Göteborgs Stad

**Tjänsteutlåtande**
Utfärdat 2019-01-22
Diarienummer 0008/18

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

# Punkt 16 Årsrapport Internrevisionen 2018 inkl. GDPR

## Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anta Årsrapporten 2018 inkl. GDPR

## Sammanfattning

I den här rapporten presenteras det internrevisionsarbete som har utförts under året.

Granskningens omfattning och identifierade fokusområden framgår av den revisionsplan som beslutades av styrelsen i december 2017.

## Ekonomiska konsekvenser

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Barnperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Mångfaldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Jämställdhetsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Miljöperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Omvärldsperspektivet

Bolaget har inte funnit några särskilda aspekter på frågan utifrån detta perspektiv.

## Bilagor

1. Årsrapport Internrevisionen 2018 inkl. GDPR

# Ärendet

## Beskrivning av ärendet

Se tidigare

## Bolagets bedömning

Det är bolagets bedömning att åtgärder angivna i kommentarsfältet kommer att kunna genomföras under 2019.

| | |
|---|---|
| Katrin Gundersen | Annika Forsgren |
| Bolagsjurist | VD |

www.pwc.com/se

# *Internrevisionsrapport från PwC*

## Försäkrings AB Göta Lejon

Göteborgs Stad
Försäkrings AB Göta Lejon

*Januari 2019*

pwc

*22 januari 2019*

**Försäkrings AB Göta Lejon**
Stora Badhusgatan 6
411 21 Göteborg

Till styrelsen för Försäkrings AB Göta Lejon.

I den här rapporten presenterar vi det internrevisionsarbete som vi har utfört under året. Syftet är att ge er en bättre bild av vår granskning utifrån de planer som fastställts av styrelsen samt informera er om de iakttagelser som vi har gjort under arbetets gång.

Granskningens omfattning och identifierade fokusområden framgår av den revisionsplan som kommunicerats till er i januari 2018. Rapporten innehåller förslag på utvecklingsområden och kopplat till de utvecklingsområden som vi har identifierat hittar ni även våra förslag på hur ni kan arbeta med dessa framöver.

Vi ser fram emot att diskutera vår rapport med er vid vårt möte den 22 januari 2019.

Med vänlig hälsning

PwC

Morgan Sandström

**Morgan Sandström**
*Partner*
E-post: morgan.sandstroem@pwc.com
Telefon: +46 (0)10 21 25 858

**Erik Ydremark**
*Granskningsledare*
E-post: erik.ydremark@pwc.com
Telefon: +46 (0)10 213 19 12

***Innehållsförteckning***

# *Internrevisionsplan*

## Internrevisionsplan

I dialog med styrelsen har vi presenterat ett förslag till internrevisionsplan vilken har fastställts av styrelsen på styrelsemöte den 2018-01-25.

*Uppföljning av tidigare års rapporterade iakttagelser*

- Genomgång och bedömning av verksamhetens hantering av tidigare iakttagelser.

*Granskning av ersättningar*

- Granskning av styrande dokument mot gällande regelverk (EU-kommissionens delegerade förordning 2015/35). Utöver granskning av styrdokumentet har även ett test av löneutbetalningarna genomförts. Anställningsavtal för fem anställda samt signerade lönerevisionslistor har inhämtats och stämts av mot lönespecifikation för en månad. Vi har vidare granskat rutiner för pensionsavsättning till VD.

*Granskning av utlagd verksamhet*

- Granskning av Göta Lejons policys, riktlinjer och övriga styrande dokument. Vi har vidare gjort en uppföljning av tidigare genomförd processgenomgång avseende Göta Lejons övervakning av outsourcad verksamhet.

*Granskning av bolagets efterlevnad av GDPR*

- En övergripande granskning och kvalitetssäkring av Göta Lejons anpassning och efterlevnad av den nya Dataskyddsförordningen (GDPR) i syfte att identifiera eventuella gap och föreslå lämpliga åtgärder för att hantera risk för sanktioner och ersättningskrav.

## Rapportstruktur

Rapporten är en så kallad avvikelserapport. Rapportens fokus och tyngdpunkt ligger i de förbättringsåtgärder som har iakttagits under granskningen. Iakttagelserna har klassificerats enligt nedan beroende på hur stor inverkan den identifierade bristen anses utgöra.


Innebär en identifierad brist med stor inverkan. Skall åtgärdas så snart som möjligt.


Innebär en identifierad brist med måttlig inverkan. Skall åtgärdas inom ett år.


Innebär en identifierad brist utan väsentlig inverkan. Skall åtgärdas i mån av tid.

