Rapport

Version 1.0
2018-10-24 Dnr/ref.

Slutredovisning av GDPR-nätverkets arbetsutskott ”Tillförlitliga biträden”

Inledning

Vid anlitande av personuppgiftsbiträden (PUB) ställer dataskyddsförordningen krav på att den personuppgiftsansvarige (PUA) endast anlitar sådana PUB som ger ”tillräckliga garantier” för att behandlingen uppfyller kraven i förordningen. Detta regleras i artikel 28.1, men också i skäl 81, där det anges att PUA endast ska använda PUB som ger *tillräckliga garantier för att genomföra tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning*. Inför anlitande av ett PUB uppkommer frågan hur sådana garantier kan lämnas och visas av PUB. Motsvarande krav vid anlitande av PUB ställs i brottsdatalagen (2018:1177).[1]

Vilka skyldigheter har PUB enligt förordningen?

För att kunna säkerställa att tillräckliga garantier lämnas måste man först klarlägga vilka krav som ställs på PUB enligt förordningen. De uttryckliga krav och skyldigheter för PUB som arbetsutskottet har identifierat i huvudsak i förordningen framgår enligt följande:

- Får endast anlita underbiträden med särskilt tillstånd från PUA alternativt underrätta PUA om nya eller byten av underbiträden om ett generellt förhandstillstånd till detta har lämnats. (art. 28.2, 28.3 d)
- Följa PUAs instruktioner (art. 28.3 a)
- Iaktta tystnadsplikt (art 28.3 b)
- Biträda PUA med att utföra vissa skyldigheter, t.ex. konsekvensbedömning, tillgång till uppgifter, spårbarhet på utlämnade uppgifter till 3:e part m.m. (art. 28.3 c, e-f)
- Återlämna eller radera uppgifter (art. 28.3 g)
- Ge PUA tillgång till information och möjliggöra granskningar, inbegripet inspektioner m.m. för kontroll av PUBs efterlevnad av skyldigheterna (art. 28.3 h)
- Informera den PUA om lämnade instruktioner strider mot dataskyddsbestämmelserna (art. 28.3 2 st.)
- Ålägga samma skyldigheter på eventuella underbiträden, kontrollera dessa samt vara fullt ut ansvariga gentemot PUA för underbiträdets behandlingar (art. 28.4)
- Föra skriftliga register över behandlingar som utförs åt PUA (art. 30.2)
- Säkerställa en adekvat säkerhetsnivå i förhållande till den behandling som utförs (art. 32)
- Underrätta PUA om inträffade personuppgiftsincidenter utan onödigt dröjsmål (art. 33.2)
- I vissa fall utse dataskyddsombud (37.1 a)

[1] 3 kap. 16 § första stycket andra meningen brottsdatalagen: ”Innan ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

- Skadeståndsskyldighet gentemot registrerade, begränsat till brott mot lagenliga instruktioner från PUA och i förordningen uttryckliga skyldigheter för PUB (art. 82)

I brottsdatalagen och brottsdataförordningen (2018:1202) finns motsvarande skyldigheter för PUB som i dataskyddsförordningen.

Av skyldigheterna ska enligt förordningen vissa av dessa särskilt regleras i ett avtal eller annan bindande rättsakt mellan PUA och PUB, ett s.k. PUB-avtal. Dessa skyldigheter framgår av art. 28.3 a-h. Detta utesluter givetvis inte att övriga skyldigheter med anledning av biträdesförhållandet kan regleras, såsom hantering av underbiträden och skadestånd och regress mellan parterna m.m.

Vad anger förordningen om ”tillräckliga garantier”?

Artikel 28.1 anger att PUB ska garantera att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och att den registrerades rättigheter skyddas. Av skäl 81 anges närmare att dessa garantier i synnerhet ska avse (1) sakkunskap, (2) tillförlitlighet och (3) resurser för att genomföra de nämnda åtgärderna, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter.

Av brottsdatalagen framgår endast att innan ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter (3 kap. 16 §). Dataskyddsförordningen ger således mer vägledning om vad en sådan ”försäkran” innebär.

När det gäller säkerheten i samband med behandlingar anger förordningen i art. 32.1 att säkerhetsåtgärderna ska vara anpassade med beaktande av bl.a. behandlingens omfattning och art, riskerna med behandlingen och genomförandekostnader m.m. De förslag och exempel på krav och hur dessa kan visas som anges nedan måste således ställas i relation till vad det är för behandling som ska utföras av PUB. PUA måste därför ytterst avgöra vilka krav som är rimliga i förhållande till den behandling som ska utföras av PUB.

Vad innebär ”tillräckliga garantier” i praktiken?

