Göteborgs Stad

Delårsrapport för dataskyddsarbetet

Gryaab

2021-05-26

Innehåll

1 Årets arbete hittills

1.1 Dataskyddsarbetet hittills

I januari 2021 översändes en kontrollplan till förvaltningen med information om hur dataskyddsombudet planerat att arbeta både enskilt och tillsammans med organisationen för att föra dataskyddsarbetet framåt.

Dataskyddsombudet ska ge råd till den personuppgiftsansvarige. Under den gångna tiden har dataskyddsombudet fått frågor om bl.a. hanteringen av personuppgifter i nya behandlingar och frågor om personuppgiftsincidenter. Dataskyddsombudet har även haft regelbunden kontakt och möten med dataskyddsgruppen som består av tre personer inom Gryaabs organisation. Utifrån de rekommendationer som lämnades på den senaste granskningen avseende personuppgiftsincidenter har dataskyddsgruppen vidtagit åtgärder i form av dokument för riskbedömning, dokumentation över hur dokumentationen ska gå till i ENIA samt mall för information som ska ges till de registrerade för att minimikraven i förordningen ska följas. Åtgärderna har stämts av med dataskyddsombudet som ser mycket positivt på att åtgärderna redan är klara och implementerade i verksamheten.

Nyhetsbrev har skickats ut som har innehållit omvärldsbevakning och annan viktig information. Dataskyddsenheten har planerar även att tillgängliggöra en digital grundutbildning som alla medarbetare i staden ska kunna ta del av.

Dataskyddsombudet ska övervaka efterlevnaden av förordningen. I kontrollplanen har dataskyddsombudet redogjort för att detta kommer att genomföras med två fördjupade kontroller som är utvalda efter verksamhetens riskområden och fasta kontrollpunkter som årligen ska stämmas av för att se hur organisationen befinner sig till i sitt dataskyddsarbete. Under första halvåret har dataskyddsombudet valt att fokusera på de fördjupade kontrollerna.

1.2 Fördjupade kontroller

De kontrollområden som valts ut för år 2021 är personuppgiftsbiträden och andra överenskommelser samt personuppgiftsbehandlingsregistret. Avseende kontrollen gällande personuppgiftsbehandlingsregistret har organisationen ombetts att svara på frågor om dokumentationen av personuppgiftsbehandlingar och hur de arbetar med och vilka rutiner som finns för att säkerställa att registret är uppdaterat och heltäckande. Dataskyddsombudet har även slumpvis valt ut behandlingar i organisationens register för att kontrollera om de uppfyller kraven enligt förordningen. Dataskyddsombudet har därefter gått igenom underlagen och presenterat resultatet i en rapport. Samma metod har använts för kontrollen av personuppgiftsbiträdesavtalen, där organisationen ombetts svara på ett antal frågor och därefter har dataskyddsombudet gjort en stickprovskontroll på tre stycken personuppgiftsbiträdesavtal. De fördjupade kontrollerna finns sammanställda i bilaga 2.

1.2.1 Iakttagelser från kontrollen avseende personuppgiftsbiträden och andra överenskommelse

Sammanfattningsvis konstateras att bolaget arbetar löpande med hanteringen av personuppgiftsbiträdesavtal och har både tagit fram en rutin som ska följas vid sådana situationer samt en egen mall för avtal. Mallen säkerställer att de obligatoriska minimikraven för personuppgiftsbiträdesavtal är uppfyllda vid personuppgiftsbiträdesavtal. I mallen saknas enbart information om biträdets skyldighet att gå med på och bistå vid granskning och inspektioner, vilket dataskyddsombudet rekommenderar bolaget att lägga till i avtalet. Slutligen rekommenderas bolaget att ta fram en rutin för att kunna följa upp så att biträdena uppfyller sina åtaganden enligt avtalet. Det kan också ske genom att det i avtalen skrivs in klausuler angående detta och då behövs ingen rutin.

