ramavtal ändras i enlighet med en ändringsklausul utan att en ny upphandling måste genomföras, om kontraktets eller ramavtalets övergripande karaktär inte ändras och klausulen (1) har angetts i något av upphandlingsdokumenten i den ursprungliga upphandlingen, (2) klart, exakt och entydigt beskriver under vilka förutsättningar den kan tillämpas, och (3) anger omfattningen och arten av ändringarna som kan komma att göras.

Utgångspunkten vid bedömningen av undantagets tillämplighet är således att ändringsklausulen till sin karaktär är så pass konkretiserad att de ändringar som vidtas i enlighet med denna är förutsebara för befintliga och potentiella leverantörer. I sammanhanget bör dock framhållas att Lagrådet, i yttrande över lagrådsremissen ”Nytt regelverk om upphandling” angav att ”[d]*et säger sig självt att en tolkning av kravet enligt ordalydelsen skulle medföra att endast få ändringsklausuler skulle uppfylla kravet. Avsikten kan dock inte vara att bara klausuler som uppfyller dessa mycket högt ställda krav ska få användas utan ny upphandling*”.[55] Det är därmed, enligt vår mening, inte osannolikt att dessa högt ställda krav på förutsebarhet kan komma att mjukas upp något i efterföljande rättspraxis.

---

54 Upphandlingsmyndighetens rapport 2017:4, *Ändringar av kontrakt och ramavtal – möjligheterna i den nya upphandlingslagstiftningen,* s. 22.

55 Lagrådets yttrande över lagrådsremissen Nytt regelverk om upphandling, s. 205.

I offentliga IT-avtal förekommer det att ändrings- respektive omförhandlingsklausuler är utformade så att myndigheten ensidigt har rätt att vidta vissa på förhand angivna villkorsändringar eller styra över vad som förhandlas. Utifrån det ovanstående kan konstateras att i den mån biträdesavtalet innehåller en ändringsklausul som till sin karaktär är klar, exakt och entydig vad gäller den upphandlande myndighetens/enhetens möjligheter att justera avtalet i enlighet med GDPR:s krav, bör ändringen i princip vara tillåten enligt LOU/LUF (förutsatt att avtalets övergripande karaktär inte ändras). EU-domstolens praxis innebär nämligen, som belysts ovan, att den upphandlande myndigheten/enheten har tämligen långtgående möjligheter att ändra ett befintligt kontrakt under förutsättning att dessa ändringar på förhand finns tydligt specificerade i upphandlingsdokumenten.[56] Det förhållandet har även bekräftats av Högsta förvaltningsdomstolen som konstaterat att en prissänkning, som hade stöd i avtalet, var tillåten eftersom samtliga leverantörer redan från början hade kännedom om att prisjusteringar kunde komma att ske under avtalstiden.[57]

Problematiken uppstår emellertid när ändringsklausuler i biträdesavtal är standardiserade och alltför generellt hållna i förhållande till de ändringar som aktualiseras med anledning av GDPR. Ändringsklausulen måste i vart fall, som minimum, ange att ändringar kan komma att ske för att tillgodose de krav som följer av tillämplig dataskyddslagstiftning från tid till annan, för att anpassningar enligt GDPR ska kunna tänkas vara tillåtna. För att den upphandlande myndigheten/enheten dessutom ska kunna ta höjd för eventuella prishöjningar eller motsvarande krav från leverantören, krävs därutöver dels att grunden för beräkningen framgår på ett tydligt och förutsebart sätt, dels att klausulen reglerar under vilka specifika omständigheter en prisjustering kan påkallas och av vem. En hänvisning till generella lagändringar/ändrade förhållanden under avtalsperioden torde därmed, enligt vår uppfattning, vara otillräcklig. För biträdesavtalens vidkommande innebär det sagda att ändringsklausuler, i den mån sådana finns, ibland inte uppfyller de krav på precisering som uppställs i upphandlingslagarna.

En särskild problematik uppstår vid tillämpningen av s.k. omförhandlingsklausuler i biträdesavtal, som definitionsmässigt inbjuder till förhandling av kontraktsvillkoren. En vanligt förekommande skrivning är exempelvis att ”[den personuppgiftsansvarige] *förbehåller sig rätten att omförhandla villkoren i avtalet, om väsentliga förändringar i förutsättningarna för avtalet skulle inträffa under avtalsperioden*”. En obegränsad omförhandlingsklausul möjliggör inte för eventuella anbudsgivare att ta ställning till hur villkoren i kontraktet kommer att se ut efter sådana förhandlingar och uppfyller följaktligen inte kravet på transparens. I sammanhanget ska dock framhållas att även för det fall omförhandlingsklausulen som sådan skulle underkännas av en domstol, utgör den ändring som förhandlats fram inte nödvändigtvis en otillåten väsentlig ändring i förhållande till villkoren i det

56 Se exempelvis EU-domstolens dom i mål C-496/99, *Succhi di Frutta*, punkt 117–118 och mål C-454/06, *Pressetext*.

57 Se HFD 2016 ref. 85

ursprungliga kontraktet. Förvaltningsrätten måste ändå, vid en rättslig prövning, bedöma huruvida den framförhandlade ändringen är förenlig med 16 kap. 14 § LUF respektive 17 kap. 14 § LOU (för utförligare resonemang gällande väsentliga förändringar, se nedan).

Det förekommer även klausuler som medför att leverantören åtar sig att tillhandahålla tjänsten i enlighet med förändrade lagkrav och således bär den ekonomiska risken för att tjänsten uppfyller vid var tid gällande lagstiftning. Avtalsvillkoren sätts i regel ensidigt (som obligatoriskt krav) av den upphandlande myndigheten/enheten, vilket sällan medför att leverantörens åtagande kompletteras med en rätt till ersättning/kompensation för leverantören. Under sådana förhållanden torde anpassningar enligt GDPR vara oproblematiska ur ett upphandlingsperspektiv, eftersom de *de facto* inte medför en villkorsändring och leverantören inte har möjlighet att förhandla sig till kompensation för sitt utökade åtagande.

Avslutningsvis ska framhållas att det inte finns någon heltäckande ändringsklausul som garanterar att justeringar i biträdesavtalet sker i enlighet med gällande upphandlingsregelverk – i väntan på vägledning från rättspraxis bör således ändringar i befintliga biträdesavtal med stöd av ändringsklausuler vidtas med viss försiktighet.

Kompletterande beställningar

Av 17 kap. 11 § LOU respektive 16 kap. 11 § LUF framgår att en kompletterande beställning av varor, tjänster eller byggentreprenader får göras från den leverantör som har tilldelats kontraktet utan att en ny upphandling måste genomföras, under förutsättning att (1) beställningen har blivit nödvändig, (2) leverantören av ekonomiska eller tekniska skäl inte kan bytas, och (3) ett byte av leverantör skulle medföra betydande olägenheter eller betydligt större omkostnader för den upphandlande myndigheten/enheten. Enligt 17 kap. 11 § LOU får en sådan ändring inte heller innebära att värdet av kontraktet eller ramavtalet ökar med mer än 50 procent (vilket således skiljer sig från motsvarande undantagsbestämmelse i LUF).

Därtill framgår, av både LOU och LUF, att om flera kompletterande beställningar görs efter varandra, ska begränsningen i fråga om ökningen av värdet tillämpas på varje enskild beställning.

17 kap. 11 § i LOU genomför artikel 72.1 första stycket b i LOU-direktivet och 16 kap. 11 § LUF genomför artikel 89.1 första stycket b i LUF-direktivet. Bestämmelserna saknar motsvarighet i 2007 års upphandlingslagar. Undantaget är avsett att tillämpas i situationer då leverantörsbyte inte kan göras på grund av exempelvis krav på utbytbarhet eller driftskompatibilitet med redan befintlig utrustning, tjänster eller installationer. Av direktiven framgår att en kompletterande beställning bör vara tillåten om ett leverantörsbyte skulle tvinga den upphandlande myndigheten att anskaffa materiel, byggentreprenader eller tjänster med andra tekniska egenskaper med åtföljande

inkompatibilitet eller oproportionerliga tekniska svårigheter vid användning eller underhåll.[58]

Enligt förarbetena till de nya upphandlingslagarna får sådana tekniska skäl som avses även anses innebära betydande olägenheter enligt första stycket 3. Det ligger nämligen, enligt regeringen, i sakens natur att det måste anses vara omöjligt att byta leverantör enligt första stycket 2 och 3, om ett leverantörsbyte skulle vara en otillåten ändring av kontraktet. Om ett leverantörsbyte är en tillåten ändring av kontraktet, men skulle medföra betydligt större omkostnader för den upphandlande myndigheten än en kompletterande beställning, får myndigheten istället göra en kompletterande beställning från befintlig leverantör. Betydligt större omkostnader enligt första stycket 3 får även anses utgöra ett ekonomiskt skäl enligt första stycket 2.[59]

Det sagda får särskild betydelse för ändringar av upphandlande IT-tjänster, eftersom tjänsterna inte sällan är av sådan karaktär att ett leverantörsbyte skulle innebära väsentliga svårigheter i tekniskt hänseende (exempelvis vad beträffar drift- eller supportleverantörer). Det skulle därmed kunna argumenteras för att en ny annonserad upphandling av sådana IT-tjänster till följd av ändringar i biträdesavtalet (som ofta ligger som bilaga till sådana tjänsteavtal), skulle föranleda betydande olägenheter eller betydligt större omkostnader för den upphandlande myndigheten/enheten. Enligt detta synsätt skulle den upphandlande myndigheten/enheten ha möjlighet att göra en kompletterande beställning till biträdesavtalet och därigenom täcka in tillkommande säkerhetsåtgärder med anledning av GDPR i form av exempelvis pseudonymisering och kryptering av personuppgifter eller förfaranden för att regelbundet testa, undersöka och utvärdera hur effektiva säkerhetsåtgärderna är.

Vår bedömning är emellertid att det framstår som ytterst tveksamt om ändringar enligt GDPR kan göras med stöd av det aktuella undantaget. Emot ovanstående resonemang kan nämligen argumenteras att det i praktiken inte rör sig om någon kompletterande beställning, eftersom leverantörens utökade åtagande föranleds av tvingande författningsändringar. Det rör sig följaktligen inte om en tillkommande beställning inom ramen för den underliggande tjänsteleveransen (dvs. huvudavtalet), utan endast om förändrade förutsättningar/villkor för genomförandet av tjänsteleveransen. Det framstår således som tveksamt att bestämmelsen skulle omfatta andra typer av kompletterande beställningar än rena volymökningar inom ramen för en underliggande tjänsteleverans (dvs. tillkommande anskaffningar av ”samma sak”). Det faktum att lagtextens utformning i 17 kap. 10 § LOU skiljer sig åt från 17 kap. 11 § samma lag, ger ytterligare stöd för en sådan uppfattning. I 10 § anges nämligen uttryckligen att det är ”*ändringar*” som avses, medan lagstiftaren istället valt att i 11 § använda termen ”*kompletterande beställningar*”. En skillnad i ordalydelse mellan två bestämmelser som antagits på samma dag får förmodas

58 Skäl 108 LOU-direktivet och skäl 114 i LUF-direktivet.

59 Prop. 2015/16:195, s. 1129-1130.

vara avsedd, med följden att man i sådana situationer ska vara försiktig med att tolka bestämmelser av samma slag, men med olika lydelse, på samma sätt. Vidare får kraven förstås som högt ställda och avsedda att tillämpas endast i rena undantagssituationer.