# *Uppföljning av tidigare års rapporterade iakttagelser*

## Uppföljning av tidigare års rapporterade iakttagelser

Syftet med uppföljning av tidigare års rapporterade iakttagelser är att säkerställa att Göta Lejon arbetar reaktivt för att verksamheten ska bedrivas på ett ändamålsenligt vis samt upprätthålla god intern kontroll för de väsentliga processer som i dialog med styrelsen kommit att ingå i internrevisionsplanen. Våra iakttagelser i rapport från 2017 fördelade sig enligt nedan tabell:

| Område | Antal iakttagelser | Ej åtgärdade |
|---|---|---|
| Ersättningspolicy samt efterlevnad av denna | 4 | 0 |
| Aktuariefunktionen | 3 | 0 |
| Skadeprocessen | 1 | 0 |
| Företagsstyrningssystemet | 1 | 1 |

# Uppföljning av status i tidigare års internrevisionsiakttagelser - Företagsstyrningssystemet

Observationer

### Syfte

Syftet med vår övergripande genomgång av Göta Lejons företagsstyrningssystem är att bedöma huruvida de lagkrav som framgår av 10 kap. Försäkringsrörelselagen samt EIOPAs utfärdade riktlinjer (”EIOPA-BoS-14/253 SV”) tillämpas samt om dessa krav efterlevs.

### Utförande

Under 2016 utförde vi en genomgång avseende Göta Lejons efterlevnad av 10 kap. Försäkringsrörelselagen samt EIOPAs riktlinjer om företagsstyrningssystem vilket resulterade i en gapanalys som tillhandahölls företagsledningen. Göta Lejon använder sig av ett gemensamt verktyg för att följa upp och åtgärda rekommendationer som lämnats av samtliga kontrollfunktioner. Vi har inhämtat och tagit del av detta verktyg och följt upp de rekommendationer avseende företagsstyrningssystemet som vi lämnade under 2016. En fullständig lista med erhållet underlag redovisas i bilaga 1.

| Status | Iakttagelse | Vår rekommendation | Företagsledningens kommentar |
|---|---|---|---|
|  | Försäkringsrörelselagen kap. 10 tillsammans med EIOPAs utfärdade riktlinjer kring företagsstyrningssystem (”EIOPA-BoS-14/253 SV”) berör hur ett försäkringsaktiebolags företagsstyrningssystem ska vara utformat. Vi har under föregående år upprättat en gapanalys för att belysa vilka åtgärder som Göta Lejon bör vidta för att i allt väsentligt efterleva lagkraven samt EIOPAs riktlinjer. Vår första genomgång (år 2016) av bolagets företagsstyrningssystem resulterade i 21 stycken observationer. Vid årets granskningstillfälle konstaterar vi att 6 stycken observationer har åtgärdats. De 15 stycken observationer som kvarstår att åtgärdas avser innehåll i ERSA och affärsplan. Dessa ej åtgärdade observationer kommer att hanteras i samband med ERSA och affärsplan för 2019. | Vår rekommendation är att åtgärder beskrivna i gapanalysen vidtags fortlöpande. | Bolaget kommer fortlöpande att vidta åtgärder beskrivna i gapanalysen. Många av PwC:s rekommendationer är omhändertagna i ERSAN och affärsplanen för 2018. |

# Resultat genomförd granskning - Ersättningssystem

### Syfte

Syftet med genomgång av ersättningssystemet är att säkerställa att Göta Lejon tillämpar och följer EU-kommissionens delegerade förordning 2015/35. Vidare är det vår uppgift att bedöma huruvida Göta Lejons interna ersättningspolicy är förenlig med samma regelverk. Göta Lejon tillämpar inte möjligheten att erbjuda personal rörlig ersättning. Vår granskning har således inte omfattat rörlig ersättning eller genomgång av prestationsmål.

### Utförande

Vi har huvudsakligen baserat vår granskning på styrdokument, protokoll från styrelsemöten och EU-kommissionens delegerade förordning 2015/35. Test av löneutbetalningar mot anställningsavtal, lönerevisionslistor och lönespecifikationer har genomförts. Vidare har test av premieinbetalningar avseende VDs pension utförts där utbetalning har granskats mot VDs anställningsavtal och senaste lönerevisionslista. En fullständig lista med erhållet underlag redovisas i bilaga 1. Vi har noterat att ledningen agerat på de iakttagelser vi noterat i rapport lämnad 2017 och har vid vår granskning 2018 ej noterat några nya iakttagelser.

# Resultat genomförd granskning – Utlagd verksamhet

Observationer

### Syfte

Syftet med vår genomgång av utlagd verksamhet är att säkerställa att kritiska moment hanteras enligt de beskrivningar som finns upprättade av bolaget. Vidare syftar vår granskning till att belysa riskområden kopplade till bolagets utlagda verksamhet, för att företagsledningen skall kunna minimera riskerna kopplade till detta.

### Utförande

Vi har granskat Göta Lejons policys, riktlinjer och övriga styrande dokument relaterade till utlagd verksamhet samt granskat de avtal som Göta Lejon har ingått beträffande utlagd verksamhet. En fullständig lista med erhållet underlag redovisas i bilaga 1. Vi har vidare gjort en uppföljning av tidigare genomförd processgenomgång avseende Göta Lejons övervakning av outsourcad verksamhet. Nedan följer de iakttagelser som vi noterat under vår granskning.