1.2.2 Iakttagelser från kontrollen avseende personuppgiftsbehandlingsregistret

Sammanfattningsvis kan konstateras att organisationen har ett register över alla sina personuppgiftsbehandlingar. Av stickprovskontrollen framkom att alla obligatoriska fält är ifyllda förutom att det på vissa behandlingar saknades kontaktuppgiften till personuppgiftsbiträde. Dataskyddsombudet har därför rekommenderat organisationen att komplettera registret med kontaktuppgifter till sina personuppgiftsbiträden där det saknas. Organisationen uppdaterar registret när nya behandlingar tillkommer och planerar att ta fram en rutin för arbetet med registret. Dataskyddsombudet rekommenderar att rutinen innehåller information om de obligatoriska kraven på ett register samt ansvar och roller inom bolaget.

1.3 Underlag

Bilaga 1 Kontrollplan för dataskyddsarbetet 2021

Bilaga 2 Fördjupade kontroller

2 Årets fortsatta arbete

2.1 Aktuella frågor

Frågor man har arbetat med under våren i verksamheten är bland annat personuppgiftsbiträdesavtal och biträden inför nya behandlingar. Dataskyddsombudet har också lämnat råd utifrån Schrems II-domen och tredjelandsöverföringar där verksamheten gjort en kartläggning av behandlingar som innebär en sådan överföring. Diskussioner har även förts gällande rättsliga grunder för behandlingar. Dataskyddsombudet har regelbundet avstämningsmöten med dataskyddsgruppen, som är aktiva inom verksamheten och jobbar återkommande med dataskyddsfrågor.

2.2 Kommande frågor

Under hösten 2021 kommer dataskyddsombudet att stämma av de fasta kontrollpunkterna med organisationen, följa upp tidigare lämnade rekommendationer samt ta fram en ny kontrollplan för 2022. Dataskyddsombudet kommer också fortlöpande att svara på inkommande frågor och agera rådgivande vid konsekvensbedömningar.

Därutöver kommer dataskyddsenheten att fortsätta att regelbundet skicka ut nyhetsbrev med information från dataskyddsenheten och aktuell omvärldsbevakning. Dataskyddsenheten arbetar även med att ta fram ett antal utbildningar som kommer att göras tillgängliga för alla stadens förvaltningar och bolag. Ett urval av dessa utbildningar kommer att hållas under hösten 2021. Dataskyddsenheten bevakar även aktivt frågan om tredjelandsöverföringar som uppstått efter Schrems II-domen (se tidigare utskick *Information från Göteborgs Stads Dataskyddsenhet med anledning av Schrems II-domen* från dataskyddsenheten till förvaltningar och bolag i Göteborgs Stad 2020-09-18). Uppdateringar, när de uppstår, kommuniceras skyndsamt till berörda inom respektive förvaltning och bolag.

Fördjupad kontroll

Personuppgiftsbiträdesavtal

Bakgrund

Den fördjupade kontrollen av personuppgiftsbiträdesavtalen syftar till att se om organisationen uppfyller kraven i förordningen gällande biträdesavtal. Kontrollen har undersökt verksamhetens rutiner gällande ingående, uppföljning, kontroll och instruktioner. Kontrollen har genomförts i två delar, del ett har bestått av ett antal frågor som besvarats av organisationen och del två har bestått av att dataskyddsombudet slumpvis valt ut tre avtal och kontrollerat om dessa uppfyller kraven.

Iakttagelser från kontrollen

Del 1

Gryaab har bifogat en lista med de aktörer som de har identifierat som personuppgiftsbiträden. Till alla de angivna aktörerna finns det upprättade personuppgiftsbiträdesavtal, som också har bifogats till dataskyddsombudet. Bolaget uppger att de inte i några utav fallen lämnat instruktioner till biträdena utan att de förlitar sig på leverantörernas avtal i de flesta fall. Möjligheten att lämna instruktioner saknades när bolaget svarade på frågorna, men har sedan dess lagts till.

Vidare uppger bolaget att det inte finns någon särskild rutin för att avgöra om en leverantör anses vara personuppgiftsbiträde, utan att verksamheten förlitar sig på de dem tecknar avtal med. Gryaab saknar rutin för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder utan bolaget litar på de man tecknar avtal med. Däremot finns det en nyligen framtagen rutin gällande regelbunden avtalsuppföljning för personuppgiftsbiträdesavtalen. Rutinen berör när personuppgiftsbiträdesavtal ska tecknas, av vem, vilket innehåll som ska finnas, vart de ska förvaras och hur de följs upp. Det framkommer också att det i Gryaabs organisation är den som är närmast behandlingen som ska teckna avtal om inget annat framgår.