När en PUA ska anlita ett PUB måste således garantierna kunna visas på något sätt. I de flesta fall kommer det troligen att röra sig om någon form av offentlig upphandling, varför kravställningen från upphandlande myndighet måste utformas så att anbudsgivarnas svar kan påvisa att garantierna kan uppfyllas med konkret innehåll. För att kunna göra detta måste PUA veta vad garantierna i praktiken ska avse. Upphandlingsrättsligt torde det primärt röra sig om kvalificeringskrav hos anbudsgivare enligt 14 kap. lagen (2016:1145) om offentlig upphandling (LOU). I de fall de upphandlingsrättsliga reglerna ska tillämpas måste de grundprinciper som gäller för dessa också beaktas vid kravställningen. Det innebär bl.a. att kraven måste vara proportionerliga i förhållande till det som ska upphandlas och hur branschen man vänder sig till ser ut. Frågan om hur många av de potentiella anbudsgivarna som rent faktiskt kan uppfylla de specifika kraven måste ställas och man bör därför tänka på när

i tiden ett visst krav rimligen ska vara uppfyllt. Att ställa ett visst specifikt krav som gäller alla anbudsgivare skulle t.ex. kunna anses som oproportionerligt enligt LOU. Att däremot ställa krav på att vinnande anbudsgivare t.ex. ska inneha en viss certifiering senast inom ett bestämt antal månader efter att kontraktet tecknats kan kanske anses mer proportionerligt i förhållande till det som ska upphandlas.

Arbetsutskottet har utgått från förordningens skäl 81 och punkterna rörande sakkunskap, tillförlitlighet och resurser för att närmare precisera exempel på krav som kan ställas på ett PUB. Dessa exempel kan givetvis läggas till grund för upphandling av PUB inom brottsutredande verksamhet, om det är aktuellt.

Sakkunskap ("expert knowledge" i engelsk översättning)

För att PUB ska kunna visa att det har sakkunskap om dataskydd och de specifika krav som kan ställas i förhållande till den behandling som ska utföras, bör PUB:s expertkunskap komma till uttryck på lämpligt sätt. Ett exempel kan vara att ställa krav på att det ska finnas ett dataskyddsombud hos företaget. Förordningen ställer i sig särskilda krav på ombudets kompetens, men det viktiga är att ombudet *de facto* innehar kompetensen. Vanligtvis vid upphandlingar visas specifika personers kompetens genom CV, referenser eller certifieringar m.m. Det är också viktigt att ombudets roll är utformad som avsetts enligt förordningen och därmed också har möjlighet att arbeta som ett sådant, dvs. ytterst en organisationsfråga.

Enligt förordningen är inte alla PUB skyldiga att utse dataskyddsombud (art. 37), men även om någon uttrycklig skyldighet inte finns för det aktuella PUB torde detta inte utgöra något hinder för att PUB ändå utsett ett ombud. Finns inte något uttryckligt krav på ett dataskyddsombud[2] torde ett PUB kunna visa på sakkunskap på liknande sätt hos särskilt utpekade nyckelpersoner med särskild kompetens inom dataskyddsfrågor. Det kan också vara viktigt att organisationen i sig är uppbyggd på ett sådant sätt att det finns funktioner, arbetssätt eller liknande som tillvaratar dataskyddsfrågor och efterlevnad av andra regler. Risken med att t.ex. endast en person innehar kunskapen är att det blir allt för personberoende. Externa experter knutna till det aktuella uppdraget kan möjligen också tänkas som en komplettering till den sakkunskap som finns inom företaget (åberopande av annans kapacitet).

Tillförlitlighet

PUB:s tillförlitlighet kan delvis ses som summan av dess sakkunskap och resurser. Förekomsten av t.ex. kvalitetsledningssystem, dataskyddspolicy, rutiner för hantering av personuppgiftsincidenter och kontinuitetsplanering torde påvisa att företaget arbetar systematisk med dataskyddsfrågor och därmed anses tillförlitlig. Sådana policys och arbetssätt kan i många avseenden följa erkända internationella eller nationella standarder, t.ex. ISO-standarder. Som exempel inom informationssäkerheten kan nämnas ISO/IEC 27001/27002 - Ledningssystem för informationssäkerhet och ITIL (principer för att hantera IT-infrastrukturen både vad gäller flexibilitet, säkerhet, människor och arbetssätt). Vidare inom specifika områden kan nämnas ISO/IEC 29151 (säkerhetsåtgärder avseende Annex A i ISO/IEC 27001), ISO/IEC 27005 och ISO/IEC 29134 (riskanalyser och riskhantering) samt ISO/IEC 27018 (skydd för personuppgifter i molntjänster). Organisationer kan certifiera sig mot dessa standarder

[2] Eftersom det endast är under vissa förutsättningar som ett PUB måste ha ett dataskyddsombud, måste ett sådant krav i en upphandling vara i enlighet med reglerna och principerna som gäller vid offentlig upphandling, bl.a. proportionalitetsprincipen.

och därmed enkelt visas följsamhet till olika delar av dataskyddsförordningens regelverk.