Göta Lejon är en förhållandevis liten organisation sett till det försäkrade beståndet. För att hantera befintligt bestånd med nuvarande organisation har flera kritiska funktioner lagts ut på extern part. Enligt Göta Lejons riktlinje för outsourcing framgår det att ett av minimikraven för att verksamhet ska få bedrivas av extern part är att både Göta Lejon och tjänsteleverantören upprättar och vidmakthåller en beredskapsplan. Vi vill poängtera vikten av att kontinuerligt analysera, utvärdera samt ta hänsyn till förändringar hos båda parter för att säkerställa att konsekvenserna för Göta Lejon vid oförutsedda händelser hos tjänsteleverantören får så liten påverkan på Göta Lejon som möjligt.

| Status | Iakttagelse | Vår rekommendation | Företagsledningens kommentar |
|---|---|---|---|
|  | Försäkringsrörelselagen 10 kap. §§ 18-22 ställer krav vad gäller innehållet i ett avtal som definieras som ett avtal för utlagd verksamhet. I samband med vår genomläsning av Göta Lejons avtal för utlagd verksamhet har vi bedömt huruvida kraven uppfylls. I allt väsentligt är vår bedömning att avtalen innehåller de obligatoriska uppgifterna. Dock är vår bedömning att det endast i avtalet med iFACTS AB framgår tydligt att tjänsteleverantören ska rapporterar om väsentliga händelser hos tjänsteleverantören som kan påverka dess förmåga att fortsätta leverera tjänsten till försäkringsbolaget. Vidare har vi noterat att det endast i avtalet med Cunningham Lindsey Sweden AB framgår att tjänsteleverantören ska låta försäkringsbolagets externrevisorer få tillgång till dess underlag och arbetspapper. | Vår rekommendation är att avtalen rörande utlagd verksamhet uppdateras på så sätt att samtliga krav enligt 10 kap. §§ 18-22 FRL uppfylls. | Bolaget kommer att göra tillägg till avtalen beträffande väsentliga händelser och externrevisorernas möjlighet att granska leverantörerna. |

# Resultat genomförd granskning - GDPR

### Syfte

En övergripande granskning och kvalitetssäkring av Göta Lejons anpassning och efterlevnad av den nya Dataskyddsförordningen (GDPR) har genomförts i syfte att identifiera eventuella gap och föreslå lämpliga åtgärder för att hantera risk för sanktioner och ersättningskrav.

### Utförande

Vi har huvudsakligen utfört granskningen genom intervjuer. Vår bedömning är att Göta Lejon har implementerat övergången från PuL till GDPR på ett ändamålsenligt sätt, i förhållande till organisationens art och komplexitet, med förbättringspotential på ett antal områden. För utfört arbete samt våra specifika observationer, vänligen se bifogad bilaga 2.

# Planering

## Internrevisionsplan

Under 2019-2020 planerar PwC (internrevisionsfunktionen) att granska följande delar inom Göta Lejon;

### År 2019

- Uppföljning av status i tidigare års internrevisionsiakttagelser
- Granskning av processen för hantering av inbetalda premier
- Granskning av aktuariefunktionens arbete
- Återförsäkringsprocessen

### År 2020

- Uppföljning av status i tidigare års internrevisionsiakttagelser
- Granskning av ersättningar
- Granskning av centrala funktioner
- Granskning av outsourcingpartners (skadereglerare)

# *Bilaga 1*

Vi har under vår granskning intervjuat följande personer och tagit del av nedan dokument.

## Granskning av ersättningssystem

*Intervjuande personer:*

Katrin Gundersen

*Inhämtade dokument:*

Riktlinje för Ersättningar version 4

Protokoll förda vid styrelsens sammanträden under 2018

Lönerevisionslistor för fem anställda inom bolaget

Lönespecifikationer för en månad för de anställda

VD:s anställningsavtal

Faktura avseende VDs pensionspremie för en månad

## Granskning av utlagd verksamhet

*Intervjuande personer:*

Katrin Gundersen

*Inhämtade dokument:*

Riktlinje för Outsourcing

Lämplighetsprövning av ledningspersoner och ansvariga för centrala funktioner

Punkt 22 Bilaga Utlagd verksamhet 2019

Mall för outsourcing

GSL – Report (Final)

Cunningham Lindsey – Report (Final)

00 – Göta Lejon – Crawford – Report (Final)

*Avtal:*

Towers Watson AB – Aktuariefunktion

AON Global Risk Consulting AB – Compliancefunktion

AON Global Risk Consulting AB – Riskfunktion

Crawford & Company Sweden AB – Skadereglering, ansvar

Cunningham Lindsey Sweden AB – Skadereglering, egendom

iFACTS AB – Försäkringssystem

Öhrings PricewaterhouseCoopers AB – Internrevision

# *Bilaga 1 – forts.*

Vi har under vår granskning intervjuat följande personer och tagit del av nedan dokument.