Gryaab arbetar i sin dataskyddsgrupp aktivt med frågor rörande personuppgiftsbiträdesavtal och har nyligen tagit fram en rutin som berör de flesta av de granskade punkterna. Bolaget har under granskningens gång tagit fram en egen mall för personuppgiftsbiträdesavtal, men har tidigare i de flesta fall förlitat sig på leverantörernas avtal. I de fallen saknas information om hur Gryaab säkerställer att alla krav för ett personuppgiftsbiträdesavtal är uppfyllda, men med kunskap om minimikraven i förordningen och den egna framtagna mallen är det enkelt åtgärdat för framtiden. I den framtagna rutinen hänvisas också till artikel 28.3 i Dataskyddsförordningen där minimikraven finns med. Med den nya mallen finns också möjlighet att lämna instruktioner vilket dataskyddsombudet tycker är bra då det är viktigt att personuppgiftsansvarige lämnar korrekta instruktioner. Det är vidare positivt att bolaget uppmärksammat på vad som saknats inom organisationen samt åtgärdat detta i form av en ny rutin och mallen. Av de existerande personuppgiftsbiträdesavtalen som saknar

instruktioner kan det vara värt att se över huruvida detta är något man bör uppdatera. Syftet med instruktioner är att säkerställa så att det är den personuppgiftsansvarige, och inte personuppgiftsbiträdet, som bestämmer vad som sker med personuppgifterna. Det innebär att om personuppgiftsbiträdet agerar utanför instruktionerna genom att själv bestämma ändamål och medel, kan biträdet istället ses som ansvarig och åläggas samma ansvar som en personuppgiftsansvarig. Instruktionerna kan följas direkt av avtalet eller ges skriftligen på annat sätt, men måste sparas så att de finns dokumenterade.

Gryaab uppger att de saknar rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder och uppger att man inte vet hur detta ska göras. Att följa upp så personuppgiftsbiträdet följer det man avtalat om är ett sätt för personuppgiftsansvarige att säkerställa att ens personuppgiftsbehandling uppfyller kraven i förordningen. Det kan tex göras genom att man enligt avtalet har möjlighet till revision eller liknande.

Slutligen svarar bolaget att man är osäker på frågan gällande hur man säkerställer att tecknande av personuppgiftsbiträdesavtalen sker i behörig ordning. Syftet med frågan var att undersöka huruvida bolaget har en rutin som säkerställer att ingen obehörig ingår avtal som sedan verksamheten blir bunden av. Bolaget uppger att den som är närmast behandlingen ingår avtalet, vilket kan vara bra så länge bolaget kan säkerställa att de som ingår avtalen har tillräckligt med kunskap gällande de krav som förordningen ställer upp på avtalen och biträden. Det är slutligen positivt att bolaget dokumenterat vem som ska ingå avtalen i sin nya rutin så att risken för att fel person ingår avtalen minskar.

Del 2

Dataskyddsombudets stickprovskontroll har omfattat de följande tre avtalen: Answer Online, Proact IT samt bolagets egen mall. Utifrån de minimikrav som anges i artikel 28.3 har dataskyddsombudet enbart kontrollerat så att dessa uppfylls.

- Answer Online: Att behandlingen enbart får ske utifrån angivna instruktioner framkommer i avtalet, men det saknas särskilda därtill hörande instruktioner. I övrigt är alla minimikrav uppfyllda.
- Proact IT: Även i detta avtal framkommer att behandlingen enbart får ske utifrån angivna instruktioner, men det saknas särskilda därtill hörande instruktioner. I övrigt är alla minimikrav uppfyllda. På punkten angående att biträdet har en skyldighet att bistå personuppgiftsansvarige att vidta åtgärder för att uppfylla de registrerades rättigheter framkommer bara att biträdet bistår i vissa delar och till en tillkommande kostnad. En kostnad tillkommer även i de fall biträdet ska bistå den personuppgiftsansvariga i frågan om dennes skyldigheter enligt artikel 32-36.
- Gryaabs egen mall: Alla obligatoriska krav enligt 28.3 finns med i mallen. Det finns även bilagt en sida för att fylla i särskilda instruktioner. Det enda som saknas är information om att biträdet är skyldigt att gå med på och bistå vid granskning och inspektioner. Det finns enbart under punkten 10 en rätt för personuppgiftsansvarige att få insyn i behandlingen.

