**Beslutsunderlag**
Utfärdat 2023-01-30
Diarienummer 0025/22

Handläggare
Björn Wennerström
Telefon: 031-368 55 06
E-post: bjorn.wennerstrom@gotalejon.goteborg.se

# Årsrapport Dataskyddsenheten 2022

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

- anteckna årsrapport från Dataskyddsenheten 2022

## Sammanfattning

Den fördjupade kontrollen har bestått av kontroll av behörighetsstyrning i Göta Lejons IT-system Insman. Verksamheten rekommenderas att, utöver nuvarande rutiner, även se över behörigheter vid avslut av tjänst och ändring av tjänst, utföra konsekvensbedömning för behandlingar i systemet där det krävs och kontrollera hur behörigheterna påverkas av bedömningen, utreda relationen med Intraservice och ta fram instruktioner i de fall det behövs, samt se över om det inte finns annan lagstiftning (till exempel sekretess) som påverkar hur behörigheter bör sättas.

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Bolaget har fått ett antal rekommendationer att arbeta med.

## Bedömning ur ekonomisk dimension

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

## Bedömning ur ekologisk dimension

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

## Bedömning ur social dimension

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

## Samverkan

Ingen samverkan har genomförts

## Bilagor

1. Årsrapport Dataskyddsenheten 2022

## Ärendet

Årsrapport från Dataskyddsenheten.

## Beskrivning av ärendet

Dataskyddsombudet ska enligt lagstiftningen rapportera till högsta förvaltningsledning dvs. styrelse eller nämnd. Detta för att den högsta ledningen ska få den information som behövs för att kunna bedöma vilka prioriteringar som ska göras och vilka risker som organisationen är beredd att ta. Dataskyddsombudet fattar inte beslut åt verksamheten. Ytterst vilar ansvaret för att verksamheterna följer lagen på nämnd/styrelse. De råd och rekommendation som ges av dataskyddsombudet syftar till att ge ledningen underlag för att kunna fatta väl underbyggda beslut.

## Bolagets bedömning

Det är bolagets bedömning att resultatet från revisionen är rimlig och korrekt.

Göteborgs Stad

# Årsrapport för dataskyddsarbetet 2022

## Försäkrings AB Göta Lejon

2022-12-22

# Innehåll

# 1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

## 1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

# 2 Granskning av dataskyddsarbetet 2022

## 2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

## 2.2 Fördjupad kontroll

### 2.2.1 Kontroll av behörighetsstyrning 2022

Den fördjupade kontrollen har bestått av kontroll av behörighetsstyrning i Göta Lejons IT-system Insman. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och lämnat ett antal rekommendationer till verksamheten. Följande rekommendationer har lämnats:

- Verksamheten rekommenderas att, utöver nuvarande rutiner, även se över behörigheter vid avslut av tjänst och ändring av tjänst.
- Utföra konsekvensbedömning för behandlingar i systemet där det krävs och kontrollera hur behörigheterna påverkas av bedömningen.

- Utred relationen med Intraservice och ta fram instruktioner i de fall det behövs (om Intraservice är personuppgiftsbiträde).
- Se över om det inte finns annan lagstiftning (till exempel sekretess) som påverkar hur behörigheter bör sättas.

# 2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

## 2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

| Risknivåer | Färgkod |
|---|---|
| Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten. | |
| Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder. | |
| Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga. | |
| Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete. | |

# 2.4 Försäkrings AB Göta Lejons dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

### 2.4.1 Kontrollpunkt 1: Dataskyddsorganisation


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

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inget att invända mot bolagets skattning gällande den interna dataskyddsorganisationen, men anser att det finns risker i att den interna dataskyddsorganisationen hittills enbart bestått av en person, eftersom det gör den väldigt personbunden. Det är därför extra viktigt att bolaget lyfter dataskyddsfrågor även på en högre nivå samt att det finns dokumenterade rutiner som kan omhändertas av någon annan i de fall dataskyddskontakten inte är på plats. Den som har rollen som dataskyddskontakt i bolaget behöver få mer resurser att arbeta med dataskyddsfrågor, då det finns en hel del förbättringar att göra kopplat till dataskydd.

### 2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter


Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig då hanteringen av personuppgiftsincidenter tidigare har granskats och de rekommenderade åtgärderna har vidtagits. För att kunna arbeta förebyggande och säkerställa högt säkerhetsmedvetande är rekommendationen att bolaget ser över och analyserar tidigare inträffade personuppgiftsincidenter samt kontinuerligt informerar sina medarbetare om vad en incident är och hur de ska hanteras.

