Beslutsunderlag
Utfärdat 2021-05-31
Diarienummer
0016/21

Handläggare
Katrin Gundersen
Telefon: 031-368 55 12
E-post: katrin.gundersen@gotalejon.goteborg.se

Delårsrapport från Dataskyddsenheten

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

- anteckna delårsrapport från Dataskyddsenheten

Sammanfattning

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

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.

Sammanfattningsvis kan konstateras att organisationen har ett register över alla sina personuppgiftsbehandlingar. Av stickprovskontrollen framkom att alla obligatoriska fält är ifyllda. Det saknas rutin för användning av registret och för att säkerställa så att alla behandlingar i registret uppfyller de obligatoriska kraven. Vidare bör det förtydligas vem inom bolaget som har ansvar för översyn och uppdatering av registret, samt vem som inför/ändrar behandlingar.

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ingen samverkan nödvändig

Bilagor

1. Delårsrapport från Dataskyddsenheten.
2. Bilaga 1 Kontrollplan

3. Bilaga 2 Fördjupade kontroller

Ärendet

Styrelsen ska besluta om att anteckna delårsrapporten från Dataskyddsenheten.

Beskrivning av ärendet

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 i form av en PM, se bilaga 2. 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. Materialet har sammanställts i en rapport i form av ett PM, se bilaga 3.

Bolagets bedömning

Det är bolagets bedömning att delårsrapporten överensstämmer med den revision som gjordes. Bolaget kommer att arbeta vidare med rekommendationerna.

Göteborgs Stad

Delårsrapport för dataskyddsarbetet

Försäkrings AB Götalejon

2021-05-26

Innehåll

1 Årets arbete hittills

1.1 Dataskyddsarbetet hittills

I januari 2021 översändes en kontrollplan till bolaget 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.

Nyhetsbrev har skickats ut som har innehållit omvärldsbevakning och annan viktig information. Dataskyddsenheten 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

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 i form av en PM, se bilaga 2. 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. Materialet har sammanställts i en rapport i form av ett PM, se bilaga 3.

1.2.1 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. Det saknas rutin för användning av registret och för att säkerställa så att alla behandlingar i registret uppfyller de obligatoriska kraven. Vidare bör det förtydligas vem inom bolaget som har ansvar för översyn och uppdatering av registret, samt vem som inför/ändrar behandlingar. Bolaget

uppger sig sakna kunskap om Draftit och har möjlighet att vända sig till Dataskyddsenheten för vidare utbildning.

1.2.2 Iakttagelser från kontrollen avseende personuppgiftsbiträden och andra överenskommelser.

Sammanfattningsvis konstateras att bolaget arbetar löpande med hanteringen av personuppgiftsbiträdesavtal och har tagit fram en egen mall för avtal. Mallen säkerställer att de obligatoriska minimikraven för personuppgiftsbiträdesavtal är uppfyllda vid personuppgiftsbiträdesavtal, förutom på en punkt. I mallen saknas enbart information om biträdets skyldighet att bistå så att den personuppgiftsansvariges skyldigheter enligt artikel 36 förhandssamråd fullgörs, vilket dataskyddsombudet rekommenderar bolaget att lägga till i avtalet. Det bör också finnas möjlighet att lämna instruktioner till biträdena. Bolaget har inkorporerat frågan om personuppgiftsbehandling i en annan rutin gällande utlagd verksamhet, men saknar särskild rutin gällande biträden. Dataskyddsombudet rekommenderar bolaget att se över om ytterligare rutin behövs eller eventuellt att nuvarande räcker eller behöver förtydligas. Slutligen rekommenderas bolaget att säkerställa så att korrekta instruktioner lämnas till personuppgiftsbiträden.

