Beslutsunderlag
Utfärdat 2021-01-028
Diarienummer 0037/21

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

Årsrapport från Dataskyddsenheten 2020

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anteckna årsrapport från Dataskyddsenheten 2020

Sammanfattning

Årets dataskyddsplan innehåller fem fokusområden som är adresserade till såväl dataskyddsombudet som till dataskyddsansvariga inom organisationen. Även om fler aktiviteter kommer att genomföras under årets gång har dessa fem bedömts som mest angelägna att genomföra under år 2020.

- Integritetspolicy
- Kvalitetskontroll av befintliga personuppgifter
- Rutiner för notifiering av personuppgiftsincidenter
- Personuppgiftsbiträden och personuppgiftsbiträdesavtal
- Kunskapsnivå hos medarbetare

Bilagor

1. Årsrapport från Dataskyddsenheten 2020
2. Information om granskning
3. Frågeställningar
4. Instruktion personuppgiftsincident
5. Register personuppgiftsincident
6. Rutin personuppgiftsincident

Katrin Gundersen — Bolagsjurist

Annika Forsgren — VD

Göteborgs Stad

Årsrapport

Göta Lejon Försäkrings AB

2020-12-21

dso@intraservice.goteborg.se
031-365 00 00 (kontaktcenter)

Versionshantering

Datum	Version	Beskrivning	Ändrat av

Innehåll

1 Inledning

1.1 Bakgrund

Det är över två år sedan dataskyddsförordningen infördes och även om kraven i förordningen har funnits sedan 1998 då Personuppgiftslagen (PuL) trädde i kraft, så ställs det nu högre krav på att personuppgifterna hanteras på ett korrekt, säkert och transparent sätt. Tillsynsmyndigheten har nu också, till skillnad från PuL-tiden, möjlighet att tilldela verksamheter som inte följer förordningen sanktionsavgifter. I Göteborgs Stad är varje enskild nämnd eller bolagsstyrelse personuppgiftsansvarig och ansvarar därigenom för att dess personuppgiftsbehandlingar utförs i enlighet med dataskyddsförordningens bestämmelser.

I samband med att förordningen trädde i kraft 2018 tilldelades varje verksamhet i Staden ett dataskyddsombud. Stadens dataskyddsombud har till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos samtliga personuppgiftsansvariga förvaltningar och bolag.

Som en del i arbetet med att informera personuppgiftsansvariga sammanställer dataskyddsombudet årligen en rapport där dataskyddsarbetet sammanfattas. Årsrapporten syftar till att ge personuppgiftsansvariga en överblick över verksamhetens personuppgiftshantering.

I början av året sändes en årsplan över till verksamheten med syfte att klargöra dataskyddsombudets roll och förtydliga hur det kommande arbetet är planerat. Denna årsrapport har därmed årsplaneringen som utgångspunkt.

1.2 Granskningsperiod

Årsrapporten avser tidsperioden från januari 2020 till december 2020.

1.3 Dataskyddsombudets roll

Dataskyddsombudets roll är att övervaka personuppgiftsansvariges efterlevnad av dataskyddsförordningen. Det innebär bland annat att dataskyddsombudet ska granska hur personuppgiftsansvarige behandlar personuppgifter, kontrollerar att bestämmelser och interna styrdokument följs, informerar och ger råd till organisationen. Utöver det ska dataskyddsombudet även ge råd om konsekvensbedömningar, vara kontaktperson för Datainspektionen, registrerade och dataskyddskontakterna samt samarbeta med Datainspektionen vid till exempelvis inspektioner. Dataskyddsombudet är oberoende gentemot personuppgiftsansvarige och får inte instrueras hur jobbet som dataskyddsombud ska utföras. Dataskyddsombudets roll och uppgifter är reglerade i artiklarna 37, 38 och 39 i Dataskyddsförordningen.

2 Efterlevnad

2.1 Information och rådgivning

Dataskyddsombudets roll är att ge råd till den personuppgiftsansvarige. Råd kan antingen ges efter att dataskyddskontakten eller andra inom verksamheten ställt en fråga, när dataskyddsombudet deltar vid konsekvensbedömning eller vid avstämningsmöten. Under året har dataskyddsombudet mottagit flertalet frågor ifrån verksamheten utifrån dess personuppgiftsbehandlingar. Frågorna har bland annat handlat om känsliga personuppgifter, personuppgiftsbiträdesrelationer, samt ny integritetspolicy. Dataskyddsombudet har genomfört en utbildning inom dataskydd för anställda under hösten 2020. Därtill har även nyhetsbrev skickats ut innehållande omvärldsbevakning och information gällande specifika frågor/ämnen.

2.2 Granskning och kontroll

Dataskyddsombudets ska övervaka personuppgiftsansvariges efterlevnad av dataskyddsförordningen. Övervakning kan ske på olika sätt, antingen genom mer formella granskningar där rapporter skrivs och skickas till verksamheten och presenteras för högsta förvaltningsledningen, eller genom att dataskyddsombudet kontrollerar olika handlingar eller rutiner och återkopplar direkt till dataskyddskontakten för eventuella åtgärder.

Kontroller har gjorts av den information som skickats till dataskyddsombudet ifrån dataskyddskontakten eller funnits tillgänglig för läsning någon annan stans. Även rutiner, mallar och andra tillhörande dokument har granskats.

2.2.1 Granskningsområden

De områden som har granskats under perioden är baserade på årsplanen som fastställts av dataskyddsombudet. För dataskyddsarbetet under 2020 lyftes fem punkter som skulle granskas särskilt. Planen för 2020 innehöll följande granskningspunkter: integritetspolicy, kvalitetskontroll av befintliga personuppgifter, rutiner för notifiering av personuppgiftsincidenter, personuppgiftsbiträden och personuppgiftsbiträdesavtalen samt kunskapsnivån hos medarbetarna.

2.2.1.1 Integritetspolicy

Dataskyddsombudet har tillsammans med verksamheten arbetat för att ta fram en ny integritetspolicy anpassad för verksamheten.

2.2.1.2 Kvalitetskontroll av befintliga personuppgifter

Dataskyddsombudet har påbörjat en granskning av verksamhetens registrerade personuppgiftsbehandlingar i personuppgiftsregistret. Fokus har varit på de

behandlingar som har samtycke som rättslig grund. På grund av tidsbrist kommer denna granskning redovisas för verksamheten i början av 2021 och eventuella åtgärder vidtagas av verksamheten då. Granskningen handlar om huruvida samtycke är lämplig rättslig grund för den aktuella behandlingen. Under 2021 kommer dataskyddsombudet fortsätta att fokusera på samtycke som rättslig grund och diskutera detta med verksamheten.

2.2.1.3 Rutiner för notifiering av personuppgiftsincidenter

Dataskyddsombudet har utfört en skrivbordstillsyn av verksamhetens hantering av personuppgiftsincidenter. Granskning har gjorts på rutiner och tillhörande dokument. En rapport har skrivits och tillsänts verksamhetens dataskyddskontakter. Dataskyddsombudet lämnade följande rekommendationer:

Rutinerna behöver kompletteras ytterligare med hänsyn till den korta tidsfrist som dataskyddsförordningen medger vid en inträffad incident. Bolaget bör fundera på hur informationen om en inträffad incident från de som upptäcker incidenten, på ett mer skyndsamt sätt kan nå fram till de som ansvarar för bedömningen av en personuppgiftsincident. För detta krävs att personalen har kompetens nog att kunna identifiera en uppkommen personuppgiftsincident varför utbildningsinsatser inom det angivna området är direkt avgörande. Vidare bör bolaget se över hur kommunikation gällande rutinen sker och säkerställa så att ändringar och uppdateringar kommuniceras ut till alla anställda. Utöver den utbildning som sker med hjälp av dataskyddsombudet under hösten bör bolaget även framgent anta en handlingsplan för uppföljning och vidareutbildning av personalen.