Ändringar till följd av oförutsebara omständigheter

Vad härefter gäller ändringar till följd av oförutsebara omständigheter, föreskriver 16 kap. 12 § LUF respektive 17 kap. 12 § LOU att ett kontrakt eller ett ramavtal får ändras utan en ny upphandling under förutsättning dels att behovet av ändringen beror på omständigheter som den upphandlande myndigheten eller enheten varken förutsåg eller borde ha förutsett vid beslutet att tilldela kontraktet eller att ingå ramavtalet, dels att ändringen inte medför att kontraktets eller ramavtalets övergripande karaktär ändras. Enligt 17 kap. 12 § LOU får en sådan ändring inte heller innebära att värdet av kontraktet eller ramavtalet ökar med mer än 50 procent (vilket således skiljer sig från motsvarande undantagsbestämmelse i LUF).

Vid tolkningen av begreppet ”*oförutsebara omständigheter*” ligger det nära tillhands att dra paralleller till bestämmelserna om förhandlat förfarande utan föregående annonsering på grund av synnerlig brådska i 6 kap. 15 § LOU (motsvarande 4 kap. 5 § första stycket 3 ÄLOU), där i princip motsvarande rekvisit återfinns. Kravet på oförutsebarhet har av EU-domstolen ställts högt, vilket innebär att omständigheterna i det närmaste ska ha karaktären av force majeure.[60] Av LOU- och LUF-direktiven framgår att begreppet oförutsebara omständigheter tar sikte på sådana *yttre* omständigheter som den upphandlande myndigheten inte hade kunnat förutse (eller borde ha förutsett) när den tilldelade kontraktet trots att myndigheten visade skälig omsorg i förberedelserna inför kontraktstilldelningen.[61]

Huruvida författningsändringar kan anses utgöra sådana oförutsebara omständigheter har, såvitt vi vet, inte behandlats i EU-domstolens praxis. Visserligen kan argumenteras för att EU-domstolens mycket restriktiva tolkning av begreppet, liksom det förhållandet att författningsändringar i civilrättslig mening inte anses utgöra force majeure (såvida parterna inte uttryckligen avtalat om annat)[62], talar emot att villkorsändringar i biträdesavtalen kan ske med stöd av undantaget för oförutsebara omständigheter. Vår uppfattning är emellertid att en sådan rigid tolkning av undantaget inte kan ha varit avsikten, eftersom undantaget syftar till att skapa viss flexibilitet när fullgörandet av kontraktet sker under en längre tidsperiod.[63]

---

60 Se EU-domstolens dom i mål C-318/94, *Kommissionen mot Tyskland* och mål C-107/92, *Kommissionen mot Italien*, liksom förenade målen C-20/01 och C-28/01, C-394/02 och C-126/03. Jfr även Kammarrätten i Sundsvalls avgöranden i mål nr 3208–14 och 3209–14.

61 Skäl 109 LOU-direktivet och skäl 115 i LUF-direktivet.

62 Jfr exempelvis 27, 40 och 57 §§ köplagen samt UNIDROIT Principles Artikel 7.1.7, i PECL 8:108 och DCFR III. – 3:104.

63 Se skäl 109 i LOU-direktivet.

Utgångspunkten måste således vara vad den upphandlande myndigheten/enheten skäligen borde ha känt till avseende orsaken till ändringsbehovet när den tilldelade kontraktet. Den relevanta frågeställningen är följaktligen huruvida den upphandlande myndigheten/enheten, vid tillfället för kontraktstilldelningen, på grundval av vad som då var känt, hade kunnat skriva en klar, precis och entydig ändringsklausul som tagit höjd för de ändrade förhållandena. Om svaret på den frågan är nekande var omständigheterna oförutsebara. Om svaret däremot är jakande var omständigheterna förutsebara, med följden att undantaget inte är tillämpligt.

Vad beträffar biträdesavtalen innebär ovanstående slutsatser att undantaget kan bli tillämpligt fram till dess att det funnits ett slutligt förslag till GDPR:s innehåll (enligt dess nuvarande lydelse). Det slutliga förslaget till GDPR fastslogs den 15 december 2015 efter överenskommelse mellan Europaparlamentet, EU-kommissionen och Europeiska unionens råd, och publicerades sedermera i EU:s officiella tidning den 4 maj 2016.[64] Det innebär att biträdesavtal som tecknats efter den senare tidpunkten skäligen borde tagit höjd för kommande författningsändringar genom införandet av en ändringsklausul. Biträdesavtal som däremot tecknats dessförinnan, borde enligt vår uppfattning kunna ändras med stöd av undantaget för oförutsebara omständigheter, givet att kontraktets övergripande karaktär inte ändras. Det kan emellertid inte uteslutas att tidigare reformförslag, beroende på dess innehåll och allmänna tillgänglighet, kan ha betydelse för den bedömningen.

Ändringar som inte är väsentliga

Slutligen framgår av 16 kap. 14 § LUF respektive 17 kap. 14 § LOU att en ändring av ett kontrakt eller ramavtal alltid får ske om den inte är väsentlig. I samma paragraf klargörs även, i en icke-uttömmande lista, vilka typer av ändringar som ska betraktas som väsentliga. Där framgår att en ändring är väsentlig bl.a. om den (1) inför nya villkor, som om de hade ingått i den ursprungliga upphandlingen, skulle ha medfört att andra anbudssökande bjudits in att lämna anbud, att andra anbud skulle ha ingått i utvärderingen eller att ytterligare leverantörer skulle ha deltagit upphandlingen, (2) innebär att kontraktets eller ramavtalets ekonomiska jämvikt ändras till förmån för den leverantör som har tilldelats kontraktet eller är part i ramavtalet, (3) medför att kontraktets eller ramavtalets omfattning utvidgas betydligt, eller (4) innebär byte av leverantör. Eftersom listan enbart är exemplifierade innebär det att även andra omständigheter kan komma att beaktas vid bedömningen av huruvida ändringen är väsentlig.

För biträdesavtalens vidkommande är punkterna 1 och 2 ovan av särskild betydelse. Innebär t.ex. eventuella prishöjningar och/eller utökade ansvarsbegränsningar i biträdesavtalen nödvändigtvis att kontraktets

64 https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#.

ekonomiska jämvikt ändras till förmån för den leverantör som tilldelats kontraktet? Vid en första anblick förefaller svaret på frågeställningen vara tämligen enkelt, men vid en närmare analys är svaret inte lika självklart. Prishöjningen föranleds ju nämligen av ett korresponderande åtagande från leverantören som annars hade rubbat den ekonomiska balansen i avtalet till leverantörens nackdel. De ändringar i biträdesavtalen som föranleds av GDPR kommer med all sannolikhet att medföra kostnader som leverantören inte haft anledning att beakta vid den ursprungliga prissättningen av IT-leveransen. Leverantören måste därutöver ta höjd för risken för eventuella sanktioner, eftersom administrativa sanktionsavgifter och skadestånd under GDPR även gäller för personuppgiftsbiträdet i vissa fall.[65] Under sådana förhållanden är det inte givet att en prishöjning per automatik innebär att avtalets ekonomiska jämvikt ändras till förmån för leverantören.[66]

Ovanstående resonemang får även bäring på punkten 1 ovan, dvs. frågan om prishöjningen, om villkoret hade ingått i den ursprungliga upphandlingen, skulle ha medfört att andra anbudssökande bjudits in att lämna anbud, att andra anbud skulle ha ingått i utvärderingen eller att ytterligare leverantörer skulle ha deltagit i upphandlingen. Under förutsättning att prishöjningen uteslutande motsvarar leverantörens utökade åtagande, och själva nettovinsten av biträdesavtalet därmed (med viss marginal) förblir oförändrad, innebär en prishöjning inte med automatik att konkurrensen vid tidpunkten för upphandlingen snedvridits till nackdel för övriga befintliga och potentiella anbudsgivare.

Däremot kan inte uteslutas att andra potentiella anbudsgivare hade kunnat offerera bättre anpassade lösningar om det var känt från början att ändringar under kontraktets löptid skulle komma att ske vid en viss senare tidpunkt för att uppfylla GDPR:s utökade krav. Kanske hade den befintliga leverantören vid den ursprungliga anbudsgivningen inte överhuvudtaget åtagit sig att uppfylla de ändrade kraven vid det tillfälle då ändringen aktualiseras, med följden att ett annat anbud skulle ha blivit det bästa anbudet. Upphandlingen skulle följaktligen kunna ha fått en annan utgång, om de ändringar som senare förväntades ske vid GDPR:s ikraftträdande varit en del av anbudsförutsättningarna från början. Det kan inte heller bortses från att det faktum att den ekonomiska obalansen från början föranletts av tvingande författningsändringar, och inte av kommersiella hänsyn, kan ha betydelse för bedömningen av huruvida en eventuell prishöjning rubbar den ekonomiska jämvikten i avtalsförhållandet. Någon vägledning i det avseendet erbjuds varken av direktiven eller förarbetena.

Som ovan konstateras är den lista som anges i 17 kap. 14 § LOU respektive 16 kap. 14 § LUF exemplifierande och inte uttömmande. Listan innehåller inte heller kumulativa rekvisit, vilket innebär att det är

65 Jfr artikel 82-83 GDPR.

66 Jfr Arrowsmith, Sue, *The Law of Public and Utilities Procurement*, volume 1, third ed., Sweet and Maxwell, 2014, s. 585.

fullt tillräckligt att ett av rekvisiten är uppfyllt för att ändringen ska betraktas som väsentlig och därmed otillåten. Mot den bakgrunden är vår bedömning sammanfattningsvis att ändringar i befintliga biträdesavtal, i den mån ett materiellt förändringsbehov finns, med övervägande sannolikhet kommer att betraktas som väsentliga, även om det finns vissa argument som också talar emot en sådan slutsats. Det medför i sin tur att ändringar som utgångspunkt inte kommer att kunna göras i biträdesavtalen utan att någon av de undantagssituationer som redogjorts för ovan föreligger.

Slutligen ska dock framhållas att vissa biträdesavtal redan i dagsläget sannolikt uppfyller flertalet av de krav som tillkommit i GDPR, såtillvida att kraven i stora delar utgör en kodifiering av tidigare praxis (se avsnitt 3). I dessa fall kan det röra sig om mindre, formella, anpassningar av avtalstexten, varvid det sakliga innehållet i stort alltjämt förblir detsamma. Under sådana förhållanden skulle ändringarna kunna vara tillåtna, eftersom det då inte rör sig om en väsentlig förändring i den mening som avses i LOU respektive LUF.

Kolliderande lagar?

Som framgår ovan kommer den upphandlande myndigheten/enheten att i vissa fall ställas inför dilemmat att antingen bryta mot bestämmelserna i GDPR eller mot bestämmelserna i LOU respektive LUF. Så är fallet om ändringen som sådan är väsentlig men nödvändig för att efterleva GDPR:s utökade krav, och ingen av undantagsbestämmelserna som redogjorts för ovan är tillämplig. Vi kommer mot denna bakgrund att redogöra för den riskavvägning som aktualiseras med anledning av ett sådant dilemma.