**Uppföljning av status i tidigare års internrevisionsiakttagelser**

*Intervjuande personer:*

Katrin Gundersen

*Inhämtade dokument:*

Sammanställning åtgärder i samtliga rapporter från 2 och 3 linjen

**Granskning av bolagets efterlevnad av GDPR**

*Intervjuande personer:*

Katrin Gundersen

Abtin Kronold

*Inhämtade dokument:*

Vänligen se bifogad bilaga 2

# *Ansvariga från internrevision*

Stockholm, 2019-01-22


Morgan Sandström
Uppdragsansvarig

Erik Ydremark
Projektledare


*Bilaga 2*

www.pwc.se

# *Försäkrings AB Göta Lejon*

# *GDPR – Gapanalys*
## *Internrevisionen 2018*

Till: Styrelsen
Januari 2019

pwc

# *1. Sammanfattning*

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), innebär en skärpning av dataskyddslagstiftningen inom EU, både avseende organisationers åligganden och de registrerade personernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare.

En övergripande granskning och kvalitetssäkring av Försäkrings AB Göta Lejon (”Göta Lejons”) anpassning och efterlevnad av den nya Dataskyddsförordningen (GDPR). Syftet med granskningen var att identifiera eventuella gap och föreslå lämpliga åtgärder för att hantera risk för sanktioner och ersättningskrav. Följande tio (10) områden har beaktats i gapanalysen:

1. Styrning
2. Roller och Ansvar
3. Behandlingsregister
4. Dokumentation
5. Ansvar som personuppgiftsbiträde
6. De registrerades rättigheter
7. Lagstiftning
8. Barn
9. Ostrukturerad data
10. Säkerhetsåtgärder

Resultatet av gapanalysen presenteras i ett spindeldiagram under avsnitt ***2. Gapanalys – diagram***. Värdeskalan i diagrammet är från 1-4 där värde 1 innebär att ingen åtgärd har vidtagits och värde 4 innebär att åtgärder har vidtagits.

**Den övergripande bedömningen av GDPR arbetet utifrån gapanalysen är:**

Utrymme för förbättring

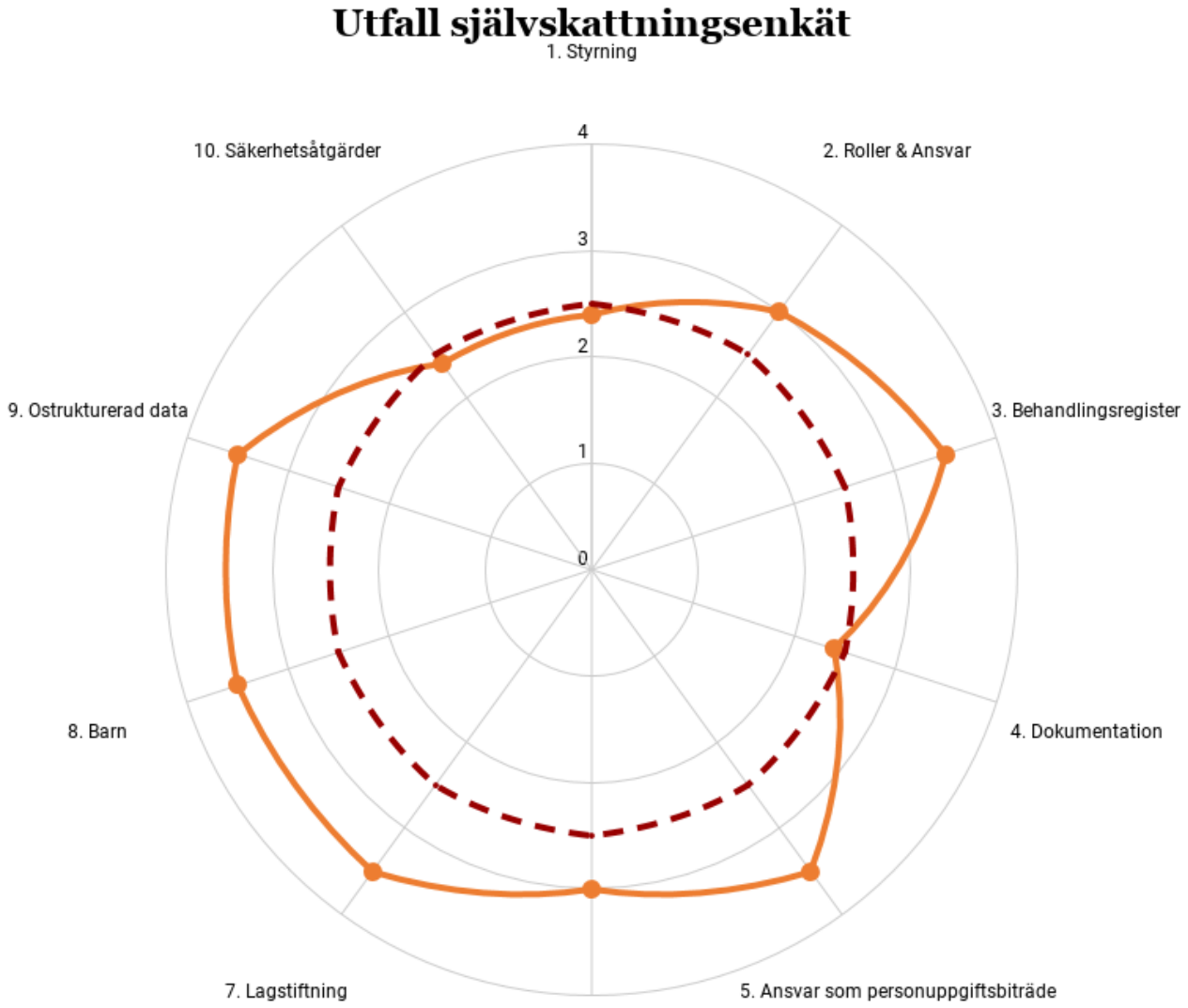
I vår gapanalys har vi bland annat identifierat följande förbättringsområden:

- Styrning (1)
- Dokumentation (4)
- Säkerhetsåtgärder (10)

Vår bedömning är att Göta Lejon har implementerat övergången från PuL till GDPR på ett ändamålsenligt sätt, i förhållande till organisationens art och komplexitet, med förbättringspotential på ett antal områden. Förbättringspunkterna avser främst dokumentation i form av rutiner/processer, styrning i form av otydliga styrdokument och bristande avrop på DSO-stöd, säkerhetsåtgärder i form av avsaknad konsekvensbedömningsprocess samt utredning av persondata i testmiljöer. Den övergripande bedömningen baseras på ett antal brister som vi bedömer som mest relevanta att hantera för att säkerställa regelefterlevnad.

Granskningen har i huvudsak utförts genom intervjuer. Det är inte säkert, men går heller inte att utesluta att en utökad granskning mot underlag skulle leda till ytterligare iakttagelser. Det detaljerade resultatet av vår gapanalys presenteras under avsnitt ***3. Gapanalys – rekommendationer***. För övriga rekommendationer se ***Bilaga 1***. Introduktion, bakgrund och metod för granskningen finns presenterat i ***Bilaga 2***. Mottagna dokument beskrivs i ***Bilaga 3*** och bedömningskriterier definieras i ***Bilaga 4.***

# *2. Gapanalys - diagram*




Område 1, 4 och 10 har resulterat i observationer, se ***3. Gapanalys – rekommendationer***.

För övriga rekommendationer, se ***Bilaga 1 – övriga rekommendationer.***

***Utfall 0*** - området är inte tillämpligt.

***Utfall 1-2,5*** - bedöms ligga under Medelvärde och bör prioriteras.

***Utfall 2,5-4*** - bedöms ligga över Medelvärde.

# 3. Gapanalys – rekommendationer

Nedan redovisas Internrevisionens observationer och rekommenderade förbättringsområden under respektive kategori som identifierats som prioriterade områden under gapanalysen.

| *Observation* | *Rating* | *Rekommendation* | *Åtgärdsplan* |
|---|---|---|---|
| ***1. Styrning***<br>Vi bedömer att Göta Lejon har utpekade roller och ansvar i dataskyddsarbetet vilket är tydligt kommunicerat i verksamheten. Göta Lejons dataskyddsombud ("DSO") har en rådgivande och granskande roll medan en intern dataskyddsansvarig (s.k. Dataskyddskontakt") ansvarar över det operativa arbetet. Dock har följande brister identifierats:<br>• Det är något otydligt hur strukturen av styrdokument etablerar styrningen av GDPR-frågor i Göta Lejon eftersom att vissa av styrdokumenten ägs av Göteborgs Stad och vissa styrdokument är framtagna internt. Vidare är enligt vår förståelse externa styrdokument inte till fullo inarbetade i verksamheten vad avser implementering och efterlevnad.<br>• Dataskyddsombudet är inte tillräckligt involverad avseende rådgivande aktiviteter kring dataskyddsfrågor, t.ex. vid frågor om upphandling och kravställning mot leverantörer.<br>• Det saknas en formaliserad arbetsplan för det kommande arbetet med dataskyddsfrågor.<br>Risk finns för bristande regelefterlevnad gentemot dataskyddsförordningen och en otydlig roll- och ansvarsfördelning mellan DSO och intern dataskyddsansvarig. | Medel | Våra rekommendationer är följande:<br>• Vi rekommenderar Göta Lejon att göra en översyn av de styrdokument som reglerar personuppgifter/GDPR och säkerställer att styrdokumenten samordnas och ger en heltäckande bild över styrningen samt fördelningen av roller- och ansvar i dataskyddsfrågor.<br>• Vi rekommenderar också Göta Lejon att tydliggöra i interna regler i vilka typfall som dataskyddsombudet ska samrådas med, t.ex. vid ingående av personuppgiftsbiträdesavtal eller vid nya behandlingar.<br>• Vi rekommenderar slutligen Göta Lejon att färdigställa utestående delar av GDPR-arbetet för att underlätta framtagandet av en riskbaserad arbetsplan som prioriterar aktiviteter och estimerar tid- och resurser för de aktiviteter som DSO respektive dataskyddsansvarig ska utföra. | **Åtgärd**: Göta Lejon kommer att upprätta en handlingsplan med en sammanställning av samtliga rekommendationer samt med tidplan<br>**Ansvarig**: Dataskyddskontakt på bolaget<br>**Tidpunkt**: Klart Q2 |