Göta Lejon behöver även se över rutinerna kring hur bolagets personuppgiftsbiträden sköter kommunikationen med Göta Lejon som personuppgiftsansvariga och att det vid inträffade incidenter anmäls till bolaget ett skyndsamt sätt.

Det finns också behov av att se över formuleringarna gällande dataskyddsombudets roll vid en personuppgiftsincident och förtydliga att dataskyddsombudet alltid ska kontaktas vid misstänt och inträffad incident. Även formuleringen gällande vilka typer av incidenter som ska anmälas bör förtydligas med att det är när risk föreligger som anmälan ska ske. Rutinen behöver också förtydligas med att de registrerade ska informeras utan onödigt dröjsmål om hög risk för deras fri- och rättigheter föreligger. Vidare rekommenderas också bolaget att dokumentera sina personuppgiftsincidenter i ett separat dokument.

2.2.1.4 Personuppgiftsbiträden och personuppgiftsbiträdesavtalen

På grund av corona-pandemin har dataskyddsombudet inte kunnat granska verksamhetens personuppgiftsbiträden och tillhörande biträdesavtal. Detta kommer istället göras under kommande år.

2.2.1.5 Kunskapsnivån hos medarbetarna

Den planerade enkäten för att undersöka medarbetarnas kunskapsnivå kunde på grund av den rådande situationen med corona-pandemin sändas ut, därför har dataskyddsombudet inte kunnat bedöma kunskapsnivån gällande dataskydd hos verksamheten.

Däremot har dataskyddsombudet utfört en grundläggande utbildning för verksamheten för att säkerställa att medarbetarna har en grundläggande kunskap om dataskydd. En uppföljning av medarbetarnas kunskapsnivå bör göras varje år och även en plan för hur verksamheten ska säkerställa att behovet tillgodoses.

2.3 Sammantagen bedömning

Verksamheten har fått information och råd av dataskyddsombudet löpande under året. Granskningsarbetet har skett utifrån ett antal punkter och utbildning har givits av dataskyddsombudet. Medvetenheten hos medarbetarna är god och bör fortsättningsvis hållas ständigt uppdaterad.

3 Framåt

Dataskyddsombudet kommer fortlöpande bistå verksamheten med information och råd, även om det är verksamheten som är ytterst ansvarig för att hålla sig informerade inom dataskyddsfrågorna. Med hjälp av löpande avstämningsmöten med dataskyddsombudet kan viktiga dataskyddsfrågor lyftas och hanteras innan det uppstår problem.

Att fortsätta utbilda personalen är viktigt, då den mänskliga faktorn är den största orsaken till att en organisation behandlar personuppgifter på ett felaktigt sätt. Genom regelbunden utbildning och uppföljning av medarbetarnas kunskap minskar verksamheten riskerna för att personuppgifter behandlas felaktigt.

Under kommande år kommer dataskyddsarbetet utgå ifrån en årsplanering, som kommer tillsändas verksamheten i början på 2021. Fördjupande granskningar kommer att utföras likväl som mindre kontrollpunkter som kommer ske löpande. Mer information kommer att lämnas till verksamheten när årsplaneringen är fastställd.

Granskning av verksamhetens rutiner för personuppgiftsincidenter

1. Inledning

Den övergripande och viktigaste uppgiften för stadens dataskyddsombud är att övervaka att personuppgiftsansvariga förvaltningar och bolag följer dataskyddsförordningen. Det innebär bland annat att dataskyddsombudet samlar in information om hur organisationen behandlar personuppgifter, kontrollerar att organisationen följer bestämmelser och interna styrdokument samt att dataskyddsombudet informerar och ger rådgivning om dataskyddsfrågor. Som ett led i detta arbete kommer därför periodiska granskningar och uppföljningar att genomföras. En grundläggande förutsättning för att detta ska vara möjligt är att den personuppgiftsansvarige bedriver ett eget förbättringsarbete inom dataskydd som kan granskas och följas upp.

2. Syftet med granskningen

Dataskyddsombudet har med stöd av dataskyddsförordningens art. 39.1 (b) beslutat att inleda en granskning som syftar till att kartlägga, utvärdera och förbättra verksamheternas rutiner och hantering av personuppgiftsincidenter. Det är av stor vikt att den personuppgiftsansvarige verksamheten i god tid skapar tydliga rutiner för att upptäcka och åtgärda personuppgiftsincidenter. En handlingsplan bör därför ha upprättats för de fall där en personuppgiftsincident inträffar så att den personuppgiftsansvarige snabbt kan agera enligt gällande lagstiftning.

3. Metod och tidsplan

I syfte att kartlägga hur verksamheterna har arbetat med detta efterfrågar dataskyddsombudet svar på ett antal frågor som rör rutiner kring hanteringen av personuppgiftsincidenter. Utskicket kommer att sändas till respektive verksamhets dataskyddskontakt samt förvaltningsbrevlåda och bör besvaras av den eller de personer som är mest insatta inom organisationens dataskyddsfrågor. Granskningen kommer således att genomföras som en skrivbordstillsyn. Besvara gärna frågorna så utförligt och detaljerat som möjligt. Framtagna rutiner och dokument skall bifogas tillsammans med svaren.

Utskicket av dessa frågor kommer att ske den 25 augusti 2020. Svaren skall ha inkommit till dataskyddsombudet senast den 25 september 2020. Därefter kommer resultatet att utvärderas och sammanställas av dataskyddsombudet som avstämmer utkastet tillsammans med verksamhetens dataskyddskontakt. Verksamheten har under en veckas tid möjlighet att klargöra eventuella faktafel och oklarheter i rapporten.

Slutligen återkopplas resultatet i form av en granskningsrapport senast vecka 43, dvs. i mitten av oktober, samt redogörs muntligt för nämnd eller styrelse i december.

Rutiner för personuppgiftsincidenter

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 25 september 2020.

1. Vilka rutiner har ni inom organisationen vid inträffande av en personuppgiftsincident?
Organisatoriska åtgärder: • inte skriva upp lösenord. Använda lösenord med specialtecken. • logga ut eller låsa datorn när man lämnar arbetsstationen. • inte använda gemensam användaridentitet. • inte ha bildskärmen vänd så att obehöriga kan läsa informationen. • inte dela med sig information till någon annan utan att vara säker på att den personen är behörig att få ta del av informationen. • inte skriva ut känslig information på en skrivare som obehöriga har eller lätt kan skaffa sig tillgång till. • inte lämna känslig information på skrivbord eller vid arbetsstationen. GDPR och säkerhetsutbildning av personal som hanterar personuppgifter. Interna riktlinjer om hantering av personuppgifter, e-post, gallring samt rapportering av incidenter. Konsekvensbedömning (DPIA) innan ny personuppgiftsbehandling påbörjas. Biträdesavtal och sekretessavtal med samarbetspartners och ingen överföring till tredje land. **Tekniska åtgärder:** **Behörighetskontroll** Autentisering med personliga användaridentiteter och behörighetskontroll för att styra åtkomst till personuppgifter samt rutiner för att tilldela och ta bort behörigheter. Tilldelning av behörigheter begränsas till de personer som behöver uppgifterna för sitt arbete. **Säkerhetskopiering** Regelbunden säkerhetskopiering av kritisk data **Datakommunikation** Känsliga personuppgifter som överförs via öppna nätverk skyddas mot förvanskning och obehörig åtkomst genom pseudonymisering och eller kryptering. För att separera Tjänsten från publika nätverk används brandvägg. **Skydd mot skadliga program**

IT-system skyddas mot skadliga program som exempelvis virus.