Bristande efterlevnad av bestämmelserna i GDPR kan resultera i administrativa sanktionsavgifter. Enligt artikel 83.7 i GDPR får varje medlemsstat emellertid reglera om och i vilken utsträckning det ska vara möjligt att besluta om sanktionsavgifter mot offentliga myndigheter och organ. I Dataskyddsutredningens betänkande till ny dataskyddslag, föreslås bestämmelser som innebär att den reglering avseende påförande av sanktionsavgifter som finns i artikel 83.1–3 i GDPR ska gälla vid beslut även mot myndigheter. Enligt den föreslagna paragrafen ska avgiften, vid överträdelser som avses i artikel 83.4 i GDPR, bestämmas till högst 10 MSEK, och annars till högst 20 MSEK.[67]

En väsentlig ändring utan föregående annonsering betraktas i sin tur som en otillåten direktupphandling enligt LOU respektive LUF. Det innebär att de sanktioner som kan aktualiseras är ogiltigförklaring och upphandlingsskadeavgift enligt 20 kap. 13 § och 21 kap. 1 § LUF respektive LOU. Därutöver riskerar den upphandlande myndigheten/enheten att ådra sig skadeståndsansvar motsvarande det positiva kontraktsintresset i förhållande till de leverantörer som kan göra

67 SOU 2017:39, *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*, s. 382-383.

sannolikt att de hade tilldelats avtalet om upphandlingen rätteligen hade föregåtts av annonsering. Av 21 kap. 4 § LOU respektive LUF framgår att upphandlingsskadeavgiften ska uppgå till lägst 10 000 kronor och högst 10 MSEK. Avgiften får dock aldrig överstiga tio procent av upphandlingens värde.

Det kan således konstateras att upphandlingsskadeavgiftens storlek enligt LOU/LUF inte ligger i paritet med de administrativa sanktionsavgifterna som följer av GPDR; sanktionsavgifterna enligt GDPR är potentiellt betydligt högre. Om och i vilken grad detta bör vara utslagsgivande i en situation där GDPR kolliderar med LOU/LUF låter vi vara osagt.

5. Direktmarknadsföring och profilering

Inledning

I detta avsnitt kommer vi att behandla GDPR:s betydelse för direktmarknadsföring. Vi kommer också att redogöra för GDPR:s bestämmelser om profilering och automatiserat individuellt beslutsfattande, framförallt såvitt avser dessa bestämmelsers eventuella inverkan på riktade marknadsföringsaktiviteter.

Avsnittet disponeras enligt följande. Inledningsvis redogör vi för såväl PuL:s som för GDPR:s reglering avseende laglig grund för personuppgiftsbehandling som sker för direktmarknadsföring. I det efterföljande avsnittet redogör vi särskilt för GDPR:s bestämmelser om profilering och frågan om huruvida profilering för marknadsföringsändamål kan omfattas av GDPR:s reglering avseende automatiserat individuellt beslutsfattande. Avslutningsvis diskuteras frågeställningarna och våra slutsatser genom en sammanfattande kommentar.

Laglig grund för direktmarknadsföring

ALLMÄNT

Integritetsskydd i förhållande till direktmarknadsföring aktualiserar en rad bestämmelser i GDPR men även i annan lagstiftning.[68]

Personuppgiftsbehandling för direktmarknadsföring får som utgångspunkt vidtas med stöd av en intresseavvägning, såväl under PuL som GDPR. Marknadsföring betraktas nämligen som ett sådant ändamål som anses utgöra ett s.k. berättigat intresse, vilket ofta väger tyngre än den registrerades intresse av att inte bli föremål för direktmarknadsföring.[69]

Möjligheterna att enligt GDPR behandla personuppgifter för direktmarknadsföring med stöd av en intresseavvägning motsvarar i stort de som redan gäller enligt PuL, varför den praxis och vägledning som finns under PuL bör vara aktuell vid tolkning och tillämpning av motsvarande bestämmelser i GDPR. Detta gäller åtminstone i avvaktan på ytterligare förtydliganden och vägledning från Datainspektionen eller behörigt EU-organ.

---

68 Jfr bestämmelserna om obeställd reklam i 19-20 §§ marknadsföringslagen (2008:486), vilka implementerar artikel 13 i 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) (det s.k. ePrivacy-direktivet). Nämnda regelverk avhandlas inte vidare i denna rapport.

69 Skäl 47 GDPR.

NÄR KRÄVS SAMTYCKE?

Följande aktiviteter i anslutning till direktmarknadsföring har i Datainspektionens praxis samt i förarbeten ansetts vara tillåtna med stöd av en intresseavvägning: [70]

- framställa adressbärare för utskick av direktadresserat reklammaterial i reklamkampanj,
- skicka ut direktreklam via eget kund-/medlemsregister eller branschregister,
- upprätta listor över telefonnummer för telefonförsäljning, eller
- följa upp direktreklamskampanjer genom statistisk bearbetning.

Följande aktiviteter har **inte** ansetts vara tillåtna med stöd av en intresseavvägning, utan har ansetts kräva laglig grund i form av samtycke från den registrerade:[71]

- lämna ut, byta eller sälja sitt medlemsregister,
- fördjupa registerinnehåll genom sambearbetning av uppgifter från olika personregister, t.ex. genom att registrera kreditupplysningsinformation,
- lämna ut uppgift om vem som har motsatt sig personuppgiftsbehandling, eller
- registrering av en kunds inköpsvanor för att ta fram kundprofiler för inköpsbaserad marknadsföring.

Vi kan konstatera att Datainspektionens vägledning i fråga om laglig grund för direktmarknadsföring baserad på PuL, knappast ger en tydlig och fullödig bild över gränsdragningen mellan intresseavvägning och samtycke. I dag används dessutom mer sofistikerade metoder vid behandling av personuppgifter för direktmarknadsföringsändamål, såsom t.ex. profilering, kundsegmentering, beteendeanalys och s.k. *marketing automation*. En modern digital marknadsföring bygger vidare ofta på att ett stort antal uppgifter samlas in från en rad olika källor. Sådana metoder som nu beskrivits medför typiskt sett större risker ur ett integritetsskyddsperspektiv än de relativt traditionella metoder som nämns i Datainspektionens praxis och uttalanden ovan. För att närmare utreda och ta ställning till om och i vilken utsträckning även sådana metoder kan utföras med stöd av en intresseavvägning under GDPR krävs en närmare analys av bestämmelserna om såväl profilering som automatiserat individuellt beslutsfattande (se vidare nedan).

SÄRSKILT OM INTRESSEAVVÄGNING

Om, och i den mån, direktmarknadsföring övervägs med stöd av en intresseavvägning, så bör åtminstone följande omständigheter tillmätas betydelse:[72]

---

70 Se Öman & Lindblom, *Personuppgiftslagen: en kommentar*, s. 247-248.

71 Ibid.

72 Ibid. Se även Artikel 29-gruppen, *Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG*, s. 35-45.

OMSTÄNDIGHET MED RELEVANS FÖR INTRESSEAVVÄGNING[73]	KOMMENTAR
Vem marknadsföringen riktas till.	Större hänsyn krävs typiskt sett om marknadsföringen riktar sig till barn, konsumenter eller andra sårbara grupper.
Marknadsföringens omfattning och vilket sätt uppgifterna ska behandlas på.	Ju mer omfattande och/eller ingående behandlingen är, desto större hänsyn krävs i förhållande till de registrerade.
Avsändarens ställning i förhållande till den registrerade.	En stark position i förhållande till den registrerade medför normalt sett mindre utrymme för att intresseavvägningen ska utfalla till den personuppgiftsansvariges fördel.
Vilken typ av personuppgifter som behandlingen i fråga är tänkt att omfatta.	Ju mer integritetskänsliga uppgifter som ska behandlas, desto större krav på säkerhet och desto mindre sannolikt är det att intresseavvägningen utfaller till den personuppgiftsansvariges fördel. I samband med behandling av sådana uppgifter bör även övervägas: • om uppgifterna kräver särskilt skydd, • om det finns särskilda bestämmelser i lag eller förordning, såsom sekretessbestämmelser, som måste beaktas, eller • vilka säkerhetsåtgärder och gallringsrutiner som behandlingen omfattas av. I detta avseende kan bl.a. beaktas huruvida: - behandlingen innebär att stora mängder personuppgifter behandlas eller kombineras (samkörs) med andra uppgifter, - behandlingen annars medför fördjupad kunskap om den registrerade, eller - behandlingen kan anses ligga inom ramen för vad en förnuftig person rimligen kan förvänta sig, samt de eventuella konsekvenserna för den registrerade.
På vilket sätt den registrerade har möjlighet att motsätta sig behandlingen enligt artikel 21.2 GDPR.	Exempelvis genom de s.k. NIX-registren, eller en direktlänk via e-post med möjlighet för den registrerade att invända mot direktmarknadsföring.
Vilken information de registrerade har fått.	Bedöms bl.a. i förhållande till vad som kan anses utgöra den registrerades rimliga förväntningar.

73 Bedömningen av personuppgiftsbehandling för direktmarknadsföring ska under PuL även ske i ljuset av vad som utgör god sed (jfr 9 § b) PuL). Datainspektionen har i praxis tillämpat bl.a. Swedmas branschöverenskommelse avseende regler om användning av personuppgifter vid direktmarknadsföring. Nämnda standard finns också omnämnd i Datainspektionens vägledande informationsskrift (se Datainspektionens informationsskrift om intresseavvägning, version reviderad 2015.) För exempel på hur Datainspektionen bedömt behandling av personuppgifter för ändamålet direktmarknadsföring med hänvisning till kravet på god sed, se Datainspektionens beslut den 8 juni 2005, dnr 1812-2004 respektive beslut den 15 oktober 2015, dnr 1382-2014. I sistnämnda fall beaktade Datainspektionen även särregler för direktmarknadsföring, i aktuellt fall i fråga om spelverksamhet.

GDPR:s legaldefinition av profilering

Vid behandling av personuppgifter för direktmarknadsföringsändamål behöver den personuppgiftsansvarige beakta om behandlingen utgör eller medför profilering i GDPR:s mening. Detta eftersom behandling som sker för marknadsföringsaktiviteter och som utgör profilering träffas av särskilda bestämmelser i GDPR.

Definitionen av profilering i artikel 4.4 GDPR lyder enligt följande:

"*profilering: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar*".

Det finns enligt vår mening anledning att ta i beaktande om flertalet metoder för dagens riktade marknadsföringsåtgärder (se ovan) uppfyller legaldefinitionen av profilering. Detta gäller exempelvis i förhållande till marknadsföring baserad på kundsegmentering, kundanalys och riktade utskick baserat på tidigare inköp.

Varför anses den enskilde särskilt skyddsvärd i förhållande till profilering?