# 3. Gapanalys – rekommendationer

| *Observation* | *Rating* | *Rekommendation* | *Åtgärdsplan* |
|---|---|---|---|
| ***4. Dokumentation***<br>Ett antal brister i dokumentationen kring dataskydd och hantering av personuppgifter har identifierats:<br>• Behandlingsregistret saknar förteckning/framställning av identifierade personuppgiftsbiträden.<br>• Informationstexten på Göta Lejons webbplats innehåller inte information till de registrerade motsvarande de krav som följer av den registrerades rätt till information.<br>• Göta Lejons webbplats hänvisar till Göteborgs Stad för mer information om hur Göta Lejon behandlar personuppgifter men hänvisningen går inte att nå utan inloggning till Göteborgs Stads tjänster.<br>• Vid granskningstillfället saknar framtagen skadeanmälansblankett information om hur personuppgifter behandlas enligt kraven i dataskyddsförordningen vilket leder till att personuppgifter samlas in utan att den registrerade tar del av en informationstext.<br>• Det saknas en formaliserad rutin/processbeskrivning för förfrågan om registerutdrag samt personuppgiftsincidenter.<br>• Det saknas en formaliserad rutin för hantering av ostrukturerad data som sparas lokalt.<br>• Vid intervju framkom att befintliga avtal avseende outsourcad verksamhet inte kompletterats med bilaga avseende dataskyddshantering.<br>Risk finns för bristande regelefterlevnad gentemot dataskyddsförordningen och försvårar möjligheten till uppföljning och kontroll. | Medel | Våra rekommendationer är följande:<br>• Vi rekommenderar att Göta Lejon kompletterar behandlingarna i PU-registret med uppgifter om personuppgiftsbiträden.<br>• Vi rekommenderar att Göta Lejon gör en översyn av innehållet i sin informationstext så att den omfattar all information som krävs enligt dataskyddsförordningen*. Informationstexten bör omarbetas i samråd med dataskyddsombud.<br>• Vi rekommenderar att Göta Lejons informationstext på webbplats omarbetas så att hänvisningen tas bort och informationstexten blir fullständig. Förslagsvis kan detta förtydligas i en integritetspolicy specifikt för Göta Lejon.<br>• Vi rekommenderar att skadeanmälansblanketten omarbetas så att den information som ska framgå vid insamlandet av personuppgifter finns med.<br>• Vi rekommenderar Göta Lejon att utarbeta interna regler för hantering av ostrukturerad data som inte omfattas av offentlighetslagstiftning.<br>• Vi rekommenderar slutligen att formaliserade rutiner och/eller processbeskrivningar för tillvägagångssätt vid förfrågan om registerutdrag och för hantering av personuppgiftsincidenter tas fram.<br>• Vi rekommenderar att Göta Lejon säkerställer att benfintliga avtal har kompletterats med information om dataskyddshantering. Detta bör även dokumenteras.<br>** För en lista över vilken information som krävs och detaljeringsnivå, se Artikel 29-arbetsgruppens Riktlinjer om öppenhet (Bilaga).* | **Åtgärd**: Se föregående<br>**Ansvarig**:<br>**Tidpunkt**: |