1.3 Underlag

Bilaga 1 Kontrollplan för dataskyddsarbetet 2021

Bilaga 2 Fördjupade kontroller

2 Årets fortsatta arbete

2.1 Aktuella frågor

Bolaget fortsätter att arbeta aktivt med dataskyddsfrågor och har sökt dataskyddsombudets råd i frågor gällande personuppgiftsincidenter och personuppgiftsbehandlingsregistret. Bolaget involverar dataskyddsombudet vid behov och dataskyddsombud och dataskyddskontakt har regelbundna avstämningsmöten.

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.

Göteborgs Stad

Försäkrings AB Göta Lejon

Kontrollplan för dataskyddsarbetet 2021

2021-01-22

Innehåll

1 Bakgrund

1.1 Dataskyddsförordningen

Dataskyddsförordningen (DSF) trädde i kraft i maj 2018 och är en EU-förordning med syfte att skydda fysiska personers grundläggande fri- och rättigheter, att garantera ett likvärdigt skydd samt att säkerställa det fria flödet av personuppgifter inom unionen. Förordningen kompletteras av dataskyddslagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessa samspelar även med annan speciallagstiftning.

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder.

Efterlevnaden av lagstiftningen övervakas av Integritetsskyddsmyndigheten och överträdelser kan leda till bland annat sanktionsavgifter eller skadestånd.

1.1.1 Personuppgiftsansvarig

En personuppgiftsansvarig kan vara en fysisk person, juridisk person, en offentlig myndighet, institution eller ett annat organ. Varje förvaltning med egen nämnd räknas som en egen offentlig myndighet. I juridisk mening så är därmed ytterst varje enskild nämnd eller styrelse ansvarig för att de personuppgiftsbehandlingar som organisationen hanterar utförs i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör enligt dataskyddsförordningen ett dataskyddsombud, med särskild sakkunskap i fråga om dataskyddslagstiftning och praxis, utses för att bistå den ansvarige med att övervaka den interna efterlevnaden av förordningen.

1.1.2 Dataskyddsombud

Dataskyddsombudet ska ge råd och information till den personuppgiftsansvarige samt övervaka efterlevnaden av dataskyddsförordningen och annan relevant dataskyddslagstiftning. Det innebär bland annat att kontrollera hur den personuppgiftsansvarige behandlar personuppgifter, att bestämmelser och interna styrdokument följs samt att ge råd och stöd vid konsekvensbedömningar. Dataskyddsombudet ska enligt dataskyddsförordningen utföra sitt arbete på ett oberoende sätt gentemot den som är personuppgiftsansvarig och får inte instrueras av denne hur arbetet ska utföras. Dataskyddsombudet är inte heller ansvarig för att lagstiftningen efterlevs.

Dataskyddsombudet är även kontaktperson för de registrerade och tillsynsmyndigheten.

2 Kontrollplan för dataskyddsarbetet 2021

2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 DSF. En del av denna övervakning innebär att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom denna kontrollplan som syftar till att informera personuppgiftsansvariga om tidplan och särskilda fokusområden för kontrollarbetet år 2021.

Målsättningen med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Maximera ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.2 Ett riskbaserat arbetssätt

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Kontrollplanen utgår därför ifrån dataskyddsombudets riskbedömning avseende verksamhetens personuppgiftsbehandlingar och tas fram i dialog med verksamheten. Primära fokusområden och prioriteringar utgår från eventuella problem som bedöms utgöra en högre risk för dataskyddet i verksamheten.

Gemensamt för stadens verksamheter har dataskyddsenheten identifierat två riskområden som är särskilt relevanta, utifrån att respektive personuppgiftsansvarig har möjlighet att genom att bedriva ett systematiskt dataskyddsarbete påverka omfattningen av de risker som dessa områden inbegriper. Det första riskområdet innefattar ekonomisk skada (exempelvis skadestånd och sanktionsavgifter), vars risker beror på huruvida verksamheten i sin personuppgiftshantering säkerställer att dataskyddsförordningen följs. Det andra riskområdet innefattar förtroendeskada (så som exempelvis försämrat varumärke och minskad tillit) och är beroende av verksamhetens förmåga att hantera de registrerades rättigheter enligt dataskyddsförordningen.