GDPR innehåller alltså, till skillnad från PuL och det bakomliggande Dataskyddsdirektivet, ett utökat skydd för enskilda vid profilering. Bestämmelserna är dock inte alldeles nya utan följer i princip den linje som tidigare utvecklats av Artikel 29-gruppen.[74]

Anledningen till att profilering har reglerats närmare i GDPR är att sådan behandling typiskt sett medför ökad risk utifrån ett integritetsskyddsperspektiv. Artikel 29-gruppen har uttalat att det finns tydliga risker med profilering, eftersom sådan kan medföra:

- (alltför) omfattande behandling av personuppgifter,
- risk för felaktiga slutsatser,
- att särskilda kategorier av personuppgifter oavsiktligt behandlas genom slutsatser av bearbetade data som sett för sig inte utgör särskilda kategorier av personuppgifter, och
- eventuella (stora) ekonomiska konsekvenser för den registrerade.[75]

Artikel 29-gruppen har vidare uttalat att en behandling som innebär att en personuppgiftsansvarig kombinerar stora mängder uppgifter om de registrerade, vilka ursprungligen har samlats in i andra sammanhang och för olika ändamål, och skapar komplexa tolkningar av

74 Jfr Artikel 29-gruppen, *Yttrande 6/2014*, s. 27.

75 Artikel 29-gruppen, *Yttrande 6/2014*, s. 35.

kundernas personligheter och preferenser utan deras vetskap, sannolikt skulle kunna innebära ”*ett betydande intrång i* [*den registrerades*] *rättigheter*” och att det kan innebära att personuppgiftsansvariges intressen överskuggas av den registrerades intressen och rättigheter.[76]

Profilering som innebär behandling av stora datamängder, eller som i övrigt är omfattande eller långtgående i förhållande till den registrerades personliga sfär, utgör enligt vår bedömning ett sådant betydande intrång i den registrerades rättigheter att behandlingen typiskt sett inte får utföras med stöd av en intresseavvägning.

Laglig grund vid förekomsten av profilering

GDPR innehåller inte något specifikt uttalat krav på inhämtande av samtycke för att kunna genomföra profilering. GDPR ställer dock särskilda krav på den personuppgiftsansvarige vad gäller öppenhet gentemot den registrerade. Detta uttrycks i skälen till GDPR, där det särskilt i fråga om profilering anges att den registrerade bör ”[...] *informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering* [...]”.[77] GDPR innehåller således numera en rekommendation om att informera den registrerade om förekomsten av profilering som sådan.[78]

Profilering betraktas och bedöms enligt GDPR således som en särskild behandlingstyp. I fråga om laglig grund framgår dock av GDPR att en intresseavvägning även i fall av profilering kan utfalla till den personuppgiftsansvariges fördel.[79] Huruvida profilering kan ske med stöd av en intresseavvägning eller inte måste dock bedömas i varje enskilt fall, beroende på bl.a. profileringens omfattning och dess väntade följder för den registrerade.

Artikel 29-gruppen har därutöver uttalat att när en organisation vill analysera eller förutsäga personliga preferenser, beteende och attityder hos enskilda kunder, för att senare informera om åtgärder eller beslut avseende dessa kunder, så är ett fritt, specifikt, informerat och ett tydligt/otvetydigt ”opt in”-samtycke nästan alltid nödvändigt för att få behandla personuppgifterna. Det kan nämnas att Artikel 29-gruppen i ett annat sammanhang har uttalat att samtycke bör inhämtas för spårning och profilering i syfte att genomföra direktmarknadsföring, beteendestyrd annonsering, reklam eller datamäklares försäljning av uppgifter, platsbaserad annonsering

76 Artikel 29-gruppen, *Yttrande 6/2014,* s. 27.

77 Skäl 60 GDPR.

78 Behovet av en balanserad syn på förekomsten av profilering som sådan, inklusive mekanismer för ökad transparens och kontroll för registrerade, uttrycktes i anslutning till lagstiftningsarbetet med GDPR med hänvisning till behovet av ökade krav på information till den registrerade i fråga om profilering, betydelsen av krav på uttryckligt samtycke till profilering samt krav på riskhantering (konsekvensbedömning). Se Artikel 29-gruppens *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation* den 13 maj 2013, s. 3-4.

79 Artikel 21.1 GDPR.

eller spårningsbaserade digitala marknadsundersökningar.[80] I sammanhanget kan också noteras att Artikel 29-gruppen avser att publicera ett nytt yttrande avseende profilering enligt GDPR.[81]

Vid behandling för direktmarknadsföringsändamål **utan** profilering kommer en intresseavvägning oftare utfalla till den personuppgiftsansvariges fördel jämfört med samma typ av behandling som **inbegriper** profilering. Detta eftersom profilering till sin natur kan innebära större intrång i den registrerades friheter och rättigheter.

I likhet med vad som gäller under PuL har den registrerade under GDPR en ovillkorlig rätt att invända mot att behandling av hans eller hennes personuppgifter sker för direktmarknadsföring.[82] I GDPR omnämns särskilt att rätten att invända omfattar profilering som sker för direktmarknadsföringsändamål.[83] Denna rätt innebär att, om den registrerade invänt mot behandling för direktmarknadsföringsändamål, så väger den registrerades intresse av att inte bli föremål för direktmarknadsföring tyngre än den personuppgiftsansvariges intresse att behandla personuppgifterna för samma ändamål. Detta innebär att den personuppgiftsansvarige inte längre får behandla den registrerades personuppuppgifter för direktmarknadsföring med stöd av intresseavvägning. Information om rätten att invända mot behandlingar av nämnda slag ska lämnas senast vid den första kommunikationen med den registrerade.[84] Notera även att den registrerade i övrigt har en allmän rätt i artikel 21 GDPR att invända mot personuppgiftsbehandling avseende honom eller henne som sker med stöd av artikel 6.1 f GDPR (intresseavvägning).

Automatiserat individuellt beslutsfattande (inbegripet profilering) enligt GDPR

ALLMÄNT

Profilering regleras även i anslutning till s.k. automatiserat individuellt beslutsfattande enligt artikel 22 GDPR:

"*Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.*"

Bestämmelsen motsvarar artikel 15 i Dataskyddsdirektivet respektive 29 § första stycket PuL.

---

80 Artikel 29-gruppen, *Yttrande 3/2013 om öppna data och vidareutnyttjande av information från den offentliga sektorn*, bilaga II, s. 45.

81 Se http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

82 Artikel 21.2 GDPR.

83 Ibid.

84 Artikel 21.4 GDPR.

Bestämmelsen tar sikte på att skydda enskilda mot utfallet av ingripande automatiserade beslut, snarare än mot förekomsten av den profilering som ofta föregår sådant beslutsfattande. Detta kritiserades av Artikel 29-gruppen under lagstiftningsarbetet med GDPR. I anslutning till detta rekommenderade Artikel 29-gruppen säkerhetsmekanismer i form av bl.a. ökade krav på information till den registrerade i fråga om profilering (se ovan). Liknande kritik har även uttalats av EU-kommissionen som redan i samband med Dataskyddsdirektivet uttryckte farhågor beträffande profilering och automatiserat beslutsfattande:"[t]*he use of extensive data profiles in individuals by powerful and private institution*[s] *deprives the individual the capacity to influence decision-making processes within those institutions* [...]".[85]

Beslut baserade på profilering som sker automatiskt utifrån vissa kriterier för bedömning av vissa personliga egenskaper, såsom vid ett automatiskt urval av individer, utgör definitionsmässigt en form av automatiserat individuellt beslutsfattande. I syfte att bedöma om artikel 22 GDPR är tillämplig måste därutöver även beaktas om sådant beslut har "*rättsliga följder*" eller på "*liknande sätt i betydande grad påverkar*" den registrerade. Härav följer att inte varje behandling som utgör profilering träffas av den särskilda bestämmelsen avseende automatiserat individuellt beslutsfattande i artikel 22 GDPR. Artikeln är tillämplig endast om och i den mån (i) det förekommer beslut, (ii) som enbart grundas på automatiserad behandling, (iii) vilket har rättsliga följder för eller på liknande sätt i betydande grad påverkar den registrerade.

Om profilering inte innebär "*rättsliga följder*" eller annars inte "*i betydande grad*" påverkar den registrerade, träffas den inte av artikel 22 GDPR. Det är då fullt möjligt att utföra profilering utan att beakta denna bestämmelse. I sådant fall är det dessutom möjligt att göra en bedömning gällande lagstöd för profilering utifrån intresseavvägning enligt artikel 6.1 f GDPR.

För det fall behandling i anslutning till direktmarknadsföring, inbegripen profilering, ger upphov till att det fattas beslut som enbart grundas på automatiserad behandling vilken **har** rättsliga följder eller på liknande sätt i betydande grad påverkar den registrerade måste artikel 22 GDPR däremot iakttas.

Om artikel 22.1 i GDPR är tillämplig gäller att den registrerade har rätt att inte bli föremål för ett beslut som omfattas av bestämmelsen. Från denna bestämmelse finns i sin tur ett antal undantag varvid ett sådant är om samtycke för behandling finns, liksom om behandlingen är nödvändig för ingående eller fullgörande av ett avtal mellan den

85 EU-kommissionens förslag *Commission Communication on the protection of individuals in relation to the processing of personal data In the Community and Information security,* COM (90)314 final-SYN 287, 13 september 1990, s. 29.

registrerade och den personuppgiftsansvarige.[86] Behandling som sker under artikel 22 GDPR kan alltså **inte** ske med stöd av en intresseavvägning. Detta gäller oavsett ändamål, dvs. oavsett om behandling sker för direktmarknadsföring eller för annat ändamål.

Automatiskt beslutsfattande inbegripet profilering enligt artikel 22 GDPR är vidare förenat med krav på obligatorisk konsekvensbedömning (se vidare avsnitt 6 nedan).[87] Det ställs även särskilda krav på information och transparens i förhållande till den registrerade i fråga om automatiserat individuellt beslutsfattande. Den registrerade ska även ges ”[...] *meningsfull information om logiken bakom* [*beslutet*] *samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade* [...]”.[88] Liknande bestämmelser finns i nuvarande lagstiftning.[89]

TILLÄMPLIGHETEN AV ARTIKEL 22 GDPR PÅ BEHANDLINGAR I DIREKTMARKNADSFÖRINGSSYFTE

Artikel 22 GDPR omfattar, liksom dess föregångare i artikel 15 Dataskyddsdirektivet, inte endast beslut som har rättsliga följder för den registrerade. Bestämmelsen tar även sikte på beslut som ”*på liknande sätt*” och ”*i betydande grad*” påverkar den registrerade.

I fråga om synen på profilering inom ramen för en bestämmelse om automatiserat beslutsfattande i GDPR efterfrågade Artikel 29-gruppen ett mer balanserat angreppssätt och rimligt tolkningsutrymme i förhållande till bestämmelsens omfattning och dess faktiska effekter – såväl positiva som negativa – som ett visst beslut medför för en registrerad. I samband med detta välkomnade Artikel 29-gruppen också ytterligare vägledning av Europeiska dataskyddsstyrelsen i fråga om tolkningen av bestämmelsens tillämpningsområde, med särskild hänvisning till uttrycket ”[*beslut som*] *i betydande grad påverkar* [*den registrerade*]”.[90] Det framhålls även i GDPR att Europeiska dataskyddsstyrelsen[91], som inrättas genom GDPR, bör kunna utfärda riktlinjer i fråga om profilering.[92]

Redan i förarbetena till 29 § första stycket PuL uttalades svårigheter med att tillämpa bestämmelsen och bedöma vilka beslut som skulle komma att omfattas. Datalagskommittén ställde sig dock positiv

86 Se artikel 22.2 c respektive artikel 22.2 a GDPR. Bestämmelsen ger även utrymme för undantag i situationer där det är nödvändigt att fatta beslut för ingående eller fullgörande av avtal mellan den registrerade och den personuppgiftsansvarige. Det ska vidare nämnas att artikel 22 GDPR hänvisar till undantag från rätten att inte bli föremål för automatiserat individuellt beslutsfattande också i fråga om s.k. särskilda kategorier av personuppgifter med hänvisning till undantagssituationer enligt EU-rätt eller nationell rätt av hänsyn till ett viktigt allmänt intresse, se artikel 22.4 GDPR samt artikel 9.2 h GDPR.