# 3. Gapanalys – rekommendationer

| *Observation* | *Rating* | *Rekommendation* | *Åtgärdsplan* |
|---|---|---|---|
| ***10. Säkerhetsåtgärder***<br>Vår bedömning är att Göta Lejon har en god och stabil IT-miljö där majoriteten av systemen driftas av extern leverantör. Ett fåtal punkter i syfte att öka säkerheten har identifierats:<br><br>• Vid intervju framkom att det är oklart om Göta Lejon använder persondata i IT-testmiljöer för att utföra tester vid IT-utveckling. Datainspektionen har i ett tidigare beslut* bedömt att personuppgifter i testmiljöer bör undvikas så långt det är möjligt, att test- och produktionsmiljöer ska hållas tydligt åtskilda och att det bör finnas rutiner för att undvika att åtgärder av misstag utförs i produktionsmiljö.<br>• Det finns i dagsläget inget förankrad process för konsekvensbedömningar (enl. artikel 35) vilket framgår i rollbeskrivningen för DSO. Innan man planerar en ny personuppgiftsbehandling som innebär särskilda risker för de registrerade ska man göra en bedömning av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska riskerna. Konsekvensbedömningar för behandling av personuppgifter ska alltid genomföras om känsliga personuppgifter behandlas.<br><br>Risken med bristande säkerhetsåtgärder kan leda till en svårighet att uppnå regelefterlevnad.<br><br>** Datainspektionens Beslut, Diarienr 1275-2013* | Låg | Våra rekommendationer är följande:<br>• Vi rekommenderar att Göta Lejon utreder i vilken omfattning skarp persondata hanteras i IT-testmiljöer och vidtar åtgärder för att i så stor utsträckning som möjligt undvika personuppgifter i dessa miljöer.<br>• Vi rekommenderar vidare att Göta Lejon tar fram rutiner för att förhindra att åtgärder av misstag vidtas i produktionsmiljön vid IT-utveckling.<br>• Vår rekommendation är att Göta Lejon formaliserar en konsekvensbedömningsprocess för framtida konsekvensbedömningar. Det bör närmare utredas vilka behandlingar som Göta Lejon utför som omfattas av kravet på att genomföra en konsekvensbedömning. Det rekommenderas att göra konsekvensbedömning på behandlingar som kan vara integritetskränkande dels för att det är ett krav att detta skall göras, men också för att på djupet förstå hur personuppgifter inom dessa områden behandlas och vilka risker som är förknippade med behandlingarna. Vidare bör en rutin tas fram för genomförande av konsekvensbedömningar vid utveckling och införskaffning av nya IT-system eller inrättande av nya processer. Informationen skulle t.ex. kunna framgå av en Informationssäkerhetspolicy. | **Åtgärd**: Handlingsplan kommer att upprättas med samtliga rekommendationer. Arbetet kommer att genomföras tillsammans med IT ansvarig på bolaget.<br>**Ansvarig**: Dataskyddskontakt på bolaget<br>**Tidpunkt**:Q4 |

# *Bilagor*

# *Bilaga 1 – övriga rekommendationer*

Nedan redovisas Internrevisionens övriga rekommendationer och rekommenderade förbättringsområden under respektive kategori som identifierats under gapanalysen och som inte resulterat i en observation.

| *Område* | *Rekommendation* |
|---|---|
| ***2. Roller och Ansvar***<br><br>Vi bedömer att det finns en roll (med formaliserad och ändamålsenlig befattningsbeskrivning) som har ett utpekat ansvar för dataskyddsfrågor och som vid behov ska samråda med DSO. | Givet få behandlingar och liten organisation bedöms Dataskyddskontakten som tillräcklig för att ta ett operativt ansvar för personuppgiftshanteringen. Det tycks vara så att dataskyddsombudet har kunnat involveras i fler frågor än vad som har varit fallet sedan GDPR trätt i kraft. |
| ***3. Behandlingsregister***<br><br>Det har skett ett arbete med att kartlägga samtliga personuppgiftsbehandlingar i ett register där viktig information såsom målgrupp och syfte specificerats. Vi bedömer således att Göta Lejon har kartlagt sina personuppgiftsbehandlingar på ett relevant sätt och enligt dataskyddsförordningens krav. | Behandlingsregistret kan kompletteras på ett antal områden även om centrala delar redan är täckta. Dataskyddskontakten bör säkerställa att behandlingsregistret blir komplett och förvaltas så att nya behandlingar fångas upp, i enlighet med ansvarsområde. |

# *Bilaga 1 – övriga rekommendationer*

| *Område* | *Rekommendation* |
|---|---|
| ***5. Ansvar som personuppgiftsbiträde***<br><br>Göta Lejon har identifierat personuppgiftsbiträden och reglerat behandlingsaktiviteterna i personuppgiftsbiträdesavtal, baserat på framtaget mallavtal. Vi ser positivt på att befintligt behandlingsregister kommer att läggas in i ett nytt systemstöd under nästa år och att uppgifter om personuppgiftsbiträden för vissa behandlingar kompletteras framgent. | Personuppgiftsbiträden bör dokumenteras i behandlingsregistret. |
| ***6. De registrerades rättigheter***<br><br>Vi bedömer att det finns förbättringspotential för att möta kraven avseende de registrerades rättigheter vilket främs avser informationen om behandling av personuppgifter som lämnas till de registrerade. | För rekommendation avseende rutiner- och processbeskrivningar, vänligen se observation ***4. Dokumentation*** |

# *Bilaga 1 – övriga rekommendationer*

| *Område* | *Rekommendation* |
|---|---|
| ***7. Lagstiftning***<br><br>Vår bedömning är att det finns en medvetenhet kring relevant lagstiftning på dataskyddsområdet och att Göta Lejon framgent kommer att fånga upp omvärldsbevakning genom enheten för Dataskydd i Intraservice och genom andra nätverk. | Ingen förbättringspotential har identifierats under granskningen. |
| ***8. Barn***<br><br>Vår bedömning är att det finns en medvetenhet kring känsligheten att hantera personuppgifter om barn. Det har skett ett arbete med att minimera personuppgifter om barn genom att exempelvis endast spara uppgift om att barn finns men i övrigt radera personuppgifter som inte är nödvändiga. | Göta Lejon behandlar personuppgifter om barn men lämnar inte någon information till dem. Det bör utredas hur information kan lämnas till barn och hur informationen ska utformas för att vara anpassad efter barnens specifika behov. |
| ***9. Ostrukturerad data***<br><br>Vår bedömning är att det finns en medvetenhet kring ostrukturerad data eftersom samtliga medarbetare har utbildats och eftersom instruktioner för hantering av fritextfält och rutin för e-posthantering är framtagna och implementerade i organisationen. | Vår rekommendation är att Göta Lejon fortbildar anställda i hanteringen av ostrukturerad data. Vi rekommenderar även att det görs uppföljningar på att det finns en medvetenhet kring ostrukturerad data samt att rutiner efterlevs. |