2.3 **Upplägg**

Kontrollarbetet består av tre delar som tillsammans syftar till att ge såväl dataskyddsombud som personuppgiftsansvariga en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot förordningen.

a) Den första delen består av fasta kontrollpunkter där varje punkt bedöms årligen. Bedömningen görs genom löpande kontroller, genom deltagande i verksamhetens arbete och i förekommande fall utifrån given information.

b) Den andra delen är en fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter.

c) Den tredje delen är en uppföljning och bedömning av hur verksamheten hanterat tidigare lämnande rekommendationer.

Kontrollarbetets olika delar kommer sammanställas och presenteras i årsrapporten för nämnd/styrelse. Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer varje personuppgiftsansvarig kunna följa utvecklingen av dataskyddsarbetet inom verksamheten över tid.

2.3.1 **Verksamhetsspecifika förutsättningar**

Dataskyddsombudets arbete kommer att bedrivas utifrån verksamhetens specifika förutsättningar. Identifierade aktiviteter kan därför komma att justeras utifrån händelser som inträffar i verksamheterna eller i omvärlden.

2.4 **Tidplan för kontroller 2021**

Månad	**Huvudaktivitet**	**Övriga aktiviteter**
Januari	Kontrollplan för året lämnas till nämnd/styrelse	Uppföljning och kontroll av övriga fasta kontrollpunkter kommer ske löpande under året.
Februari-April	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs	
Maj	Fördjupad kontroll slutförs och rekommendationer lämnas till verksamheten	
Juni	Delårsrapportering avseende verksamhetens dataskyddsarbete för nämnd/styrelse	
September-Oktober	Uppföljning av tidigare lämnade rekommendationer	
November	Årsrapport lämnas till verksamheten	
December	Årsrapport presenteras för nämnd/styrelse	

3 Kontrollpunkter

3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas omfattning utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 DSF). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i verksamhetens ordinarie processer. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 DSF, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att personuppgiftsansvarig, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.

Med principen om inbyggt dataskydd avses att man tar hänsyn till förordningen vid utformning av IT-system och rutiner, och på så sätt från början säkerställer att både kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Principen om dataskydd som standard innebär att personuppgifter i standardfallet inte behandlas i onödan, vilket kan göras genom att ha lämpliga tekniska och organisatoriska åtgärder som standard.

Med principerna som utgångspunkt har elva kontrollpunkter definierats, av både organisatorisk och teknisk karaktär, vilka är gemensamma för alla verksamheter inom Göteborgs Stad. De punkter som fastställts utgör en del av fundamentet i lagstiftningen. Syftet med arbetssättet är att tillsammans hitta strategier, rutiner och arbetssätt som hanterar punkterna så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

Kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Personuppgiftsregister
5. Övergripande strategi för dataskydd
6. Utbildning
7. Integritetspolicy
8. Mejl- och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.1.1 **Beskrivning av fasta kontrollpunkter**

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenten, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd. En verksamhetsspecifik strategi som anger ramarna för arbetet med dataskydd kan både främja ett riskbaserat arbetssätt och bidra till en kontinuitet i dataskyddsarbetet.

Kontrollpunkten innefattar även verksamhetens strategi för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddsförordningen efterlevs.

Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för mejl och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.

3.2 **Fördjupad kontroll 2021**

Den fördjupade kontrollen utgår från verksamhetens specifika risker. För verksamhetsåret har följande punkt/punkter fastställts:

Fokusområde 1: Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Den personuppgiftsansvarige är ansvarig för all behandling som utförs å dennes vägnar. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde att utföra personuppgiftsbehandlingar för sin räkning är alltså fortfarande personuppgiftsansvarig och kan inte avsäga sig de skyldigheter som följer av detta ansvar. Det är således av stor vikt att personuppgiftsansvariga har överblick över sina anlitade personuppgiftsbiträden och att de uppfyller de kvalitetskrav och krav vid, bl.a., anlitande av underbiträden som uppställs i förordningen. Förordningen kräver även att förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet regleras genom avtal (eller annan rättsakt), och det är den personuppgiftsansvarige som är ansvarig för att ett sådant avtal upprättas. Förordningen uppställer även vissa krav på vad ett sådant avtal ska innehålla.