87 Artikel 35.3 a GDPR.

88 Artikel 13.2 f respektive artikel 14.2 g GDPR.

89 29 § 2 st. PuL samt artikel 12 i Dataskyddsdirektivet.

90 Artikel 29-gruppen, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 13 maj 2013, s. 4.

91 Artikel 68 GDPR.

92 Skäl 72 GDPR.

till en ”*generell lösning*” i form av ett ”*minimiskydd*” mot automatiserade beslut. I sammanhanget uttalade kommittén vidare att beslut som skulle kunna omfattas av bestämmelsen i flertalet fall ”*torde avse ekonomiska förhållanden som skatter och tullar*”.[93]

I ingressen till GDPR anges att de beslut som avses ska medföra ”*rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne*”. Som exempel på sådant beslut nämns ”*automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt*”.[94]

Den brittiska dataskyddsmyndigheten (ICO) har föreslagit att beslut som ”*i betydande grad påverkar* [*den registrerade*]” skulle kunna innefatta beslut som:

- orsakar skada, förlust eller oro (eng. *distress*) hos en enskild,
- begränsar den registrerades rättigheter eller nekar denne möjligheter,
- påverkar den registrerades hälsa eller välmående,
- påverkar den registrerades finansiella eller ekonomiska ställning,
- försätter den registrerade i en situation där han eller hon kan diskrimineras,
- innebär att särskilda kategorier av personuppgifter eller andra känsliga uppgifter, såsom uppgifter om barn, behandlas,
- föranleder att den registrerade måste ändra sitt beteende på ett märkbart vis, eller
- har osannolika, oförutsedda eller oönskade konsekvenser för individer. [95]

I sammanhanget erinrar ICO om att själva förekomsten av profilering i sig utgör en särskild form av personuppgiftsbehandling, som oavsett ändamål kan användas gentemot en enskild registrerad på ett sätt som stödjer stereotyper, segregation eller som begränsar den enskildes val och lika möjligheter.[96] ICO välkomnar, liksom Artikel 29-gruppen, en allmän standard att använda som stöd för tolkningen av artikel 22 GDPR.[97]

Det har ifrågasatts om beslut som ”*i betydande grad påverkar* [den registrerade]” endast ska omfatta situationer då den enskilde (direkt) påverkas finansiellt eller materiellt. Ett exempel på behandling av personuppgifter som, enligt denna uppfattning, också skulle kunna omfattas av bestämmelsen är marknadsföring som involverar orättvis diskriminering; t.ex. i form av att vissa personer, baserat på tidigare

93 SOU 1997:39, *Integritet ´ Offentlighet ´ Informationsteknik,* s. 407. I den politiska debatten har även försäkringsbeslut av rättslig betydelse eller som annars påverkar en individ märkbart (eng. ”*significantly*”), anses utgöra exempel på beslut som inte ska fattas automatiserat enligt vissa förutbestämda kriterier. Se Council of Europe (Europarådet), *Recommendation Rec (2002)9 on the protection of personal data collected and processed for insurance purposes* (18 September 2002), s. 9.

94 Skäl 71 GDPR.

95 ICO, *Feedback request – profiling and automated decision-making, v 1.0,* den 6 april 2017, s. 7.

96 ICO, *Feedback request – profiling and automated decision-making, v 1.0,* den 6 april 2017, s. 9.

97 ICO, *Feedback request – profiling and automated decision-making, v 1.0,* den 6 april 2017, s. 7.

sökhistorik, erbjuds varor och tjänster till olika priser eller att andra utesluts från möjligheten att införskaffa vissa varor och tjänster.[98] Enligt vår bedömning är det dock osannolikt att sådana åtgärder skulle träffas av artikel 22 GDPR.

Det finns för närvarande tämligen begränsat med vägledning för tolkning av artikel 22 GDPR. Det är enligt vår bedömning tveksamt om bestämmelsen är avsedd att omfatta behandling som sker för direktmarknadsföringsändamål, utom vid flagranta fall såsom vid stötande former av diskriminering. Direktmarknadsföringsaktiviteter kan i vår mening sällan anses vara sådana beslut som har ”*rättsföljd*” eller på liknande sätt ”*i betydande grad*” påverkar den registrerade. Av bestämmelserna i GDPR om automatiserat individuellt beslutsfattande (inbegripet profilering) samt den vägledning och de uttalanden som vi redogjort för ovan går dock att konstatera att det finns en rättspolitisk vilja att särskilt adressera problematiken med sådan ingripande behandling.

Avslutande kommentar

Reglerna i GDPR om personuppgiftsbehandling för direktmarknadsföring och profilering motsvarar i stor utsträckning de regler som gäller redan under PuL och Dataskyddsdirektivet. I GDPR adresseras och regleras, till skillnad från i Dataskyddsdirektivet, dock förekomsten av profilering som sådan uttryckligen. GDPR:s reglering i fråga om profilering har emellertid i princip begränsats till sådan profilering som sker inom ramen för automatiserat individuellt beslutsfattande enligt artikel 22 GDPR. Som nämnts ovan avser denna bestämmelse i första hand inte direktmarknadsföringsaktiviteter.

Det återstår att se hur GDPR kommer att tillämpas i förhållande till sådana avancerade metoder för personuppgiftsbehandling som dagens digitala och datadrivna marknadsföring bygger på. Såväl Artikel 29-gruppen som ICO kommer med all säkerhet lämna utförlig vägledning på området, som förhoppningsvis kan förtydliga synen på profilering i förhållande till GDPR:s bestämmelser.

98 *Consultative Committee of the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data, T-PD(2008)01,* se: www.coe.int/dataprotection.

6. Risk- och konsekvens-bedömning

Inledning

I detta avsnitt presenteras en modell för **dels** hur personuppgifts-ansvariga bör gå tillväga för att analysera de risker som kan aktualiseras vid en viss behandling av personuppgifter,[99] **dels** hur en konsekvens-bedömning enligt artikel 35 GDPR kan genomföras (eng. *Data Protection Impact Assessment*).

Som närmare redogörs för nedan anser vi att en personuppgifts-ansvarig först bör genomföra en s.k. riskanalys och därefter, om risk-analysen visar att det är sannolikt att behandlingen kommer att leda till en hög risk för fysiska personers rättigheter och friheter samt om inga undantag är tillämpliga, genomföra en konsekvensbedömning enligt artikel 35.1 GDPR.

Våra slutsatser och rekommendationer i detta avsnitt baseras till stor del på Artikel 29-gruppens *Guidelines on Data Protection Impact Assesment*, från den 4 april 2017.[100] Med hänsyn till Artikel 29-gruppens ställning och oberoende roll utgör dessa den centrala rättskällan på området. Ytterligare vägledning från bl.a. Datainspektionen kommer dock förhoppningsvis att meddelas innan GDPR börjar tillämpas och personuppgiftsansvariga bör noga följa rättsutvecklingen.[101] Sådan vägledning kan eventuellt även komma att påverka våra ställnings-taganden i detta avsnitt.

En bedömning i två steg

Artikel 35.1 GDPR anger följande:

”*Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.*”

99 Kravet på en sådan riskbedömning följer av bl.a. artikel 24-25 och artikel 32 GDPR. Detta påminner i hög grad om den ”risk- och sårbarhetsanalys” som en personuppgiftsansvarig är skyldig att göra enligt PuL. Se Datainspektionens informationsblad, *Molntjänster och personuppgiftslagen*, 2016, för mer information.

100 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.*

101 Se artikel 35.4 GDPR.

Innan en planerad behandling utförs ska den personuppgiftsansvarige således ta ställning till om en konsekvensbedömning avseende dataskydd är nödvändig eller inte. Vi menar att ett rationellt sätt att ta sig an såväl kravet på konsekvensbedömning enligt artikel 35 GDPR som en rad andra, liknande bedömningsfrågor i GDPR är att göra en bedömning i två steg.

I ett **första steg** bör den personuppgiftsansvarige bedöma hur sannolik och allvarlig en viss risk är utifrån behandlingens art, omfattning, sammanhang och ändamål.[102] Denna inledande riskbedömning och analys fyller som sagt flera syften och möter olika krav i GDPR, och är principiellt nödvändig att göra och dokumentera för varje planerad behandling av personuppgifter. Riskanalysen bör ytterst leda **dels** till en bedömning av vad som utgör ”lämpliga” säkerhetsåtgärder för den aktuella behandlingen, **dels** till att den personuppgiftsansvarige kan ta ställning till om behandlingen leder till en hög risk för fysiska personers rättigheter och friheter. Vi har valt att hädanefter kalla detta första steg för ”riskanalys”.

Om riskanalysen utvisar att det är sannolikt att den planerade behandlingen kommer att leda till en hög risk för fysiska personers rättigheter och friheter, ska den personuppgiftsansvarige i ett **andra steg** genomföra en bedömning av den planerade behandlingens konsekvenser enligt artikel 35 GDPR (nedan ”konsekvensbedömning”). En konsekvensbedömning ska särskilt övervägas vid användning av ny teknik, vid ny typ av behandling för vilken någon konsekvensbedömning inte tidigare har genomförts, eller om sådan är nödvändig pga. den tid som har förflutit sedan den ursprungliga behandlingen.[103]

Riskanalysen och den eventuellt efterföljande konsekvensbedömningen ska, som sagt, genomföras innan den planerade behandlingen utförs.[104] En personuppgiftsansvarig bör således redan när GDPR börjar tillämpas ha lämpliga rutiner och processer för att kunna göra den tvåstegsbedömning som beskrivs i detta avsnitt. Bedömningarna bör genomföras tidigt i planeringen av en behandling och bör påbörjas även om delar av den planerade behandlingen ännu är oklar eller osäker.[105] Detta gäller särskilt mot bakgrund av kraven på inbyggt dataskydd och dataskydd som standard (eng. *Privacy by Design* och *Privacy by Default*).