Utplåning

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska

användas för sitt ändamål förstörs de på ett sådant sätt att uppgifterna inte kan återskapas.

Uppdatering

Regelbundna säkerhetsuppdateringar av program och systemkomponenter.

Privacy by Design.

Vid utveckling av produkter och tjänster ska principer för design och utformning beaktas (riskbedömas) med hänsyn tas till integritetsskydd. Detta innebär att skydd för personuppgifter ska ingå i processens samtliga faser, från kravinsamling via utformning av arbetsprocesser eller IT-systems gränssnitt till avveckling.

Privacy by Default. System och tjänster där behandling av personuppgifter sker, ska i standardfallet vara inställda för att säkerställa att inte fler personuppgifter görs tillgängliga för användare än vad som behövs för det specifika ändamålet med behandlingen. Detta inkluderar begränsning av åtkomst till personuppgifter baserat på syftet med den behandling som sker i systemet/tjänsten.

2. Vilka inom organisationen är utsedda för att ansvara för just personuppgiftsincidenter? Vem informerar och är kontaktperson gentemot tillsynsmyndigheten?

Personuppgiftsansvarig inom Göta Lejon är Katrin Gundersen
katrin.gundersen@gotalejon.goteborg.se

Katrin kontaktar DSO för vidare utredning och samverkan innan eventuell anmälan till DI.

3. På vilket sätt bedömer ni riskerna för personer som har drabbats av en personuppgiftsincident?

Finns dokumenterat i instruktionen för personuppgiftsincident

Denna instruktion är upplagd som en steg-för-steg-instruktion där svaret på respektive fråga hänvisar dig vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver efterföljande frågeställningar inte besvaras.

Stödjande dokument:
Dokumentation från genomgång av denna instruktion sker i följande bilagor:

- *Bilaga A – Dokumentation över Personuppgiftsincident*
- *Bilaga B - Anmälan till Integritetskyddsmyndigheten, DI*
- *Bilaga C – Information till den registrerade*

Riskbedömning vid personuppgiftsincident:

Typ av incident (Art):

Kategorier av registrerade som kan komma att beröras:

Ungefärligt antal personer som berörs:

Ungefärligt antal personuppgifter:

Sannolika konsekvenser av personuppgiftsincidenten:

Följande åtgärder har vidtagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter):

Följande åtgärder har föreslagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter):

Namn och kontaktuppgifter för dataskyddsombud eller annan kontakt som kan erbjuda mer information

4. Hur bedömer ni om en incident skall rapporteras till tillsynsmyndigheten?
Steg 1, Finns dokumenterat i instruktionen för personuppgiftsincident Denna instruktion är upplagd som en steg-för-steg-instruktion där svaret på respektive fråga hänvisar dig vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver efterföljande frågeställningar inte besvaras. **Riskbedömning vid personuppgiftsincident:** Typ av incident (Art): Kategorier av registrerade som kan komma att beröras: Ungefärligt antal personer som berörs: Ungefärligt antal personuppgifter: Sannolika konsekvenser av personuppgiftsincidenten: Följande åtgärder har vidtagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter): Följande åtgärder har föreslagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter): **Steg 2,** kontakta DSO för samverkan innan eventuell anmälan till DI.

5. Dokumenterar ni samtliga incidenter, även de som inte inrapporteras till tillsynsmyndigheten?
Göta Lejon för logg över alla incidenter

6. Vilken utbildning har personalen fått för att kunna hantera uppkomna personuppgiftsincidenter?
- Utbildning för ledning och personal- GDPR i arbetsvardagen 2018 - Nyhetsbrev sporadiskt

Instruktion för Personuppgiftsincident

Syfte

En personuppgiftsincident såsom dataläckage eller dataintrång ska av personuppgiftsansvarig anmälas till Datainspektionen utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha personuppgiftsansvarige fått vetskap om det inträffade.

Denna instruktion har till syfte att beskriva hur en personuppgiftsincident ska hanteras på Försäkrings AB Göta Lejon. Genom en gemensam instruktion för hantering kan bolaget upprätthålla en enhetlig och effektiv behandling av dessa frågor.

Instruktionen riktar sig till samtliga medarbetare på bolaget med fokus på de roller som kan komma i kontakt med personuppgiftsincidenter, samt dataskyddskontakten.

Instruktionens utformning

Denna instruktion är upplagd som en steg-för-steg-instruktion där svaret på respektive fråga hänvisar dig vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver man inte besvara de efterföljande frågeställningarna.

Utförande roller

Följande roller är primära utförare:

- Incident koordinator (Dataskyddskontakt, alternativt ansvarig/utförare för den tilltänkta hanteringen)

Stödjande

Dataskyddsombud

IT

PUB

Stödjande dokument

Dokumentation från genomgång av denna instruktion sker i följande bilagor:

- *Bilaga A – Dokumentation över Personuppgiftsincident*

- *Bilaga B - Anmälan till Datainspektionen*
- *Bilaga C – Information till den registrerade*

I instruktionen står vilken eller vilka bilagor som blir relevanta för den aktuella situationen.

Instruktion:

1) Dataskyddskontakt besvarar om en personuppgiftsincident där bolaget är **personuppgiftsansvarig** eller **personuppgiftsbiträde** har skett?

Kommentar: En personuppgiftsincident kan definieras som en säkerhetsincident rörande personuppgifter, som leder till att personuppgifter kommer i orätta händer, förloras eller uppdateras felaktigt. T.ex. dataintrång eller oavsiktlig förlust av personuppgifter på grund av tekniska problem.

Nästa steg	
Om svaret är ja	Om ja och **personuppgiftsansvarig**: Gå vidare till fråga 2) Om ja och **personuppgiftsbiträde**: Notifiera omedelbart personuppgiftsansvariges Dataskyddsombud och uppdatera personuppgiftsansvarig kontinuerligt med mer information om incidenten när den blir känd. Informationen bör innehålla motsvarande information i bilaga B).
Om svaret är nej	Ingen ytterligare åtgärd krävs
Om osäker	Kontakta Dataskyddsombud dso@intraservice.goteborg.se

2) Rapportör underrättar bolagets Dataskyddsombud om personuppgiftsincidentens art, samt
   a) Om möjligt, kategorier av och ungefärligt antal registrerade som berörs samt kategorier av och ungefärligt antal personuppgiftsposter som berörs
   b) Sannolika konsekvenser
   c) Åtgärder som vidtagits och/eller föreslagits för att minska risken för negativ effekt

Nästa steg	
Efter att dataskyddsombudet fått informationen	Dataskyddsombudet tar emot informationen och utvärderar denna, bedömer eventuellt osäkra fall samt besvarar eventuella frågor

3) Dataskyddskontakt besvarar följande frågeställning (och rådgör vid behov med berörd registeransvarig/rapportör):
   a) Är det **osannolikt** att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter? (Se separat dokument om instruktion för konsekvensanalys, för riktlinjer om hot/händelser/risk att förhålla sig till.)