Sammanfattade rekommendationer

- Verksamheten har tagit fram en rutin för personuppgiftsbiträdesavtal som bör följas vid framtida personuppgiftsbiträdessituationer.
- Verksamheten har också tagit fram en egen mall med möjlighet att lämna instruktioner som bolaget bör använda sig av vid framtida tecknande av avtal. Det saknas information om biträdets skyldighet att gå med på och bistå vid granskning och inspektioner.
- Bolaget bör ta fram rutin eller annat tillvägagångssätt för att kunna följa upp så att biträdena gör de som utlovats. Detta kan också ske genom att det i avtalen skrivs in klausuler angående revision eller granskning.

Bilagor

1. Frågeställningsutskick

Fördjupad kontroll 2021

Biträdesavtal

Del 1

Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga även relevanta dokument, underlag och aktuella rutiner som ni har tagit fram. Svaren skall ha inkommit till dataskyddsombudet **senast den 5 april 2021**.
Har du frågor, kontakta ditt dataskyddsombud.

1. Ange/bifoga lista över vilka ni har identifierat som personuppgiftsbiträden.
    a. Ange för vilka personuppgiftsbiträden som det finns personuppgiftsbiträdesavtal med.
    b. Har ni gett instruktioner till de personuppgiftsbiträden som ni har avtal med (enligt art. 28.3 a dataskyddsförordningen)?
2. Finns det rutiner för bedömningen av om en leverantör eller annan motpart ska anses vara personuppgiftsbiträde?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni går tillväga för att annars göra den bedömningen.
3. Finns det rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni annars går tillväga för att göra den bedömningen.
4. Finns det rutiner för regelbunden avtalsuppföljning (t.ex. om tjänsten ändras eller avslutas) för personuppgiftsbiträdesavtalen?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni säkerställer att era personuppgiftsbiträdesavtal är aktuella och uppdaterade?
5. Ange hur ni säkerställer att tecknande av personuppgiftsbiträdesavtal sker i behörig ordning.

Fördjupad kontroll

Personuppgiftsbehandlingsregistret

Bakgrund

Den fördjupade kontrollen av personuppgiftsbehandlingsregistret syftar till att se om organisationen uppfyller kraven om att systematiskt dokumentera alla behandlingar i form av ett register enligt artikel 30 i dataskyddsförordningen och att rutiner finns för att säkerställa att registerförteckningen hålls aktuell. Kontrollen har genomförts i två delar, del ett har bestått av ett antal frågor som besvarats av organisationen och del två har bestått av att dataskyddsombudet slumpvis valt ut tre behandlingar från registret och kontrollerat om dessa uppfyller kraven.

Iakttagelser från kontrollen

Gryaab uppger att de använder sig av Draftit för att registrera sina personuppgiftsbehandlingar i ett register. Bolaget uppger att all information enligt artikel 30 i GDPR ska vara komplett för varje behandling, men att kontaktuppgifter till personuppgiftsbiträde saknas i vissa behandlingar då detta varit okänt för dem. Bristen kommer att ses över vid nästa genomgång och åtgärdas. Kontroll av registret gjordes 2021-03-16. I dagsläget finns 36 behandlingar registrerade. Dataskyddsombudets stickprovskontroll gjordes på 3 av de registrerade behandlingarna. I de kontrollerade behandlingarna var alla obligatoriska fält ifyllda varpå inga synpunkter finns utöver det som bolaget själva uppmärksammat. De tre kontrollerade behandlingarna var Besöksregistrering, Körjournalsregistrering samt Personaladministration Rekrytering.