---

102 Artikel 35.1 och skäl 76 GDPR.

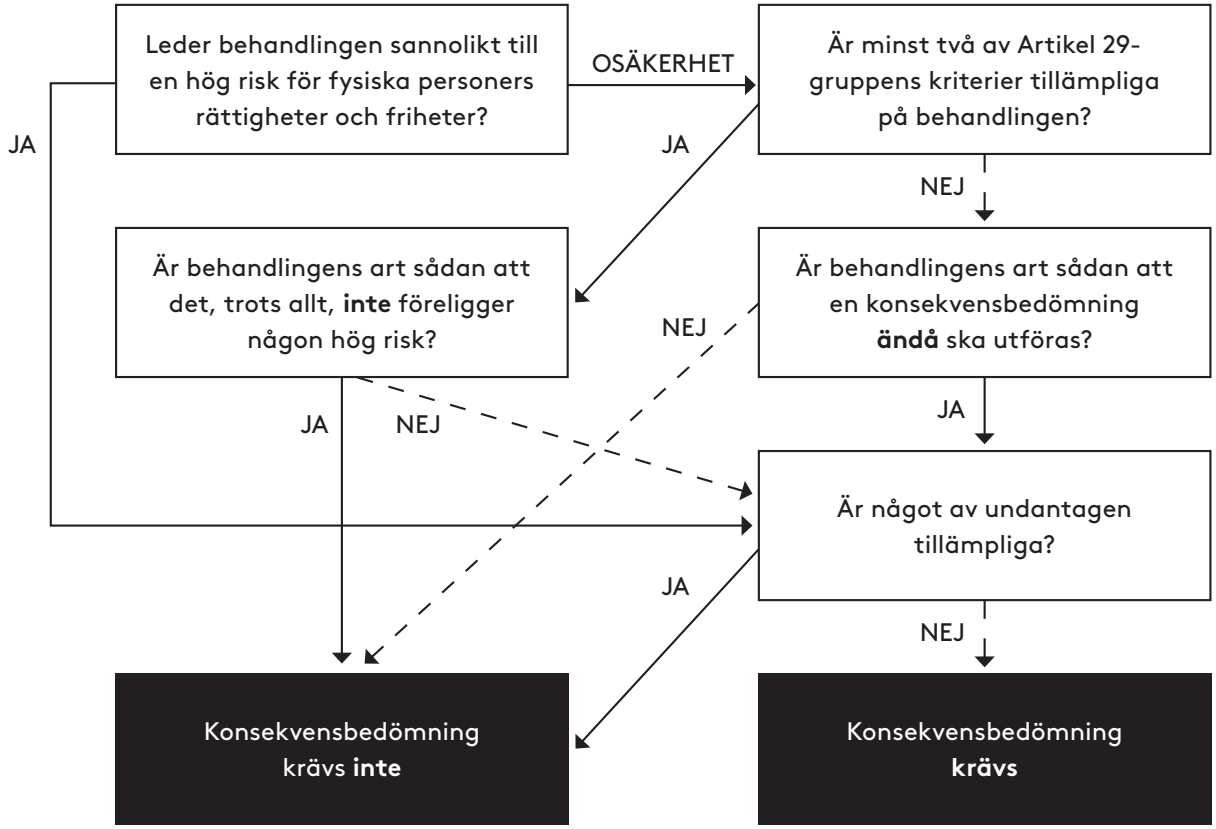
103 Skäl 89 GDPR.

104 Artikel 35.1 GDPR. Se även skäl 90 och 93 GDPR samt artikel 35.10 GDPR.

105 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 13.

Närmare om riskanalys (steg 1)

Nedanstående flödesschema sammanfattar de grundläggande principerna för en riskanalys avseende en planerad behandling av personuppgifter. Det bör noteras att vi i detta schema har fokuserat på riskanalysens betydelse för uppfyllnad av kravet på konsekvensbedömning enligt artikel 35 GDPR. Som ovan nämnts fyller den initiala riskanalysen flera olika syften, vilka alltså inte närmare redogörs för nedan.



LEDER BEHANDLINGEN SANNOLIKT TILL EN HÖG RISK FÖR FYSISKA PERSONERS RÄTTIGHETER OCH FRIHETER?

Artikel 35.3 GDPR innehåller en icke-uttömmande uppräkning då en konsekvensbedömning särskilt ska genomföras eftersom sådana behandlingar anses leda till en hög risk för fysiska personers rättigheter och friheter:

- Vid systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

- Vid behandling i stor omfattning av särskilda kategorier av personuppgifter eller av personuppgifter som rör fällande domar i brottmål och överträdelser.

- Vid systematisk övervakning av en allmän plats i stor omfattning.

Ytterligare vägledning om när en konsekvensbedömning krävs finns i Artikel 29-gruppens riktlinjer.[106] Mer vägledning och ytterligare bedömningskriterier är dessutom att vänta innan GDPR börjar tillämpas. Enligt artikel 35.4 ska Datainspektion nämligen ta fram och offentliggöra en förteckning över de slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd. Datainspektionen får enligt artikel 35.5 GDPR också ta fram en förteckning över behandlingsverksamhet som inte omfattas av kravet på konsekvensbedömning.

ARTIKEL 29-GRUPPENS "TVÅ-KRITERIE-REGEL"

Enligt Artikel 29-gruppen bör en konsekvensbedömning, som en tumregel, genomföras om den personuppgiftsansvarige bedömer att minst två av nedanstående tio kriterier är tillämpliga på behandlingen i fråga.[107]

1. Behandlingen innehåller **bedömningar eller värderingar** av den registrerade (inklusive profilering) särskilt när uppgifterna används för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar (skäl 71 och 91 GDPR). Exempel på detta är då en bank kontrollerar sina kunder mot en kreditreferensdatabas eller då företag skapar beteende- eller marknadsföringsprofiler baserat på besökarnas användning eller navigering på dess webbplats.

2. Behandlingen syftar till att fatta **automatiserade beslut** som har rättsliga följder för eller som på liknande sätt i betydande grad påverkar den registrerade (artikel 35.3 a GDPR), såsom när behandlingen kan leda till att vissa personer utesluts eller diskrimineras. Behandling som har obefintlig eller liten effekt på registrerade omfattas således inte.

3. Behandlingen innefattar **systematisk övervakning av registrerade**, vilket även omfattar systematisk övervakning av en allmän plats (artikel 35.3 c GDPR). Denna typ av övervakning är bland kriterierna eftersom personuppgifter kan samlas in under omständigheter där de registrerade möjligen inte är medvetna om vem som samlar in uppgifterna eller hur de ska användas, samtidigt som det kan vara omöjligt för de registrerade att undvika sådana allmänna utrymmen för att inte bli föremål för den typen av behandling.

---

106 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*.

107 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 7-10.

4. Behandlingen innefattar **känsliga personuppgifter**, vilket omfattar dels *särskilda kategorier av personuppgifter* (som definieras i artikel 9 GDPR, t.ex. uppgift om medlemskap i fackförening), dels personuppgifter som rör fällande domar i brottmål eller överträdelser. Därutöver omfattas även sådana personuppgifter som generellt kan anses medföra en ökad risk för individers rättigheter och friheter, såsom elektronisk kommunikation, lokaliseringsdata, betaluppgifter (som kan användas för bedrägerier). I detta fall är det dock relevant om uppgifterna har offentliggjorts av den registrerade eller tredje man då det kan påverka bedömningen av huruvida uppgifterna förväntades att behandlas för vissa ändamål. Slutligen kan även sådan information av privat karaktär vars offentliggörande, eller behandling för något annat syfte än just för enskildas privata användande, kan uppfattas som mycket påträngande omfattas (t.ex. molntjänster för personlig dokumenthantering, e-post och olika livsstilsapplikationer som kan innehålla mycket personlig information).

5. Behandlingen innebär att personuppgifter behandlas **i stor omfattning**. GDPR definierar inte vad som menas med behandling i stor omfattning. Artikel 29-gruppen menar, med utgångspunkt i skäl 91 GDPR, att följande ska beaktas vid bedömning av huruvida behandlingen sker i stor omfattning:
   - antalet registrerade som berörs,
   - volymen av uppgifter eller vidden av olika typer av personuppgifter,
   - behandlingens varaktighet/beständighet och
   - den geografiska omfattningen av personuppgiftsbehandlingen.

6. Behandlingen innebär **samkörning eller kombination** av olika register. Exempelvis om uppgifterna härstammar från två eller flera olika behandlingar som utförts för olika ändamål, och/eller av två olika personuppgiftsansvariga på ett sätt som inte skulle stämma överens med de registrerades rimliga förväntningar.

7. Behandlingen omfattar personuppgifter om **särskilt utsatta/sårbara eller skyddsvärda** typer av registrerade (skäl 75 GDPR). Behandling av denna typ av personuppgifter kan kräva konsekvensbedömning på grund av rubbad maktbalans mellan den registrerade och den personuppgiftsansvarige, vilket innebär att den registrerade inte kan samtycka till eller motsätta sig behandlingen. Exempelvis anställda som svårligen kan motsätta sig den behandling som utförs av arbetsgivaren när den är kopplad till personalhantering[108] eller barn som kan ha svårt att på ett medvetet/genomtänkt sätt motsätta sig eller samtycka till behandling. Därutöver omfattas även psykiskt sjuka, asylsökande, patienter eller äldre personer och andra situationer där en obalans i förhållandet mellan den registrerade och den personuppgiftsansvarige kan identifieras.

8. Behandlingen innebär att personuppgifterna **behandlas på ett innovativt sätt** vilket även omfattar behandling med ny teknik

108 Jfr Artikel 29-gruppen, *Opinion 2/2017 on data processing at work*, s. 6-7.

(t.ex. applikationer kopplade till "Internet of Things") eller behandlas **för att tillämpa tekniska eller organisatoriska lösningar**, såsom att kombinera användningen av fingeravtryck och ansiktsigenkänning för att åstadkomma en förbättrad behörighetskontroll (artikel 35.1 och skäl 89 samt 91 GDPR).

9. Behandlingen innebär att personuppgifter ska **föras över till ett land utanför EU/EES** med beaktande av destinationen för överföringen, möjligheten till ytterligare överföring eller sannolikheten av överföring (skäl 116 GDPR).

10. Behandlingen i sig förhindrar **de registrerade från att utöva en rättighet** (t.ex. behandling som utförs på en allmän plats som förbipasserade personer inte kan undvika) eller **från att använda en tjänst eller ett avtal** (såsom när en bank inhämtar uppgifter om sina kunder i en kreditreferensdatabas för att kunna avgöra om de ska erbjudas lån) (artikel 22 och skäl 91 GDPR).

Ju fler av kriterierna som är tillämpliga på den planerade behandlingen, desto mer sannolikt är det att behandlingen utgör en hög risk för de registrerades rättigheter och friheter. Om en personuppgiftsansvarig anser att behandlingen inte innebär en hög risk för registrerade, trots att minst två av ovan nämnda kriterierna är uppfyllda, måste skälen till varför en konsekvensbedömning inte genomförs dokumenteras. I vissa fall bör dock den personuppgiftsansvarige, beroende på behandlingens art och övriga omständigheter, genomföra en konsekvensbedömning trots att endast ett eller kanske t.o.m. inget av de ovanstående kriterierna är uppfyllda.[109] Vidare bör en personuppgiftsansvarig genomföra en konsekvensbedömning i de fall den ansvarige är osäker på om behandlingen sannolikt kan leda till hög risk eller inte. Viss försiktighet är därför påkallad vid tillämpning av Artikel 29-gruppens s.k. "två-kriterie-regel".

Exempel:[110]

1. Anta att den personuppgiftsansvarige planerar att ersätta sitt befintliga HR-system med ett nytt. HR-systemet innehåller samtliga anställdas personuppgifter, inklusive uppgifter om de anställdas hälsa och eventuellt medlemskap i en fackförening. Anställda räknas till kategorin särskilt utsatta/sårbara eller skyddsvärda typer av registrerade (se punkten 7 ovan) och uppgifterna om hälsa och medlemskap i fackförening utgör känsliga personuppgifter (se punkten 4 ovan). Den personuppgiftsansvarige bör i detta exempel således genomföra en konsekvensbedömning, då minst två kriterier är tillämpliga.