Nästa steg	
Om svaret är ja	Dokumentera personuppgiftsincident enligt bilaga A. Ingen ytterligare åtgärd krävs därefter.
Om svaret är nej	Skicka en anmälan om personuppgiftsincident till behörig tillsynsmyndighet utan onödigt dröjsmål, inom 72 timmar. För det fall att anmälan inte gjorts inom 72 timmar måste detta åtföljas av en motivering till förseningen. För anmälan, se bilaga B. Gå sedan vidare till fråga 4). *Kommentar: Behörig tillsynsmyndighet i Sverige är Integritetsskyddsmyndigheten. Om incident påverkar registrerade i andra länder än Sverige ska myndighet i dessa länder kontaktas.*

4) Dataskyddskontakt besvarar vidare följande frågeställningar:
   a) Leder personuppgiftsincidenten sannolikt till en hög risk för fysiska personers rättigheter och friheter? (se separat dokument om instruktion för konsekvensanalys, för riktlinjer om hot/händelser/risk att förhålla sig mot)

Nästa steg	
Om svaret är ja på a)	Gå vidare till fråga 5)
Om svaret är nej på a)	Dokumentera personuppgiftsincident enligt bilaga A). Ingen ytterligare åtgärd krävs.

5) Är något av följande kriterier uppfyllda?
   a) Försäkrings AB Göta Lejon har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de

personuppgifter som påverkades av personuppgiftsincidenten? (Särskilt åtgärder som ska göra uppgifter oläsbara för alla personer som inte ska få tillgång till personuppgifterna, som kryptering.)

b) Försäkrings AB Göta Lejon har tagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses inte längre kommer att uppstå?

c) Det skulle innebära en oproportionell ansträngning att informera de berörda registrerade om incidenten.

Nästa steg	
Om svaret är ja på punkt a) eller b)	Dokumentera personuppgiftsincident enligt bilaga A). Ingen ytterligare åtgärd krävs.
Om svaret är ja på punkt c)	Allmänheten ska informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt som om allmänheten informerats. Använda bilaga C) som mall för vilken information som ska lämnas. Dokumentera sedan personuppgiftsincident enligt bilaga A). *Kommentar: Vid användning av bilaga C) bör Dataskyddsombud stämma av med* ***Kommunikationsavdelningen****. Kvalitativt innehåll får dock inte ändras.*
Om svaret är nej	Informera de personer som kan beröras av personuppgiftsincidenten, se bilaga C). Dokumentera sedan personuppgiftsincident enligt bilaga A). *Kommentar: Vid användning av bilaga C) bör Dataskyddsombud stämma av med* ***Kommunikationsavdelningen****. Kvalitativt innehåll får dock inte ändras.*

Bilaga A – Dokumentation över Personuppgiftsincident

Enligt GDPR art. 33.5 ska varje personuppgiftsincident dokumenteras, i syfte att göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av anmälningsskyldigheten.

Rubrikerna nedan anger vilken information som är obligatorisk att dokumentera enligt GDPR art. 33.

Omständigheterna kring incidenten:

Incidentens potentiella effekter:

Korrigerande åtgärder som vidtagits, inklusive motivering av varför just dessa åtgärder har tagits och hur de korrigerar incidenten:

Bilaga B – Anmälan av personuppgiftsincident till Integritetsskyddsmyndigheten

[Rubrikerna nedan anger – förutom där annat särskilt framgår – vilken information som är obligatorisk enl. GDPR art. 33]

Typ av incident (Art):

Kategorier av registrerade som kan komma att beröras:

[anges om så är möjligt]

Ungefärligt antal personer som berörs:

[anges om så är möjligt]

Ungefärligt antal personuppgifter:

[anges om så är möjligt]

Sannolika konsekvenser av personuppgiftsincidenten:

Följande åtgärder har vidtagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter):

Följande åtgärder har föreslagits för att åtgärda personuppgiftsincidenten (inklusive eventuella åtgärder för att minska incidentens potentiella negativa effekter):

Namn och kontaktuppgifter för dataskyddsombud eller annan kontakt som kan erbjuda mer information:

Bilaga C – Information till den registrerade

[Texten nedan utgörs av förslag till formuleringar. Se kommentarer avseende vilka delar som är obligatoriska (enl. GDPR art. 34).]

Meddelande om personuppgiftsincident

Det har nyligen skett en säkerhetsincident gällande personuppgifter som rör Försäkrings AB Göta Lejon. Vi vill se till att du har den information du behöver om det som har hänt, om vilka uppgifter det rör sig om och om de steg vi tar för att skydda dig.

Vad har hänt? [Beskrivning av personuppgiftsincidentens art är obligatorisk]

Den (DATUM) (MÅNAD) (ÅR) fick vi kännedom om att (BESKRIV INCIDENTENS ART OCH OMSTÄNDIGHETER RUNT DENNA).

Vi vidtog omedelbart åtgärder, och (BESKRIV VILKA ÅTGÄRDER SOM TAGITS). De typer av kunder som blivit påverkade är (NÄMN KUNDTYPERNA) och detta är på grund av (NÄMN VARFÖR JUST DESSA BLIVIT PÅVERKADE).

Vilka personuppgifter handlar det om?

(NÄMN DE PERSONUPPGIFTER SOM DET HANDLAR OM + EVENTUELL FÖRKLARING OM NÅGON UPPGIFT BEHÖVER FÖRKLARAS)

Vad är de sannolika konsekvenserna av det inträffade? [Obligatoriskt]

(BESKRIV DE SANNOLIKA KONSEKVENSERNA AV DET INTRÄFFADE)

Vad gör Försäkrings AB Göta Lejon? [Obligatoriskt]

(NÄMN DE ÅTGÄRDER SOM MAN TAGIT ELLER FÖRESLAGIT FÖR ATT ÅTGÄRDA INCIDENTEN/MINSKA DEN NEGATIVA EFFEKTEN, SAMT VAD MAN GÖR GENERELLT FÖR ATT FÖRHINDRA ATT NÅGONTING LIKNANDE SKER I FRAMTIDEN, GE EXEMPEL PÅ BÅDA)

Vad kan du göra?

(GE EXEMPEL PÅ VAD DEN ENSKILDE KAN GÖRA, T.EX.: Försäkrings AB Göta Lejon jobbar hårt för att säkerställa att alla information om våra kunder hålls säker. På bolaget gör vi allt vi kan, och föreslår också att du XXXXXXX)

Kontaktuppgifter till dataskyddsombud [obligatoriskt]

Om du har frågor relaterade till detta är du välkommen att höra av dig till vårt Dataskyddsombud: Abtin Kronold, dso@intraservice.goteborg.se. eller bolagets dataskyddskontakt Katrin Gundersen, katrin.gundersen@gotalejon.goteborg.se. Du kan även läsa mer om vårt arbete med personuppgiftsskydd på goteborg.se.