I avsaknad av formella certifieringar bör tydliga redogörelser kunna vara tillräckligt för att ge en bild av hur företaget hanterar dataskyddsfrågor. Även företagets tidigare erfarenheter av liknande åtaganden/uppdrag bör kunna påvisa någon form av tillförlitlighet, vid tillfredsställande referenser.

Resurser

Beträffande resurser kan dessa delas upp i tekniska resurser, personal- och organisationsresurser samt ekonomiska resurser. Tekniska resurser torde främst ta sikte på förmågan hos PUB att uppfylla de tekniska säkerhetskrav och övriga lösningar som PUA bedömer vara nödvändiga för den aktuella behandlingen. Vilka typer av säkerhetskrav som kan komma ifråga anges bl.a. i art. 32 och det är som nämnts ovan PUA:s ansvar att göra en bedömning av exakt vilka krav som ska ställas utifrån riskerna med behandlingen (art. 32.1).

Resurser avseende personal och organisation har berörts ovan under ”sakkunskap” och ”tillförlitlighet”. Vid sidan av sådan specifik expertkunskap såsom det beskrivs ovan kan dock andra personalresurser i vissa fall vara nödvändiga för att behandlingen ska kunna fullgöras. Vid väldigt höga säkerhetskrav kan det t.ex. vara nödvändigt med väktarbevakning (t.ex. av serverhall eller liknande) och i andra situationer kanske en viss kundtjänstbemanning krävs för att upprätthålla en viss servicenivå kopplat till den personuppgiftsbehandling som utförs av PUB. I LOU benämns krav på tekniska resurser respektive personal- och organisationsresurser som ”teknisk och yrkesmässig kapacitet”, 14 kap. 1 §.

Krav på ekonomiska resurser benämns i LOU som krav på ”ekonomisk och finansiell ställning”. Sådana krav får enligt 14 kap. 3 § avse en viss minsta omsättning, en viss kvot mellan tillgångar och skulder eller en lämplig ansvarsförsäkring. Kraven bör i en biträdessituation – utöver ”ordinarie” ekonomiska krav som vanligtvis ställs för att en anbudsgivare ska ha förmåga att fullgöra hela kontraktsperioden – särskilt ta höjd för de särskilda sanktioner och skadeståndskrav som kan bli följden för PUA om PUB brister i fullgörandet av avtalet.

Sammanfattning

Sammanfattningsvis ställs det tydligare krav i förordningen, men inte nödvändigtvis högre krav, på PUA:s och PUB:s ansvar att skydda personuppgifter och säkerställa att registrerades fri- och rättigheter inte kränks. Det är emellertid bara PUA som formellt bär ansvaret att kunna ”visa” ansvarsskyldighet, dvs. kunna visa att dataskyddsregelverket följs. Det följer indirekt av dessa krav vid anlitande av PUB en motsvarande skyldighet att kunna visa följsamhet på olika sätt, såsom anges i skäl 81. PUA måste således i sin roll som ansvarig för dataskyddet analysera skyddsvärde och adekvata tekniska och organisatoriska skyddsåtgärder för de behandlingar av personuppgifter som ska outsourcas och ge uttryck för dem i upphandlingsunderlaget.

Att i detalj ange vilka krav som ska ställas på ett PUB går inte att fastställa generellt. Som påpekats ovan ska PUA göra en bedömning av vilka krav som är relevanta med beaktande av bl.a. behandlingens omfattning och art, riskerna med behandlingen och genomförandekostnader m.m. PUA måste därför, i större utsträckning än tidigare,

analysera vilka krav utifrån ett dataskyddsperspektiv som bör ställas vid varje enskilt tillfälle då en viss behandling av personuppgifter ska överlämnas till ett PUB.

Ett krav som alltid bör kunna ställas på PUB är kompetens och kännedom rörande dataskyddsregelverket. Men även här får omfattningen av kravet anpassas utifrån behandlingens omfattning och art m.m.. Hur de krav som PUA väljer att ställa ska bevisas och uppfyllas av PUB, får göras på samma sätt som andra, liknande krav som ställs i upphandlingar

Efter upphandling och tecknande av avtal måste PUA aktivt följa upp de garantier som PUB lämnat. Dataskyddsförordningen tillhandahåller ”verktyg” för sådan uppföljning, bl.a. stipuleras en rätt för PUA att inspektera PUB:s verksamhet.

Med denna rapport anser vi att arbetsutskottet har uppfyllt sitt uppdrag. Utskottet avslutas därför i och med detta. Arbetsutskottet har bestått av Manólis Nymark, Inera AB, och Henrik Wallman, Pensionsmyndigheten.