2. Anta att den personuppgiftsansvarige övervakar sina anställdas aktivitet och bl.a. bevakar deras arbetsstation samt vilka webbplatser de besöker. Anställda räknas till kategorin särskilt utsatta/sårbara eller skyddsvärda typer av registrerade (se punkten 7 ovan)

---

109 Jfr Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 9-10.

110 Jfr Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA),* s. 10.

och det är även fråga om systematisk övervakning (se punkten 3 ovan). Den personuppgiftsansvarige bör även i detta exempel således genomföra en konsekvensbedömning, då minst två kriterier är tillämpliga.

3. Anta att den personuppgiftsansvarige har en e-handelsbutik för sina kunder, där annonser med personliga erbjudanden för kunderna visas baserat på kundernas tidigare köpbeteende. I detta fall är det förvisso fråga om en typ av profilering av besökare (se punkten 1 ovan) men profileringen är varken systematisk eller omfattande (punkterna 3 och 5 ovan), varför en konsekvensbedömning inte ter sig nödvändig.

Slutsatsen av riskanalysen och de olika stegen som ledde till slutsatsen bör dokumenteras. Riskanalysen bör även dokumenteras i de fall som den personuppgiftsansvarige bedömer att den planerade behandlingen sannolikt **inte** leder till en hög risk. Enligt artikel 30 GDPR ska personuppgiftsansvarig föra ett register över behandlingar som utförts under dess ansvar. Dokumentering av att riskanalys har utförts och resultatet av sådan analys kan lämpligen ske i detta register.

UNDANTAG

GDPR innehåller tre uttryckliga undantag från skyldigheten att genomföra en konsekvensbedömning. Om något av de nedanstående undantagen är tillämpliga behöver inte den personuppgiftsansvarige genomföra en konsekvensbedömning:

- Behandlingens art, omfattning, sammanhang och ändamål är mycket lik en annan behandling för vilken **konsekvensbedömning redan har genomförts** av den personuppgiftsansvarige. I dessa fall kan resultatet från den första konsekvensbedömningen även användas för den andra behandlingen som medför liknande höga risker.[111]

- Om behandlingen är (i) nödvändig för att den personuppgiftsansvarige antingen ska kunna fullgöra en rättslig förpliktelse (enligt artikel 6.1 c) eller ska kunna utföra en uppgift av allmänt intresse (enligt artikel 6.1 e) och (ii) har rättslig grund i unionsrätten eller i en medlemsstats nationella rätt (som den personuppgiftsansvarige omfattas av) vari (iii) den aktuella specifika behandlingsåtgärden (eller serien av åtgärder) regleras och (iv) en **konsekvensbedömning redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund**, ska konsekvensbedömning inte genomföras. Detta gäller dock inte om medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.[112] Det är således upp till medlemsstaterna att inom ramen för nationell rätt reglera när undantaget ska gälla.

---

111 Artikel 35.1 GDPR enligt vilken *"En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker"*

112 Artikel 35.10 GDPR.

- Behandlingen finns **uppräknad i den förteckning som Datainspektionen får upprätta och offentliggöra**, över de slags behandlingsverksamheter för vilka det inte kommer att krävas att en konsekvensbedömning genomförs.[113]

Närmare om konsekvensbedömningen (steg 2)

Om den personuppgiftsansvarige vid riskanalys enligt ovan bedömer att behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, såvida inget av undantagen är tillämpliga, genomföra en konsekvensbedömning. En konsekvensbedömning kan omfatta en behandling eller en serie liknande behandlingar som medför liknande höga risker.[114]

Syftet med konsekvensbedömningen är att avgöra riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska risken, säkerställa personuppgiftskyddet och visa att GDPR efterföljs.[115]

I artikel 35.7 GDPR anges att en konsekvensbedömning *åtminstone* ska innehålla:

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt den personuppgiftsansvariges berättigade intresse,
b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
c) en bedömning av riskerna för de registrerades rättigheter och friheter, och
d) de åtgärder som planeras för att hantera riskerna, för att säkerställa skyddet av personuppgifterna och för att visa att GDPR efterlevs.

Enligt Artikel 29-gruppen bör även nedanstående kriterier beaktas och de kan användas som en checklista vid bedömningen av huruvida en konsekvensbedömning eller en metod för att utföra en konsekvensbedömning är tillräckligt omfattande för att efterfölja GDPR:[116]

113 Artikel 35.5 GDPR. Se närmare Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 11.

114 Artikel 35.1 GDPR.

115 Skäl 90 GDPR.

116 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 21.

1. En systematisk beskrivning av behandlingen har tillhandahållits genom: (artikel 35.7 a GDPR)

- att beakta behandlingens art, omfattning, sammanhang och ändamål (skäl 90 GDPR),
- att registerföra vilka kategorier av personuppgifter det är fråga om, vilka mottagare personuppgifterna lämnas ut till samt den period för vilken personuppgifterna ska lagras,
- att tillhandahålla en funktionell beskrivning av behandlingen,
- att identifiera de tillgångar som behandling av personuppgifter är beroende av (t.ex. hårdvara, programvara, nätverk eller särskilda personer), samt
- att beakta efterlevnad av godkända uppförandekoder (artikel 35.8 GDPR).

2. En bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till ändamålen har gjorts genom att: (artikel 35.7 b GDPR)

- Fastställa de planerade åtgärder som ska vidtas för att uppfylla kraven i GDPR (artikel 35.7 d GDPR). Detta ska göras med beaktande av:
  - Åtgärder som bidrar till proportionaliteten och nödvändigheten av behandlingen, på grundval av:
    - särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b GDPR),
    - behandlingens laglighet (artikel 6 GDPR),
    - adekvata, relevanta personuppgifter som är begränsade till vad som är nödvändigt (artikel 5.1 c GDPR), samt
    - begränsad lagringstid (artikel 5.1 e GDPR).

  - Åtgärder som bidrar till att de registrerades rättigheter tillgodoses, såsom:
    - information till den registrerade (artikel 12, 13 och 14 GDPR),
    - rätt till tillgång och dataportabilitet (artikel 15 respektive 20 GDPR),
    - rätt till rättelse, radering, begränsning av behandling och rätten att göra invändningar (artikel 16–19 och 21 GDPR),
    - mottagare av personuppgifterna,
    - personuppgiftsbiträden (artikel 28 GDPR),
    - skyddsåtgärder vid överföringar till tredje land[117] (artikel 44–50 GDPR), samt
    - förhandssamråd med Datainspektionen (artikel 36 GDPR).

3. En bedömning av riskerna för de registrerades rättigheter och friheter har gjorts genom att: (artikel 35.7 c GDPR)

- Uppskatta varje risks ursprung, art, särdrag och allvar (se skäl 84 GDPR) ur de registrerades perspektiv (inbegripet obehörig åtkomst, oönskad ändring och förlust av data), genom att:
  - beakta upphovet till risken (skäl 90 GDPR),
  - identifiera eventuella konsekvenser för de registrerades rättigheter och friheter som kan uppstå vid obehörig åtkomst, oönskad ändring och förlust av data,
  - identifiera hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av data, samt
  - bedöma varje risks sannolikhetsgrad och allvar (skäl 90 GDPR).
- Fastställa de åtgärder som planeras för att hantera riskerna (inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna) (artikel 35.7 d och skäl 90 GDPR).

4. Involvera de parter som berörs av behandlingen genom att: (artikel 35.2 och 35.9 GDPR)

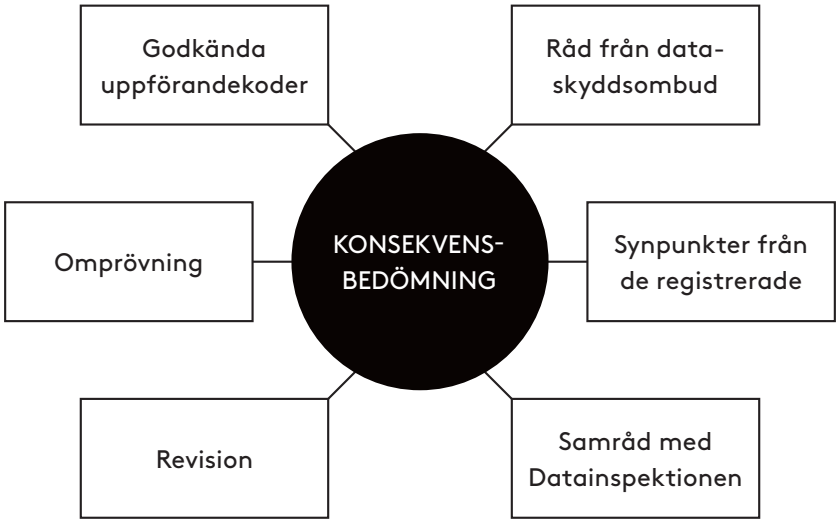
- Rådfråga eventuella dataskyddsombud (artikel 35.2 GDPR), och
- Inhämta synpunkter från de registrerade eller deras företrädare (artikel 35.9 GDPR).

117 Med tredje land menas ett land utanför EU/EES.

Ytterligare vägledning om konsekvensbedömningen finns i av olika tillsynsmyndigheter publicerade riktlinjer.[118]

SÄRSKILT OM GENOMFÖRANDET AV KONSEKVENSBEDÖMNINGEN

Vid genomförandet av konsekvensbedömning ska den personuppgiftsansvarige särskilt iaktta följande (se vidare nedan):



GODKÄNDA UPPFÖRANDEKODER

I GDPR uppmuntras att sammanslutningar eller andra organ som företräder kategorier av personuppgiftsansvariga, eller personuppgiftsbiträden, upprättar särskilda uppförandekoder för att tillgodose särdragen hos den behandling som sker inom specifika sektorer. Sådana uppförandekoder ska godkännas av Datainspektionen.[119]

Den personuppgiftsansvariges efterlevnad av godkända uppförandekoder ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av den personuppgiftsansvarige, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.[120] Detta förutsätter givetvis att uppförandekoden är anpassad och lämplig för den aktuella behandlingen.[121]

Såvitt känt har i dagsläget inte några uppförandekoder upprättats eller godkänts.

---

118 Se t.ex. ICO, *Conducting privacy impact assessments code of practice*, 2014. Se även CNIL, *Privacy Impact Assessment (PIA)*, 2015.

119 Artikel 40.2 och 40.5 GDPR.

120 Artikel 35.8 GDPR.

121 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 15.