Förfrågningar beträffande personuppgiftshantering/incidenthantering
2018-2020

Namn	Adress	Inkommen datum	Besvarad datum	Personnummer	Kommentar	Åtgärd
Nils Jackie Senor	jean.de-gothia@outlook.com	2018-11-19.	2018-12-14.	740123-5176	Inga handlingar/personuppgifter finns på denna person i våra system. Personen har ej styrkt sin identitet.	Besvarat begäran. Svar skickat till diariet.
Mischenia Fritzsche och Dennis Fritzsche	Byälvsvägen 241, 128 47 Bagarmossen	2019-08-05	2019-08-05	880226-0185 810505-3337	Inga handlingar/personuppgifter finns på denna person i våra system. Personen har ej styrkt sin identitet.	Besvarat begäran. Svar skickat till diariet. Brevet har skickats rekommenderat till folkbokföringsadress.
Katrin Gundersen	Katrin.gundersen@gotalejon.goteborg.se	2019-09-17	2019-09-17	1 individ med namn och e-postadress	Återkallning av mailet försöktes men misslyckades pga mailet redan var läst	Ingen anmälan till Datainspektionen då det är den mänskliga faktorn hos Intraservice (PUB). Det är osannolikt att individens fri och rättigheter riskeras.
Fahran Öznur	yenice_88@hotmail.com	2020-09-23	2020-09-24	Namn, mailadress, telefonnummer, personnummer, skadenummer samt beskrivning av skadehändelsen.	Mail skickades fel och person som fick mailet kontaktade Crawford för att informera om detta. Konsekvensanalys har gjorts på Göta Lejon och skadelidande har informerats. Regelefterlevnadsfunktionen gör bedömningen att det inte behöver anmälas till Dataskyddsinspektionen utan endast till DO i Staden.	Ingen anmälan till Datainspektionen då det är den mänskliga faktorn hos Crawford (PUB). Det är osannolikt att individens fri och rättigheter riskeras.

Göteborgs Stad

Rutiner vid personuppgiftsincidenter

Granskningsrapport för Försäkrings AB Göta Lejon

2020-12-21

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-12-01	1	Utkast för granskning av DSK	Andréa Bergqvist
2020-12-21	2	Slutgiltig version efter kommentarer ifrån DSK	Andréa Bergqvist

Innehåll

1 Inledning

1.1 Bakgrund

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Personuppgiftsansvariga verksamheter och personuppgiftsbiträden ska sträva efter att arbeta medvetet och proaktivt för att undvika personuppgiftsincidenter. Ansvarsskyldigheten i artikel 5.2 dataskyddsförordningen ålägger den personuppgiftsansvarige verksamheten att se till att de personuppgifter som behandlas inom ramen för verksamheten utförs i enlighet med dataskyddsförordningens bestämmelser. Inom Göteborgs stad är det varje enskild nämnd eller bolagsstyrelse som är personuppgiftsansvarig och således ansvarig för att verksamheten har god och regelriktig följsamhet mot dataskyddsförordningen.

Det är av stor vikt att verksamheten i god tid har skapat tydliga rutiner för att upptäcka personuppgiftsincidenter. En komplett och metodisk handlingsplan ska ha upprättats för de fall en personuppgiftsincident inträffar så att verksamheten snabbt kan och vet hur den ska agera. De uppmuntras därför att i god tid planera och införa processer för att skyndsamt kunna begränsa en incident, bedöma riskerna för enskilda och därefter avgöra om det är nödvändigt att anmäla incidenten till tillsynsmyndigheten. Vid behov ska även den drabbade registrerade informeras om inträffad incident. Anmälan till tillsynsmyndigheten bör utgöra en del av incidenthanteringsplanen.

Den övergripande och viktigaste uppgiften för stadens dataskyddsombud är att övervaka att personuppgiftsansvariga förvaltningar och bolag följer dataskyddsförordningen. Det innebär bland annat att dataskyddsombudet samlar in information om hur organisationen behandlar personuppgifter, kontrollerar att organisationen följer bestämmelser och interna styrdokument samt att dataskyddsombudet informerar och ger rådgivning om dataskyddsfrågor. Som ett led i detta arbete kommer därför periodiska granskningar och uppföljningar att genomföras. En grundläggande förutsättning för att detta ska vara möjligt är att den personuppgiftsansvarige bedriver ett eget förbättringsarbete inom dataskydd som kan granskas och följas upp. Vad gäller personuppgiftsincidenter ska den personuppgiftsansvarige verksamheten omedelbart efter inträffandet av en personuppgiftsincident eller annan incident kontakta dataskyddsombudet för att konsultera tillvägagångssätt, enligt Artikel 29-arbetsgruppen för skydd av personuppgifter och dess vägledning gällande ”Riktlinjer om dataskyddsombud”.

1.2 Granskningens utförande

1.2.1 Granskningsområdet

Granskningsområdet för denna rapport är verksamhetens rutiner och processer för personuppgiftsincidenter.

1.2.2 Syfte

Granskningens syfte är att säkerställa att verksamheten har arbetat med att ta fram fungerande rutiner för hanteringen av personuppgiftsincidenter, att personalen inom verksamheten är väl insatta i hur de ska agera vid inträffad incident och att verksamheten vid en inträffad incident är införstådd med de skyldigheter som åligger dem enligt dataskyddsförordningen. Syftet är också att se över vilka delar av rutinen som kräver förbättringsarbete framgent.

1.2.3 Tillvägagångssätt

Granskningen utförs i form av en skrivbordstillsyn där den personuppgiftsansvarige verksamheten har beretts tillfälle att inkomma med all nödvändig dokumentation som rör hanteringen av personuppgiftsincidenter. Metoden består av att dokumentgranska verksamhetens rutiner, processer och handlingsplan, samt att genom ett frågeställningsutskick få svar på ett antal grundläggande frågor som rör verksamhetens rutiner vid personuppgiftsincidenter.

1.2.4 Bilagor

Bilaga 1	Information om granskningen
Bilaga 2	Svar på frågeformuläret
Bilaga 3	Instruktion för Personuppgiftsincident
Bilaga 4	Register personuppgiftsincidenter

2 Tillämplig lagstiftning

2.1 Definitionen av en personuppgiftsincident

Det är viktigt att den personuppgiftsansvarige verksamheten kan fastställa vad en personuppgiftsincident är. Enligt artikel 4.12 dataskyddsförordningen definieras en personuppgiftsincident på följande sätt:

”En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Enligt dataskyddsförordningen har en personuppgiftsincident inträffat om personuppgifter på ett oavsiktligt eller olagligt sätt har förstörts, förlorats, ändrats eller röjts till någon obehörig. Det är varje personuppgiftsansvariges skyldighet att dels kunna identifiera en incident, dels agera korrekt och lagenligt när detta inträffar.

2.2 Den personuppgiftsansvariges skyldigheter

2.2.1 Ansvarsskyldighet

Den personuppgiftsansvarige verksamhetens ansvarsskyldighet regleras i artikel 5.2 och artikel 24 dataskyddsförordningen. Det är inte längre tillräckligt att enbart följa lagen utan den som är ansvarig för personuppgiftsbehandlingen måste också kunna visa hur och på vilket sätt man följer bestämmelserna i dataskyddsförordningen, bland annat genom att beakta risker för fysiska personers rättigheter och friheter. Detta kan verksamheten göra genom att visa att det finns tydliga rutiner för personuppgiftsincidenter, en upprättad handlingsplan samt dokumentation av samtliga inträffade incidenter. Dessa ska kontinuerligt ses över och uppdateras vid behov.

Dataskyddsförordningen ställer krav på att personuppgifter, med användning av lämpliga tekniska och organisatoriska åtgärder, ska behandlas på ett sätt som säkerställer kvalificerad säkerhet för personuppgifterna. Dessutom måste alla lämpliga tekniska skyddsåtgärder och organisatoriska åtgärder ha vidtagits för att omedelbart fastställa om en incident har ägt rum för att därefter kunna avgöra om rapporteringsskyldigheten ska fullgöras, enligt beaktandeskäl 87 i dataskyddsförordningen.