Denna fördjupade kontroll syftar till att undersöka vilka som behandlar personuppgifter för Göta Lejons räkning och ifall dessa förhållanden är reglerade genom adekvata avtal. För att skapa en överblick över Göta Lejons generella och övergripande arbete med personuppgiftsbiträden inkluderar kontrollen även en undersökning av vilka rutiner och arbetssätt som Göta Lejon har vid anlitande av personuppgiftsbiträden.

Fokusområde 2: Kontrollpunkt 4: Personuppgiftsbehandlingsregister

Personuppgiftsbehandlingsregistret är ett krav enligt förordningen och ska kunna visas för tillsynsmyndigheten vid efterfrågan. I Göteborgs Stad används i nuläget programmet Draftit där verksamheterna registrerar sina behandlingar. Dataskyddsförordningen ställer krav på vad som ska förekomma i registret över personuppgiftsbehandlingar. Det handlar bland annat om ändamål för behandlingen, kategorier av registrerade och huruvida överföring av personuppgifter till tredjeland sker.

Eftersom tillsynsmyndigheten kan begära att ta del av registret är det av yttersta vikt att verksamheten dokumenterar sina behandlingar korrekt i registret. Denna fördjupade kontroll avser undersöka Göta Lejons dokumentation av personuppgiftsbehandlingarna för att säkerställa att de krav som förordningen ställer upp efterlevs. Kontrollen avser också att granska Göta Lejons arbete med och rutin för registret för att säkerställa så att kraven efterlevs.

4 Uppföljning

4.1 Uppföljning av lämnade rekommendationer

I dataskyddsförordningen anges att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå, för att säkerställa att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer. Detta är grunden för ett proaktivt arbetssätt och utgör en trygghet för nämnd/styrelse som uppmärksammas på status och observerade brister i dataskyddsarbetet. Det är då också av vikt för nämnd/styrelse att veta hur eventuella rekommendationer/brister omhändertagits. Dataskyddsombudet kommer därför årligen att följa upp hanteringen av de rekommendationer som lämnats till verksamheten och rapportera detta i årsrapporten.

4.1.1 Uppföljning av hittills genomförda kontroller

Sedan dataskyddsförordningen trädde i kraft i maj 2018 har dataskyddsombudet genomfört 2 kontroller för er verksamhet. Dessa kontroller kommer att följas upp inom ramen för de fasta kontrollpunkterna under 2021. Under året kommer dataskyddsombudet att se över vilka åtgärder som vidtagits med anledning av de rekommendationer som lämnats vid tidigare kontroller.

Kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet

Följs upp inom kontrollpunkt: Dataskyddsorganisation

Kontroll 2 (2020): Granskning av hantering av personuppgiftsincidenter.

Följs upp inom kontrollpunkt: Personuppgiftsincidenter

5 Avrapportering till nämnd/styrelse

5.1 Delårsrapportering

I juni månad kommer respektive nämnd/styrelse att få en delårsrapportering för dataskyddsarbetet av dataskyddsombudet. Fokus för delsårsrapporteringen är den verksamhetsspecifika fördjupade kontrollen som genomförs under våren.

Genom en delårsrapportering säkerställs att personuppgiftsansvarig nämnd/styrelse hålls informerad om dataskyddsombudets observationer av verksamhetens personuppgiftshantering. Formen för rapporteringen anpassas efter dataskyddsombudets bedömning av verksamhetens behov.

5.2 Årsrapport

Verksamhetens dataskyddsarbete kommer att sammanställas i en skriftlig årsrapport till nämnd/styrelse. Årsrapporten kommer innehålla information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig nämnd/styrelse ska årsrapporten presenteras i möte med nämnd/styrelse.