Gryaab anger att registret uppdateras löpande och gås igenom två gånger per år. För att säkerställa att denna process genomförs korrekt, ska en rutin tas fram där detta dokumenteras utförligare. Dataskyddsombudet anser att det är positivt att verksamheten tar fram en rutin, för att säkerställa att arbetet sker på ett korrekt sätt. I dagsläget finns det enbart dokumenterat i ett mötesprotokoll. Trots att bolaget inte har en rutin för att kontinuerligt uppdatera registret görs regelbundet en översyn av registret. Att det två gånger årligen gås igenom minska risken för att det dels finns behandlingar som blivit inaktuella, vilket innebär att personuppgifterna i dessa behandlingar inte längre får behandlas, dels att det finns behandlingar som är felaktigt påbörjade eller att personuppgifter behandlas på fel rättsligt grund – kanske till och med utan rättslig grund och är därmed inte tillåtna. Fördelarna med att ha ett korrekt, uppdaterat register är att medarbetare, dataskyddsombud och i slutändan registrerade får en god överblick av vilka personuppgiftsbehandlingar som verksamheten har. Det i sin tur bidrar till en följsamhet gentemot dataskyddslagstiftningen och mindre risk att tillsynsmyndigheten utfärdar vite.

Bolaget uppger att registret är en naturlig del i arbetet genom just den återkommande genomgången samt vid behov av nya personuppgiftsbehandlingar. Registret används också för kontroll av tex syfte med en behandling och vilka behandlingar som finns registrerade. Att bolaget använder personuppgiftsbehandlingsregistret som en naturlig del i arbetet för att övervaka efterlevnaden av dataskyddslagstiftningen är positivt. Eftersom det är ett krav enligt förordningen att personuppgiftsansvarig ska ha ett korrekt och uppdaterat register är det naturligt att vid påbörjandet av en ny behandling även föra in denna behandling i registret. Vidare är det positivt att bolaget tar fram en rutin för ett

följsamt arbetssätt, som minskar risken för att registret blir utdaterat och sannolikt inte uppfyller kraven i dataskyddsförordningen. För att säkerställa att alla obligatoriska fällt är ifyllda kan en hänvisning till artikel 30 vara lämplig. I rutinen bör det också framkomma vem eller vilka inom organisationen som har ansvar för registret. Faller ansvaret på dataskyddskontakterna bör dataskyddskontakterna också få möjlighet att sätta sig in i varje ny behandling för att kunna fylla i registret korrekt. Dock innebär inte det att övriga medarbetare som påbörjar nya behandlingar undkommer ansvar, utan även de måste ha tillräckligt med kunskap för att kunna avgöra t.ex. rättslig grund. Personuppgiftsbehandlingsregistret är också ett verktyg för att få en förståelse för sin verksamhet och kunna överblicka var processer och aktiviteter härrör. Registret är ett ypperligt sätt att avgöra exempelvis vilken laglig grund som kan vara lämplig, om behandlingen verkligen ska anses utgöra en ny behandlingen eller kan täckas in av en annan behandling och för att avgöra vem som bör och kan ha ansvar.

Sammanfattande rekommendationer

- Se till att den planerade rutinen säkerställer att alla obligatoriska krav enligt förordningen uppfylls
- Rutinen bör också peka ut ansvar och roller inom bolaget i förhållande till registret
- Bolaget bör, som de själva påpekat, åtgärda att kontaktuppgifter till personuppgiftsbiträden i vissa behandlingar saknas

Bilagor

2. Kontrollfrågor om personuppgiftsbehandlingsregistret

Fördjupad kontroll 2021

Personuppgiftsbehandlingsregistret

Del 1

Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga även relevanta dokument, underlag och aktuella rutiner som ni har tagit fram. Svaren skall ha inkommit till dataskyddsombudet **senast den 11 mars 2021**.
Har du frågor, kontakta ditt dataskyddsombud.

1. Har verksamheten ett personuppgiftsbehandlingsregister där alla behandlingar är dokumenterade?
2. Är all information enligt artikel 30 i GDPR komplett för varje behandling (obligatoriska fälten)? Om inte, vilka obligatoriska fält har inte fyllts i och varför?
3. Finns det en rutin för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändrats? När gjorde ni senast en översyn av registrets innehåll?
4. Använder dataskyddsorganisationen personuppgiftsbehandlingsregistret som en naturlig del i arbetet? Beskriv hur och när det används.