2.2.2 Rapporteringsskyldighet

Enligt artikel 33 dataskyddsförordningen ska den personuppgiftsansvarige utan onödigt dröjsmål inte senare än 72 timmar efter att ha fått vetskap om personuppgiftsincidenten, anmäla den till Datainspektionen i enlighet med ansvarsprincipen, såvida det inte är osannolikt att incidenten medför ***en risk*** för fysiska personers rättigheter och friheter. Den personuppgiftsansvarige ska därmed undersöka incidentens allvarlighet och väsentlighet. Det är omständigheterna i det enskilda fallet som avgör huruvida det är nödvändigt att anmäla incidenten till tillsynsmyndigheten och underrätta de personer som påverkas. Den personuppgiftsansvarige måste bedöma sannolikheten för i vilken grad den uppkomna incidenten påverkar fysiska personers rättigheter och friheter.

De konsekvenser som kan uppstå är fysisk, materiell eller immateriell skada enligt beaktandeskäl 85 i dataskyddsförordningen. Det kan exempelvis handla om identitetsstöld, ekonomisk förlust och diskriminering. Datainspektionen kan utöva sina tillsynsbefogenheter för att se till att den personuppgiftsansvarige de facto har vidtagit lämpliga och nödvändiga åtgärder.

2.2.3 Informationsplikt

Den personuppgiftsansvarige verksamheten har en informationsplikt gentemot den registrerade som har utsatts för incidenten, så att den enskilde kan vidta nödvändiga försiktighetsåtgärder. Informationsplikten gäller när en personuppgiftsincident sannolikt kommer att medföra ***en hög risk*** för den registrerades rättigheter och friheter, enligt artikel 34 och skäl 86 i dataskyddsförordningen. Personuppgiftsansvarig ska i underrättelsen beskriva incidentens art samt ge en rekommendation till den drabbade om hur de potentiellt negativa effekterna kan mildras. Underrättelsen ska ske så snart det rimligtvis är möjligt.

2.2.4 Dokumentationsskyldigheten

Den personuppgiftsansvarige verksamheten har en skyldighet enligt artikel 33.5 dataskyddsförordningen att dokumentera samtliga inträffade incidenter oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska också innefatta omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska kunna uppvisas till tillsynsmyndigheten vid en eventuell granskning för kontroll av efterlevnad av artikel 33 i dataskyddsförordningen. En förutsättning för att tillsynsmyndigheten ska kunna följa upp en personuppgiftsincident baserat på dokumentation är att den är samlad och ger en rättvisande bild av händelseförloppet.

2.3 Konsekvenser om kraven inte efterlevs

Tillsynsmyndigheten kan besluta att en verksamhet som bryter mot reglerna i dataskyddsförordningen ska betala en administrativ sanktionsavgift. I Sverige uppgår sanktionsavgiften för myndigheter till högst 10 miljoner kronor för allvarligare överträdelser och högst 5 miljoner kronor för mindre allvarliga överträdelser. För bolag är den högsta avgiften 20 miljoner euro eller fyra procent av bolagets globala årsomsättning. Sanktionsavgiftens storlek baseras på vilken bestämmelse som överträdelsen gäller samt på omständigheter i det enskilda fallet. De faktorer som avgör allvarlighetsgraden av överträdelsen är hur stor skada som har skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig. Tillsynsmyndigheten ska enligt artikel 83 i dataskyddsförordningen se till att sanktionsavgiften är effektiv, proportionerlig och avskräckande, vilket medför att verksamhetens storlek har betydelse vid bedömningen.

Om den personuppgiftsansvarige har behandlat den enskildes personuppgifter i strid med dataskyddsförordningen på ett sätt som har orsakat materiell eller immateriell skada, kan den enskilde väcka skadeståndstalan i allmän domstol för att begära ersättning. Vad som utgör ett skäligt skadeståndsanspråk baseras

på vägledning från förarbeten till motsvarande bestämmelse i den tidigare gällande personuppgiftslagen och den rättspraxis som utvecklats kring den (se SOU 2017:39 s. 304 och rättsfallet NJA 2013 s. 1046).

3 Granskning av verksamheten

3.1 Verksamhetens rutiner vid personuppgiftsincidenter

Göta Lejon har redogjort för hur verksamheten hanterar personuppgifter genom att bifoga organisationens rutiner för personuppgiftsincidenter som har namnet ”Instruktion för personuppgiftsincident” samt dess tre bilagor som avser mer specifika rutiner kring dokumentation över personuppgiftsincidenter, anmälan till tillsynsmyndigheten och information till den registrerade. Göta Lejon har också besvarat frågeutskicket som har sänts ut till bolaget samt bifogat sitt register över personuppgiftsincidenter.

Bolagets rutiner för personuppgiftsincidenter är konstruerad som en steg-för-steg-instruktion. Målgruppen för rutinen är samtliga medarbetare på bolaget med fokus på de roller som kommer i kontakt med personuppgiftsbehandling samt dataskyddskontakten. Enligt rutinen är utsedd ansvarig hanterare för personuppgiftsincidenter bolagets dataskyddskontakt som är incidentkoordinator. Instruktionen är uppdelad utifrån ett personuppgiftsansvars- och personuppgiftsbiträdesroll där bolaget agerar olika utifrån vilken roll de innehar vid inträffad incident.

3.1.1 Identifiering av en incident

Vid inträffad incident är det av stor vikt att bolaget har en utbildad personalstyrka som har kompetens nog att kunna identifiera en personuppgiftsincident. Göta Lejon har svarat att personalen har fått en grundläggande utbildning i GDPR-frågor år 2018. Dataskyddsombudet har också tillsammans med dataskyddskontakten planerat in ett utbildningstillfälle under november 2020 där en allmän genomgång av personuppgiftsincidenter kommer att äga rum.

Göta Lejon redogör i sin instruktion för hur identifieringen av en personuppgiftsincident ska göras. Det är dataskyddskontakten tillika incidentkoordinatorn som avgör huruvida det är en personuppgiftsincident eller inte. I rutinen definieras en personuppgiftsincident som en säkerhetsincident rörande personuppgifter, som leder till att personuppgifter kommer i orätta händer, förloras eller uppdateras felaktigt. Det framgår också att incidentkoordinatorn vid osäkerhet ska kontakta dataskyddsombudet.

3.1.1.1 Analys

I bolagets rutiner definieras och exemplifieras vad en personuppgiftsincident är. Det ställs höga krav på att incidentkoordinatorn som har att avgöra huruvida en personuppgiftsincident har inträffat eller inte, har tillräckligt med kompetens inom området för att kunna göra fullgod bedömning av situationen och utifrån lagstiftningen. I synnerhet med tanke på att definitionen och exemplifieringen i rutinerna inte är uttömmande. Dataskyddsombudet ser det dock som positivt att det finns en strukturerad och genomtänkt mall som ska följas vid misstanke om inträffad incident. Det är också positivt att det framgår av rutinerna att dataskyddsombudet ska rådfrågas. Dock bör dataskyddsombudet kontaktas, inte bara vid osäkerhet vid identifieringen av incidenten, utan även vid misstanke om en inträffad incident. Detta är ett tillägg som bör göras i nuvarande instruktioner.

En incident behöver emellertid identifieras redan i ett tidigare skede innan det når incidentkoordinatorn. Det bör därför framgå av rutinerna hur övrig personal som arbetar med eller som hanterar personuppgifter ska gå tillväga för att anmäla incidenten till ansvarig koordinator. Det ska också framgå vilka nyckelpunkter de bör beakta i sitt dagliga arbete och som ska fungera som en varningsklocka för dem för att kunna identifiera en eventuell personuppgiftsincident. Instruktionerna för personuppgiftsincidenter tydliggör inte detta i dagsläget. För att minimera riskerna är det därför av stor vikt att personalen kompetensutvecklas inom det här området samt får information om vilka rutiner som finns på plats. Eftersom dataskyddsförordningen ställer höga krav på skyndsamhet i det här läget är det mycket viktigt att rutinerna inte bara är på plats, utan att de också är lättillgängliga för personalen och att de är införstådda med hur de ska gå tillväga för att anmäla incidenten så snart som möjligt till ansvarig incidentkoordinator.