RÅD FRÅN DATASKYDDSOMBUD

Personuppgiftsansvarig som har utsett ett dataskyddsombud ska rådfråga sådant ombud vid genomförandet av konsekvensbedömningen.[122] Dataskyddsombudets råd och de beslut som tas ska dokumenteras i konsekvensbedömningen.[123]

Dataskyddsombud ska även övervaka genomförandet av konsekvensbedömningen[124] och bör bl.a. ge den personuppgiftsansvarige råd om huruvida en konsekvensbedömning är nödvändig eller inte, vilken metod som ska användas vid genomförandet, vilka skyddsåtgärder som bör tillämpas för att mildra eventuella risker för de registrerade, om bedömningen har genomförts på ett korrekt sätt samt om slutsatserna överensstämmer med kraven i GDPR. Om den personuppgiftsansvarige inte beaktar dataskyddsombudets råd ska den personuppgiftsansvarige dokumentera skälen för sitt beslut.[125]

SYNPUNKTER FRÅN DE REGISTRERADE

Den personuppgiftsansvarige ska när det är lämpligt inhämta synpunkter från de registrerade rörande den avsedda behandlingen.[126] Sådana synpunkter kan inhämtas på olika sätt, beroende på sammanhanget. Exempelvis kan så ske vid undersökning av den planerade behandlingens ändamål och medel. Vidare kan i vissa fall frågor ställas till företrädare för t.ex. anställda, fackföreningar eller framtida kunder.[127]

För det fall den personuppgiftsansvarige behandlar personuppgifter på ett sätt som avviker från de registrerades synpunkter, bör den personuppgiftsansvarige dokumentera skälen för sitt beslut. Så är även fallet om den personuppgiftsansvarige avstår från att inhämta de registrerades synpunkter, i de fall det inte ansetts lämpligt.[128]

SAMRÅD MED DATAINSPEKTIONEN

I de fall som konsekvensbedömningen visar att den planerade behandlingen skulle leda till en hög risk om inte åtgärder vidtas för att minska risken, ska den personuppgiftsansvarige samråda med Datainspektionen före behandlingen.[129] Av Artikel 29-gruppens yttrande framgår att den personuppgiftsansvarige måste samråda med Datainspektionen om de identifierade riskerna inte i tillräckligt stor utsträckning kan hanteras av den personuppgiftsansvarige. Exempel

122 Artikel 35.2 GDPR.

123 Artikel 29-gruppen, *Guidelines on Data Protection Officer ('DPO's')*, s. 13.

124 Artikel 39.1 c GDPR.

125 Artikel 29-gruppen, *Guidelines on Data Protection Officer ('DPO's')*, s. 17.

126 Artikel 35.9 GDPR.

127 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 13.

128 Ibid.

129 Artikel 36.1 GDPR.

på sådana oacceptabelt höga risker är om de registrerade kan uppleva betydande, eller kanske t.o.m. bestående, men till följd av behandlingen eller i de fall som det ter sig uppenbart att de befarade riskerna med behandlingen kommer att inträffa.[130] Samrådet ska äga rum innan behandlingen utförs.

Datainspektionen ska inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige (och i tillämpliga fall personuppgiftsbiträdet) skriftliga råd. Denna period får förlängas med ytterligare sex veckor beroende på hur komplicerad den planerade behandlingen är. Därutöver får dessa perioder tillfälligt upphöra att löpa i avvaktan på att Datainspektionen erhåller den information som den har begärt med tanke på samrådet.[131] Organisationer bör följaktligen, i planeringen av sina projekt, ta höjd för handläggningstiden och föregående riskanalys och konsekvensbedömning.

För det fall Datainspektionen anser att den planerade behandlingen skulle strida mot GDPR kan Datainspektion komma att använda sina befogenheter enligt artikel 58 GDPR.[132] Det innebär att Datainspektionen bl.a. kan begära tillgång till all nödvändig information, utfärda varningar och förelägga den personuppgiftsansvarige om rättelse eller radering.

Vid samråd med Datainspektionen ska den personuppgiftsansvarige lämna viss information om den avsedda behandlingen och den genomförda konsekvensbedömningen.[133] Om den personuppgiftsansvarige inte har utfört en konsekvensbedömning eller inte har samrått med Datainspektionen när så borde ha skett, kan detta leda till att administrativ sanktionsavgift utdöms mot den personuppgiftsansvarige.[134]

Det kan även tillkomma tvingande bestämmelser i svensk rätt som medför en skyldighet för personuppgiftsansvariga som behandlar personuppgifter att vid utförandet av en uppgift av allmänt intresse (inbegripet behandling avseende social trygghet och folkhälsa) samråda med och erhålla förhandstillstånd av Datainspektionen.[135] Den svenska utredningen som tillsatts för att föreslå en ny nationell reglering som kompletterar GDPR har bedömt att sådana bestämmelser, i de fall de bedöms nödvändiga, ska regleras i sektorspecifik lag.[136]

---

130 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 18.

131 Artikel 36.2 GDPR.

132 Ibid.

133 Artikel 36.3 GDPR.

134 Artikel 83.4 a GDPR.

135 Artikel 36.5 GDPR.

136 SOU 2017:39, s. 244.

REVISION

Den personuppgiftsansvarige ska vid behov utföra en översyn i syfte att bedöma om aktuell behandling genomförs i enlighet med konsekvensbedömningen, åtminstone när den risk som behandlingen medför förändras.[137] Risken för behandling kan förändras vid en förändring av någon av komponenterna i behandlingen (t.ex. personuppgifter, riskkällor, tänkbara konsekvenser och hot) eller till följd av att behandlingens sammanhang ändras (t.ex. ändamål, funktion, m.m.).[138]

System i vilka personuppgifter behandlas kan snabbt ändras och utvecklas, vilket kan innebära att nya sårbarheter uppkommer. Den personuppgiftsansvariges revision av konsekvensbedömningen är således inte endast viktigt för att löpande förbättra systemen i fråga utan även för att på lång sikt upprätthålla nivån av dataskydd i dessa ständigt föränderliga miljöer.[139]

OMPRÖVNING

Enligt Artikel 29-gruppen bör konsekvensbedömningen som utgångspunkt lämpligen omprövas vart tredje år. Beroende på behandlingens art, förändringar i behandlingen och andra omständigheter som påverkar behandlingen kan omprövningen behöva ske oftare än så.[140]

BEHANDLINGAR SOM PÅBÖRJATS FÖRE GDPR:S IKRAFTTRÄDANDE

Kravet på konsekvensbedömning enligt artikel 35 GDPR gäller endast sådana behandlingar som inleds efter det att GDPR har börjat tillämpas.[141] Artikel 29-gruppens rekommendation är dock att konsekvensbedömning även genomförs i förhållande till behandlingar som påbörjats innan GDPR har börjat tillämpas. Även kravet på löpande revision medför att konsekvensbedömning ska genomföras i de fall en betydande förändring av den aktuella behandlingen har skett efter den 25 maj 2018. Sådan förändring kan t.ex. bestå i att ny teknik används eller att ändamålen med behandlingen ändras.[142]

Avslutande kommentarer

Den tvåstegsmodell som presenterats ovan är ett sätt att praktiskt hantera GDPR:s krav på analys och bedömning avseende risker på behandlingsnivå. Det är dock ingen tvekan om att GDPR:s krav och regelverk i denna del är både relativt komplext och delvis motsägelsefullt.

---

137 Artikel 35.11 GDPR.

138 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 12.

139 Ibid.

140 Ibid.

141 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 11.

142 Artikel 29-gruppen, *Guidelines on Data Protection Impact Assessment (DPIA)*, s. 11-12.

Ovanstående innebär att Datainspektionens kommande vägledningar tveklöst kommer att tillmätas stor betydelse, liksom eventuella framtida uppförandekoder. Vi tror dock, utifrån nu tillgänglig information, att den presenterade modellen väl möter de krav som GDPR uppställer och dessutom bygger på en metodik som relativt enkelt kan implementeras i praktiken. Ett hållbart arbete med dataskyddsfrågor förutsätter att de arbetsrutiner och processer som skapas klarar att både omhänderta GDPR:s krav och samtidigt innehåller mekanismer för att genomföra en mera djuplodande analys vid behov.

Vi vill också avslutningsvis understryka vikten av att riskanalysen utförs tidigt i planeringen av en behandling. Detta är en förutsättning både för att kunna beakta principerna om inbyggt dataskydd och dataskydd som standard[143] och för att hinna göra en kompletterande konsekvensbedömning i de fall detta är nödvändigt. Oavsett hur en personuppgiftsansvarig väljer att möta kraven i artikel 35 GDPR bör denne tillse att rutiner för genomförande av riskanalyser och konsekvensbedömningar finns på plats senast när GDPR ska börja tillämpas.

143 Artikel 25 GDPR.

7. Avslutande kommentarer

GDPR är en oerhört omfattande lagstiftningsprodukt. Den är tillämplig för i princip alla verksamheter och innehåller en till synes outsinlig källa till komplexa juridiska, tekniska och organisatoriska frågeställningar. Från juridiskt perspektiv aktualiseras en mängd olika rättsområden såsom arbetsrätt, offentlig rätt, EU-rätt, förvaltningsrätt samt avtalsrätt (och annan civilrätt). För att förstå och kunna ge råd om regelverket krävs, utöver juridiska kunskaper, både teknisk förståelse och erfarenhet av att arbeta med frågor rörande organisations- och verksamhetsutveckling. Vi har i denna rapport valt ut några frågeställningar som vi funnit intressanta i vår rådgivning och som vi vet att många organisationer just nu brottas med i sitt anpassningsarbete till GDPR.

I skrivande stund finns ett stort behov av fler utlåtanden från Artikel 29-gruppen, vägledning från Datainspektionen och ytterligare statliga utredningar angående svensk rätts anpassning till GDPR. Sådan information och vägledning kommer förhoppningsvis att ge värdefulla insikter. Därutöver finns det flera uppenbara oklarheter i lagtexten som kommer att kräva ställningstaganden och klargöranden från EU-domstolen.

Vi tror det är nödvändigt att ha en förnuftig, pragmatisk och riskorienterad syn på GDPR och dataskydd. Vi ser exempelvis många företag som nu investerar stora summor i nya tekniska lösningar för att automatisera delar av de förändringar som GDPR medför, t.ex. verktyg för uppfyllande av de registrerades rättigheter. I många fall står dock investeringen, enligt vår uppfattning, inte i rimlig proportion till den fördel som uppnås. Det finns inget hinder i GDPR mot att uppfylla regelverket med hjälp av manuella åtgärder, och många av de viktigaste bedömningarna och ställningstaganden som krävs (t.ex. riskanalys, bedömning av laglig grund, specificering av ändamål och tydlig informationsgivning) kommer alltid att kräva en bedömning i det enskilda fallet av en dataskyddskunnig person. Vi tror att en ännu viktigare aspekt av GDPR är att regelverket ofta kräver en kulturförändring i organisationen. Första steget i en sådan kulturförändring är ökad medvetenhet och kunskap hos den egna personalen. Därför tror vi att en ordentlig investering i utbildning av anställda, förändring/anpassning av arbetsprocesser, ökad transparens och förbättrade rutiner för dokumentation i många fall vore betydligt mer värdefullt än nya tekniska lösningar.

Vi vill avslutningsvis understryka en ofta uttalad sanning: de organisationer som arbetat seriöst med dataskydd under PuL kan känna sig relativt trygga även när GDPR börjar tillämpas. Skillnaderna mot PuL är, för många verksamheter, av mindre ingripande karaktär och kan hanteras genom relativt enkla åtgärder. Efterlevnad av GDPR uppnås inte heller genom ett kartläggnings- eller anpassningsprojekt utan

istället genom dokumentation, kunskap och en verksamhetsanpassad och långsiktig organisation för dataskyddsfrågor.

Det riktiga dataskyddsarbetet upphör alltså inte den 25 maj 2018, det är då det börjar. Vi ser fram emot att hänga med på resan!

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mer information.

Författarna till denna rapport är:

Daniel Lundqvist, advokat och partner.

Fredrik Gustafsson, advokat.

Emily Tomas da Costa, biträdande jurist.

Hanna Bogsjö Österberg, biträdande jurist.

Emma Jarkell, biträdande jurist.

Tahmina Sahibli, biträdande jurist.

www.kahnpedersen.se

ISBN 978-91-983215-3-1