# *Bilaga 2 – Introduktion, bakgrund och metod*

### *Introduktion och bakgrund*

En övergripande granskning och kvalitetssäkring av Försäkrings AB Göta Lejon (”Göta Lejons”) anpassning och efterlevnad av den nya Dataskyddsförordningen (GDPR). Syftet med granskningen var att identifiera eventuella gap och föreslå lämpliga åtgärder för att hantera risk för sanktioner och ersättningskrav.

### *Metod*

Granskningen genomfördes under December 2018 av Louise Wennström och Johan Lindfors.

Resultatet av gapanalysen baseras på genomgång med för granskningen relevanta personer inom kontrollfunktionerna, vilka listas i avsnittet *Intervjuade personer*. Tillsammans med funktionerna gick vi igenom samtliga 10 områden som resulterade i ett slutgiligt medelvärde för respektive område, baserat på ett antal frågor. Värdeskalan i diagrammet är från 1-4 där värde 1 innebär att ingen åtgärd har vidtagits och värde 4 innebär att åtgärder har vidtagits.

Rapporten är upprättad i avvikelseformat. Tyngdpunkten har lagts på de brister och förbättringsområden som iakttagits, medan de områden som granskats utan anmärkning bara övergripande omnämns ovan. Rapporten är endast för Göta Lejons information och är inte avsedd att användas för annat syfte och kan endast distribueras i enlighet med den överenskommelse som finns mellan Öhrlings PricewaterhouseCoopers AB (“PwC”) och Göta Lejon.

### *Intervjuade personer*

Katrin Gundersen - Bolagsjurist och Dataskyddsansvarig (“Dataskyddskontakt”)

Abtin Kronold - Dataskyddsombud

# *Bilaga 3 – Dokumentförteckning*

***Dokumentation som beaktats***

1. GDPR Göta Lejon - risklista_åtgärdsplan
2. DSF_ GL_Mall migrering av pu till nytt behandlingssystem
5. Befattningsbeskrivning dataskyddsansvarig
5. Enkel checklista över lagkraven för biträdesavtal
5. Instruktion för arkivering av skador 2015-12-08
5. MALL Instruktion för gallrings- och bevaranderutiner _level 2
5. rutin för e-post - utkast 171208
8. PersonuppgiftsbiträdesavtalGÖTAL20180420_komentar
9. Gapanalys_ lagliggrund_göta_lejon_2018
AKRDB4DEZB
AKRDB6BELS
Bilaga 1 rättning och borttagning av registrerad personuppgift
Bilaga 2 Instruktion för hantering av risker
Bilaga till anställningsavtal
Checklista avseende följsamhet mot EU dataskyddsförordning
Checklista information till den registrerade
Checklista laglig grund
Checklista samtycke
Försäkrings Göta Lejon_GDPR FAQ
Policy och riktlinje för hantering av peronuppgifter i Försäkrings AB Göta Lejon
Riktlinje för fritextfält
Stöd för hantering av personuppgifter

# *Bilaga 4 - Bedömningskriterier*

| ***Bedömningsskala*** | ***Internrevision*** |
|---|---|
| **Tillfredsställande** | *Lednings-, riskhanterings- och kontrollprocesser bedöms fungera tillfredsställande. Inga väsentliga observationer har identifierats* |
| **Utrymme för förbättring** | *Lednings-, riskhanterings- och kontrollprocesser bedöms fungera relativt väl. Observationer har identifierats, vilka bör hanteras för att upprätthålla en god intern kontroll.* |
| **Bristfällig** | *Lednings-, riskhanterings- och kontrollprocesser bedöms inte fungera väl. Observationer har identifierats, vilka bedöms som väsentliga.* |

| ***Bedömningsskala*** | ***Observation och risk*** |
|---|---|
| **Låg** | *Visar en brist som inte har någon väsentlig påverkan på system, processer och kontroller men som indikerar en möjlighet till förbättrad effektivitet och/eller verkningsgrad av processer och kontroller.* |
| **Medel** | *Visar en brist, som ensam eller i kombination med andra brister kan påverka funktionaliteten/integriteten i system, processer och kontroller.* |
| **Hög** | *Visar en brist med stor påverkan på system, processer och kontroller, vilken kan innebära en väsentlig förlust, ineffektivitet och/eller publik eller laglig påverkan.* |

Stockholm, 22 januari 2019

_____

Morgan Sandström
*Uppdragsansvarig, PwC*