Dataskyddsombudet ser det som positivt att bolaget efterfrågar utbildningsinsatser från Dataskyddsenheten och att dessa kommer att genomföras för samtlig personal på Göta Lejon under hösten. Därutöver rekommenderas att bolaget också på egen hand planerar in kontinuerliga utbildningar eller informationsträffar så att personalen håller sig à jour med bolagets rådande rutiner och instruktioner.

Bolaget har förgrenat instruktionen utifrån deras roll som dels personuppgiftsansvarig, dels personuppgiftsbiträde, vilket dataskyddsombudet ser som mycket positivt. En ytterligare aspekt som saknas i nuvarande rutiner och som bör tilläggas är hur bolagets personuppgiftsbiträden ska meddela bolaget vid inträffad personuppgiftsincident som sker hos biträdet. Hanteringen och ansvarsfördelningen av personuppgiftsincidenter är också något som bör framgå av respektive personuppgiftsbiträdesavtal.

3.1.2 Anmälan av en incident till tillsynsmyndigheten

Göta Lejon har i frågeutskicket svarat att bedömningen för huruvida en incident ska rapporteras till tillsynsmyndigheten finns i instruktionen för personuppgiftsincidenter. Riskbedömningen görs baserat på typ av incident,

kategorier av registrerade som kan komma att beröras, ungefärligt antal personer som berörs, ungefärligt antal personuppgifter och sannolika konsekvenser av personuppgiftsincidenten. Vidare utvärderas vilka åtgärder som har vidtagits och föreslagits för att åtgärda personuppgiftsincidenten samt minska dess potentiella effekt. Efter den här utvärderingen ska verksamhetens dataskyddsombud kontaktas för samråd kring en eventuell anmälan till tillsynsmyndigheten. Därefter görs bedömningen kring huruvida det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

I den bifogade rutinen med steg-för-steginstruktioner beskrivs i fråga 3 huruvida en incident ska anmälas till tillsynsmyndigheten. Då ska frågan om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter besvaras. Är svaret nej, ska anmälan skickas till tillsynsmyndigheten utan onödigt dröjsmål, inom 72 timmar.

3.1.2.1 Analys

Göta Lejon har i sin rutin korrekt angivit att en anmälan till tillsynsmyndigheten ska ske om det föreligger risk för att de registrerades rättigheter och friheter påverkas. I detta steg (steg 3) hänvisas också till separat konsekvensanalys för riktlinjer om hot/händelser/risk att förhålla sig till. Vilket dokument det är man hänvisar till här framkommer inte i det presenterade underlaget, varpå en bedömning av dokumentet inte går att göra. Däremot har bolaget i frågeunderlaget presenterat en riskbedömning som man uppger att man använder vid personuppgiftsincident. Riskbedömningen framkommer också i den presenterade rutinen, och genom att svara på olika frågor så kan ansvarig person därmed avgöra huruvida en risk föreligger. Dataskyddsombudet ser det som positivt att man har en tydlig rutin med ett tillvägagångssätt som ”tvingar” den som fyller i frågorna att göra en riskbedömning. Det är vidare positivt att man också ska ange åtgärder som har vidtagits och föreslås att vidta vid inträffandet av en incident. Slutligen har man också antagit en mall för anmälan till tillsynsmyndigheten med den information som ska uppges i enlighet med dataskyddsförordningen, vilket också underlättar för själva anmälan.

Under syfte för instruktion för personuppgiftsincident anges att ”en personuppgiftsincident såsom dataläckage eller dataintrång ska av personuppgiftsansvariga anmälas till Datainspektionen utan onödigt dröjsmål, och om så är möjligt, inte senare än 72 timmar efter att ha personuppgiftsansvarige fått vetskap om det inträffade”. Dataskyddsombudet vill uppmärksamma riskerna på att man under rubriken syfte exemplifierar två typer av incidenter som *ska* anmälas till tillsynsmyndigheten, när det är riskbedömningen vid inträffandet av en incident som är det väsentliga. Incident som medför **risk** för de registrerades fri- och rättigheter ska anmälas, oavsett vilken typ av incident det är. Om syftet kan formuleras om, minskar bolaget risken för att incidenter som ska anmälas på grund av att risk föreligger, missas på grund av att man tror att de inte ska anmälas på grund av att de inte är av de angivna typerna.

Vid frågan om vem som är kontaktperson gentemot tillsynsmyndigheten vid inträffad personuppgiftsincident bör Göta Lejon fastställa att det är dem som personuppgiftsansvariga som är kontaktpersoner och således även skyldiga att informera tillsynsmyndigheten när deras rapporteringsskyldighet aktualiseras. Göta Lejon har i frågeutskicket svarat att det är dataskyddskontakten som är personuppgiftsansvarig inom bolaget. Det är bolaget som är personuppgiftsansvarig och därmed styrelsen som har det yttersta ansvaret, inte en enskild medarbetare. Att dataskyddskontakten är utsedd för att hantera incidenter inom bolaget är däremot positivt. Dataskyddsombudet ska av den personuppgiftsansvarige kontaktas omedelbart vid misstanke om inträffad incident för rådgivning och stöttning kring hanteringen av personuppgiftsincidenten. Dataskyddsombudet finns också tillgänglig i de fall tillsynsmyndigheten vill kontakta denna, men är inte kontaktpersonen för inträffade personuppgiftsincidenter utan det ansvaret tillfaller verksamheten som är personuppgiftsansvarig. Dataskyddsombudet är inte heller den som ska utreda incidenten, utan det faller också på personuppgiftsansvarige. Därför bör bolaget i sin rutin förtydliga att den som inom bolaget är utsedd som ansvarig incidentkoordinator är den som ska ta emot informationen gällande incidenten, och incidentkoordinator bör rimligtvis därefter kontakta dataskyddsombudet.

3.1.3 Information och vägledning till den registrerade

I rutinen har Göta Lejon en fråga som undersöker huruvida det är sannolikt att personuppgiftsincidenten leder till en hög risk för fysiska personers rättigheter och friheter. Om svaret på frågan är ja, går man vidare till nästa steg. Steg 5 beskriver de undantag för när personuppgiftsansvarige inte måste meddela de registrerade. Om inget av undantagen är uppfyllda, ska de registrerade informeras. Information ges enligt en bilaga.

3.1.3.1 Analys

Dataskyddsombudet tycker det är positivt att Göta Lejon har en steg-för-stegrutin där man också förklarar undantagen för när informationsplikten gentemot de registrerade inte föreligger. Det är viktigt att komma ihåg att huvudregeln är att de ska informeras om **hög** risk föreligger. Därför ska en riskbedömning alltid göras i första ledet innan man tittar på undantagen. I rutinen hänvisas det återigen till en konsekvensanalys för riktlinjer om hot/händelser/risk att förhålla sig emot, som inte har presenterats som underlag för granskningen. Därmed kan dokumentet inte tas med i bedömningen. Däremot har man i frågeunderlaget presenterat den riskbedömning som görs vid en personuppgiftsincident, vilket dataskyddsombudet tycker är positivt. De kriterier som man anger i frågeunderlaget framkommer inte alla i rutinen. Om det separata dokumentet benämnt konsekvensanalys inte finns att tillgå för den som utför riskbedömningen, bör dessa kriterier förtydligas även i rutinen.