5.3 Särskilt yttrande till högsta ledning

Om det skulle uppstå situationer där den ansvarige fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, till exempel om en allvarlig brist kvarstår och inte åtgärdas, har dataskyddsombudet möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten.

5.4 Beslutanderätten i dataskyddsfrågor

Beslutanderätten i dataskyddsfrågor ligger alltid på den personuppgiftsansvarige och aldrig på dataskyddsombudet. Dataskyddsombudet är en specialist med en rådgivande roll och är en resurs som, på ett oberoende sätt, fokuserar på dataskyddsfrågorna i verksamheten och på det sättet bistår den personuppgiftsansvarige med bedömningar och råd. Om nämnden/styrelsen väljer att inte följa dataskyddsombudets rekommendationer ska skälen till detta motiveras och dokumenteras i enlighet med god praxis samt för att uppfylla ansvarsskyldigheten. Detta är även viktigt för det fall att frågan senare skulle bli föremål för tillsyn.

6 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till er kontaktperson/ert dataskyddsombud. Frågor kan också alltid ställas till dso@intraservice.goteborg.se.

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

Götalejon har bifogat en lista med de aktörer som de har identifierat som personuppgiftsbiträden. Till alla de angivna aktörerna finns det upprättade personuppgiftsbiträdesavtal. Vidare uppger bolaget att det inte finns någon särskild rutin för att avgöra om en leverantör anses vara personuppgiftsbiträde, utan att bedömningen görs beroende på vilket uppdrag man har för Göta Lejon. Att bolaget inte har någon rutin för att hantera personuppgiftsbiträden och tillhörande avtal kan vara en risk då man inte säkerställer följsamhet mot förordningen. Eftersom bolaget inte har särskilt många personuppgiftsbiträden, kan det vara en anledning till att man inte prioriterat att ta fram någon rutin för ändamålet. Men att ha en rutin underlättar för bolaget att se till så att alla krav enligt förordningen säkerställs i avtalsförhållandet, då detta i dagsläget inte framkommer hur det görs. Utifrån de personuppgiftsbiträdesavtal som skickats in till stickprovskontrollen framkommer det att bolaget har någon typ av mall för personuppgiftsbiträdesavtal för eget användande. Huruvida bolaget har säkerställt att mallen uppfyller minimikraven i förordningen eller i vilken omfattning mallen används vid tecknande av personuppgiftsbiträdesavtal, framkommer inte. Det är däremot positivt att bolaget har en egen mall och att man inte enbart förlitar sig på leverantörernas avtal. För att säkerställa att de egna avtalen uppfyller kraven kan exempelvis en checklista baserat på artikel 28.3 vara behjälplig.

Bolaget uppger vidare att de inte har lämnat instruktioner enligt artikel 28.3 i dataskyddsförordningen till alla avtal. Varför det inte finns instruktioner till alla avtal framkommer inte, men det kan vara av värde för bolaget att se över huruvida man bör lägga till instruktioner. 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. Kravet enligt artikel 28.3 är att det i personuppgiftsbiträdesavtalet ska framgå att personuppgiftsbiträdet enbart får behandla personuppgifter på

dokumenterade instruktioner från personuppgiftsansvarige, vilket har uppfyllts i de angivna avtalen. Däremot kan dataskyddsombudet inte hitta några ytterligare instruktioner om vad behandlingen egentligen innebär. Därmed vill dataskyddsombudet bara uppmärksamma bolaget på att det finns risker med att inte tydligt instruera biträdena hur personuppgiftsbehandlingen innebär, eftersom det då inte är lika tydligt när personuppgifterna behandlas felaktigt.

I övrigt så uppger bolaget att det saknas det rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder. Det måste nödvändigtvis inte heller vara en separat rutin utan kan skrivas in direkt i avtalen, så länge bolaget har kontroll över att detta sker vid varje avtalstecknande. Det gör också att biträdet är medveten om hur kontroller sker och vad som kontrolleras. Eftersom Göta Lejon som personuppgiftsansvarig också ansvarar för det biträdet gör, är det viktigt att bolaget kan kontrollera att biträdet gör det som utlovas. Garantierna är ett sätt för biträdet att visa för personuppgiftsansvarige att man vidtar de åtgärder som krävs för behandlingen.

Avtalsuppföljning däremot görs enligt bolagets Riktlinje för utlagd verksamhet som har bifogats till dataskyddsombudet. Däri ingår en punkt under “uppdragsavtalets innehåll” som heter “hantering av personuppgifter i enlighet med Dataskyddsförordningen”, där punkten ska regleras. I den mall som finns för utlagd verksamhet ska punkten “hanteras ansvar om personuppgifter/GDPR i avtalet eller via PUB-avtal" fyllas i. Det visar på att bolaget tar dataskyddsfrågor på allvar och har inkorporerat det i det dagliga arbetet.

Slutligen ser dataskyddsombudet det som positivt att det alltid är VD:n i bolaget som skriver under avtalen minskar risken för att någon obehörig ingår avtal som hela organisationen blir bunden av. Det kan vara av vikt att behörighetsordningen dokumenteras så att detta säkerställs. Följaktligen är det också bra att VD har kunskap angående dataskyddsfrågor och de krav som ställs på ett biträdesavtal.

Del 2

Dataskyddsombudets stickprovskontroll har omfattat de följande tre avtalen: MSB, Cunningham Lindsey och Göteborgs Stads Leasing AB. Utifrån de minimikrav som anges i artikel 28.3 har dataskyddsombudet enbart kontrollerat så att dessa uppfylls.

- MSB: Framkommer att behandlingen enbart får ske på angivna instruktioner men det saknas särskilda sådana instruktioner. Avseende biträdets skyldighet att bistå så att den personuppgiftsansvarige skyldigheter enligt artikel 32-36 fullgörs, saknas uttrycklig information rörande artikel 35 (konsekvensbedömning) samt artikel 36 (förhandssamråd). I övrigt är alla minimikrav uppfyllda.
- Cunningham Lindsey (utifrån Götalejons egen mall): Framkommer att behandlingen enbart får ske på angivna instruktioner och det finns sådana bilagda. Avseende biträdets skyldighet att bistå så att den personuppgiftsansvarige skyldigheter enligt artikel 32-36 fullgörs, saknas uttrycklig information rörande artikel 36 (förhandssamråd). I övrigt är alla minimikrav uppfyllda.
- Göteborgs Stads Leasing AB: Framkommer att behandlingen enbart får ske på angivna instruktioner men det saknas sådana särskilda instruktioner. Avseende

biträdets skyldighet att bistå så att den personuppgiftsansvarige skyldigheter enligt artikel 32-36 fullgörs, saknas uttrycklig information rörande artikel 36 (förhandssamråd). I övrigt är alla minimikrav uppfyllda.

Sammanfattning

- Kartlägg vilket behov verksamheten har av att ta fram en rutin för bedömning och avtalsskrivande med biträden.
- Säkerställ så att den mall verksamheten tagit fram uppfyller kraven enligt förordningen och försök i den mån det går att använda den, så att bolaget kan säkerställa att kraven enligt förordningen efterlevs.
- Säkerställ så att instruktioner lämnas till biträden så att personuppgiftsbehandlingen sker på rätt sätt.