Vidare är det positivt att Göta Lejon har en redan framtagen mall för vilken information som ska lämnas till de registrerade. De punkter som räknas upp är dels de som enligt dataskyddsförordningen är minimikrav, dels ytterligare information som personuppgiftsansvarige föreslår att man lämnar.

Dataskyddsombudet ifrågasätter kommentaren som säger att om bilagan med vilken information som de registrerade får används, så ska dataskyddsombudet stämma av med kommunikationsavdelningen. Dataskyddsombudet är rådgivande och granskande, men utför inte dataskyddsarbetet inom organisationen. Göta Lejon kan be dataskyddsombudet om råd i förhållande till reglerna i Dataskyddsförordningen, men beslut gällande anmälan, information med mera görs alltid av den personuppgiftsansvarige.

Slutligen bör det också förtydligas i rutinen att tidsaspekten är viktig även i förhållande till de registrerade, och att de ska informeras utan onödigt dröjsmål.

3.1.4 Dokumentation av incidenter

Det framkommer i Göta Lejons rutin att alla personuppgiftsincidenter ska dokumenteras. Bolaget har bifogat ett Excel-ark där alla incidenter samlas.

3.1.4.1 Analys

Tillsynsmyndigheten ställer högra krav på dokumentationen vid en inträffad personuppgiftsincident. Därför är positivt att Göta Lejon i sin rutin förtydligar och uppmanar till att alla incidenter ska dokumenteras. Det innebär att även incidenter som inte anmäls till tillsynsmyndigheten eller som inte de registrerade informeras om, ska dokumenteras. Genom bilaga A framkommer också hur dokumentationen ska gå till, utifrån reglerna i dataskyddsförordningen. Genom att ha en färdig mall att tillgå minskar bolaget riskerna för att incidenter dokumenteras felaktigt och inte sparas ordentligt. Eftersom tillsynsmyndigheten kan begära att ta del av dokumentation beträffande incidenter är det av yttersta vikt att bolaget har koll på sin dokumentation.

Vidare är det positivt att bolaget har ett samlat dokument där man för logg över alla personuppgiftsincidenter. Det framkommer dock inte vart det här registret finns någonstans. Dokumentet förefaller samla både utlämnande, radering och incidenter i samma ark. Då det inte framkommer vad som är vad i dokumentet, finns risk för att de olika sakerna sammanblandas. Personuppgiftsincidenterna bör dokumenteras separat, för att bolaget lättare ska kunna bevisa att man uppfyller sin dokumentationsskyldighet. Då det inte har skickats in några tillhörande riskbedömningar eller beskrivningar av inträffade incidenterna, kan dataskyddsombudet inte göra någon bedömning av dessa.

3.2 Iakttagelser och risker

Inför granskningen har dataskyddsombudet efterfrågat allt underlag och dokumentation som verksamheten har avseende rutiner för personuppgiftsincidenter. Dataskyddsombudet har också efterfrågat detaljerade beskrivningar och svar i det frågeställningsutskick som har sänts ut till verksamheten. Bolaget har återkopplat med svar i frågeställningen och inkommit med flera handlingar som underlag, vilket har underlättat granskningsarbetet och syftet att hjälpa bolaget i de relevanta delar som är

nödvändiga. Dock saknas det ett dokument som bolaget hänvisar till i rutinen (konsekvensanalys). Därför kan det mycket väl vara så att arbetet gällande bolagets hantering av personuppgiftsincidenter i praktiken går till på ett sätt som är mer tillfredsställande och omfattande än vad bolaget har uppgett inför granskningen. I den här granskningen måste dock hänsyn tas till de uppgifter som faktiskt har framkommit för att på så vis täcka upp för de delar som är bristfälliga och som behöver åtgärdas.

Det är positivt att Göta Lejon har en rutin för personuppgiftsincidenter med tillhörande mallar. Det tyder på att bolaget har börjat arbeta aktivt med den här frågan och tar den på allvar. Det framgår dock inte om personalen har blivit informerade om rutinerna, var rutinerna finns och huruvida den är lättillgänglig för personalen att ta del av. Det utgör också en risk att personalen inte har blivit utbildade för att i ett första skede kunna identifiera en personuppgiftsincident.

Dataskyddsombudet ser vidare att risk finns för missförstånd på grund av beskrivningarna gällande ansvar och roller. Därutöver föreligger det en risk för sammanblandning genom att man dokumenterar utlämnande, radering och incidenter i samma dokument.

3.3 Rekommendationer

Rutinerna behöver kompletteras ytterligare med hänsyn till den korta tidsfrist som dataskyddsförordningen medger vid en inträffad incident. Bolaget bör fundera på hur informationen om en inträffad incident från de som upptäcker incidenten, på ett mer skyndsamt sätt kan nå fram till de som ansvarar för bedömningen av en personuppgiftsincident. För detta krävs att personalen har kompetens nog att kunna identifiera en uppkommen personuppgiftsincident varför utbildningsinsatser inom det angivna området är direkt avgörande. Vidare bör bolaget se över hur kommunikation gällande rutinen sker och säkerställa så att ändringar och uppdateringar kommuniceras ut till alla anställda. Utöver den utbildning som sker med hjälp av dataskyddsombudet under hösten bör bolaget även framgent anta en handlingsplan för uppföljning och vidareutbildning av personalen.

Göta Lejon behöver även se över rutinerna kring hur bolagets personuppgiftsbiträden sköter kommunikationen med Göta Lejon som personuppgiftsansvariga och att det vid inträffade incidenter anmäls till bolaget ett skyndsamt sätt.

Det finns också behov av att se över formuleringarna gällande dataskyddsombudets roll vid en personuppgiftsincident och förtydliga att dataskyddsombudet alltid ska kontaktas vid misstänt och inträffad incident. Även formuleringen gällande vilka typer av incidenter som ska anmälas bör förtydligas med att det är när risk föreligger som anmälan ska ske. Rutinen behöver också förtydligas med att de registrerade ska informeras utan onödigt dröjsmål om hög risk för deras fri- och rättigheter föreligger. Vidare rekommenderas också bolaget att dokumentera sina personuppgiftsincidenter i ett separat dokument.

4 Sammanfattning

Göta Lejon får anses vara förberedda för att kunna hantera en personuppgiftsincident på grund av den gedigna rutinen samt tillhörande mallar och dokument. Genom att förtydliga de punkter och åtgärda de risker som dataskyddsombudet påpekat minskar bolaget risken för att en incident hanteras felaktigt. Eftersom Dataskyddsförordningen innehåller korta tidsfrister när det kommer till personuppgiftsincidenter är det viktigt att den personuppgiftsansvarige agerar snabbt och korrekt när en incident inträffar. I ett sådant läge är det viktigt att samtliga inblandade vet hur de ska gå tillväga och vad som behöver göras, vilket säkerställs genom tydliga rutiner och utbildning. Vid en eventuell tillsyn kommer bristfälliga rutiner att anses vara uppsåtliga och därmed föranleda till sanktionsavgifter. Personuppgiftsansvarige behöver också se till att vidta åtgärder för att skyndsamt bli informerade av både personal och personuppgiftsbiträden som får kännedom om en inträffad incident. Detta kan göras genom kompetensutveckling och tydligt upprättade rutiner som är lättillgängliga och som berörda parter har god kännedom om.