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

Göta Lejon uppger att de har alla sina personuppgiftsbehandlingar registrerade i Draftit. All information enligt artikel 30 i GDPR ska vara komplett för alla behandlingar. Bolaget har ingen skriftlig rutin för hur ofta eller vad som ska kontrolleras i systemet. Det har inte heller gjorts någon direkt översyn av systemet sedan det implementerades. Utifrån de rekommendationer som erhållits i revisioner har verksamheten dock varit inne och gjort uppdateringar. Att inte ha åtminstone en årlig uppföljning av verksamhetens behandlingar i registret innebär en stor risk 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. Det framkommer inte på vilket sätt bolaget säkerställer att all information enligt artikel 30 är komplett för varje behandling, då det saknas rutin för att föra in och följa upp information i systemet. Den stickprovskontroll som utförts av dataskyddsombudet visar att i de tre behandlingar som granskats så är alla obligatoriska fält ifyllda. Däremot bör innehållet ses över, exempelvis vad gäller behandlingen Facebook som fått ändrade förutsättningar nu allt sedan rättsläget ändrades i juli 2020 efter Schrems II-domen. I registret framkommer att ingen överföring till tredjeland sker, men det är felaktigt på grund av att Facebook är ett amerikanskt ägt bolag som delar data i hela världen. Bolaget uppmanades redan i höstas att kartlägga vilka behandlingar som innebar en tredjelandsöverföring. Det är bör påpekas att stickprovskontrollen gjordes på 3 behandlingar, medan det finns 81 behandlingar registrerade.

I dagsläget finns ingen rutin eller arbetssätt för att använda personuppgiftsregistret som en naturlig del i det dagliga arbetet. Registret används idag vid frågor kring personuppgiftshantering och när nya behandlingar som ska föras in i registret. Registret kan då ge en ledning till huruvida det ska registreras en ny behandling eller om den aktuella personuppgiftsbehandlingen kan täckas in av en tidigare registrerad behandling. Bolaget uppger som förklaring att det föreligger en kunskapsbrist i hur systemet fungerar och att de inte fått tillräckligt med information om hur det ska

användas. Bolaget uppger att de saknar utbildning i verktyget för att kunna hantera det korrekt och ändamålsenligt. Man saknar också ett uttalande från Dataskyddsenheten om hur man har tänkt sig användningen av systemet. Bolaget uppger att de kan bli bättre på att använda systemet med hjälp av instruktioner från Dataskyddsenheten. Dataskyddsenheten har vid implementeringen av Draftit erbjudit alla som berörs, utbildning i systemet. Det finns även en serviceportal man kan vända sig med frågor, samt att det på Dataskyddsenheten finns en systemförvaltare som arbetar med detta. Bolaget har erbjudits och deltagit i utbildningen som Dataskyddsenheten erbjöd i mars 2019. Därefter har bolaget även fått hjälp från Dataskyddsenheten med att föra över information ifrån en excelfil till systemet. Vid behov av ytterligare hjälp och stöd finns Dataskyddsenheten tillgänglig.

Dataskyddsombudet rekommenderar att bolaget tar fram en rutin eller plan för att se över systemet och behandlingarna, rimligtvis åtminstone två gånger per år. Utifrån den checklista som bifogats i granskningen kan bolaget också säkerställa så att alla behandlingar uppfyller de lagstadgade kraven. I dagsläget finns det inget sätt för bolaget att säkerställa detta. I den mån bolaget anser sig sakna kunskap och utbildning om systemet finns möjlighet att vända sig till Dataskyddsenheten för ytterligare hjälp. I rutinen bör det också framkomma vem eller vilka inom organisationen som har ansvar för registret. Faller ansvaret på dataskyddskontakten bör dataskyddskontakten 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. Dataskyddsombudet vet att systemet som idag finns för att registrera sina behandlingar inte är helt optimalt men det går att använda till mer än bara registerförfrågningar. Registret bör till exempel kunna finnas som stöd vid utredning, rapportering och dokumentation vid personuppgiftsincidenter – om det blivit ett intrång i ett system kan registret användas för att söka fram vilka behandlingar som görs i det berörda systemet samt att kontrollera vilka personuppgifter och kategorier av drabbade personer som berörs.

Sammanfattande rekommendationer

- Bolaget bör ta fram en rutin eller plan för att säkerställa att alla behandlingar uppfyller de obligatoriska kraven i förordningen.
- Förtydliga vem inom organisationen som har ansvar för registret.
- Bolaget bör kartlägga vilket behov av utbildning av Draftit som behövs och ta fram en plan för att det säkerställs.

Bilagor

2. Frågeställningsutskick

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.