### 2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser


Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har

identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Bolagets resultat på kontrollpunkten är i år bättre än förra året och bolaget uppger att de flesta åtgärder som dataskyddsombudet rekommenderade i 2021 års rapport har vidtagits. Eftersom dataskyddsombudet inte har sett dessa åtgärder, kan dataskyddsombudet inte uttala annat än att det är positivt om bolaget har vidtagit åtgärder då resultatet innebär färre risker. Dataskyddsombudet vill särskilt lyfta risken när det kommer till bolagets kompetens att bedöma hela kedjan av underbiträden vid anlitande av personuppgiftsbiträden. Bolaget uppger också att det till viss del saknas rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade biträden. Dataskyddsombudet rekommenderar att bolaget ser över hur verksamheten kan kontrollera att biträden följer sina skyldigheter enligt avtalen.

### 2.4.4 Kontrollpunkt 4: Personuppgiftsregister


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

Dataskyddsombudets kommentarer:

Bolaget bedömer att det inte föreligger några risker kopplat till användningen av registret. Utifrån förra årets fördjupade kontroll uppgav bolaget att verksamheten tagit fram en rutin för hantering av registret. Trots detta är årets skattning lägre både avseende rutinen och uppdateringen av registret. Dataskyddsombudet kommer därför återigen följa upp om verksamheten vidtagit åtgärder utifrån den fördjupade granskningen. Dataskyddsombudet kan se att registret inte har uppdaterats sen 2021 vilket tolkas som att det inte används regelbundet och inte uppdateras.

Utifrån förändringar i den interna dataskyddsorganisationen är rekommendationen att förtydliga vem som ansvarar för registret.

### 2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd


Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets resultat på kontrollpunkten kopplat till övergripande strategi för dataskydd är detsamma som förra året och indikerar att risker fortfarande föreligger. Verksamheten saknar en fullgod övergripande strategi för dataskydd och arbetar inte aktivt och medvetet med ett riskbaserat arbetssätt kopplat till dataskydd i alla frågor. För ett gott dataskyddsarbete på operativ nivå behöver ledningen och styrelsen fatta strategiska beslut och stärka den interna kontrollen genom att sätta periodiska aktiviteter med tydligt ansvar för att verifiera att informationssäkerhetsaktiviteter genomförs ändamålsenligt i enlighet med stadens styrande dokument. Enligt uppgift pågår arbetet med att identifiera och validera bolagets informationstillgångar. Eftersom arbete kvarstår är dataskyddsombudets rekommendation att detta åtgärdas. I den mån bolaget anordnar möten, sammankomster och liknande behöver rutiner för hantering av personuppgifter tas fram.

### 2.4.6 Kontrollpunkt 6: Utbildning


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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i bolagets bedömning. Dataskyddsombudet rekommenderar att bolaget regelbundet utreder behovet av utbildningsinsatser och säkerställer att verksamheten upprätthåller en god kunskap i dataskyddsfrågor. Olika befattningar kan kräva olika utbildningsinsatser och få olika typer av information.

### 2.4.7 Kontrollpunkt 7: Integritetspolicy


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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer med bolagets skattning, men rekommenderar att bolaget regelbundet ser över integritetspolicyn för att säkerställa att den hålls uppdaterad. Det är också viktigt att de registrerade kan nå integritetspolicyn ifrån verksamhetens samtliga digitala kanaler. Dataskyddsombudet rekommenderar att bolaget ser över, dokumenterar och förbättrar sina rutiner för att informera medarbetarna om hur deras personuppgifter behandlas. Dataskyddsombudet har inte granskat integritetspolicyn i detalj.

### 2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering


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

#### Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i bolagets bedömning och anser att det föreligger stora risker på kontrollpunkten. Bolaget uppger att det finns en uppdaterad dokumenthanteringsplan med gallringsrutiner, vilket är en förutsättning för att bolaget ska kunna säkerställa principen om lagringsminimering enligt GDPR. Bolaget rekommenderas att se över hur medarbetarna får information om dokumenthantering och gallring, då det också säkerställer medarbetarnas följsamhet på dataskyddsområdet. Bolaget uppger att ca 25% av bolagets personuppgiftsbehandlingar har informationsklassificerats utifrån stadens riktlinje för informationssäkerhet. Dataskyddsombudet rekommenderar att bolaget ser över informationsklassningen för att säkerställa att den är korrekt och uppdaterad. Bolaget behöver vidare se över hur de registrerade får information om hur deras personuppgifter hanteras, direkt vid kontakt med verksamheten. Rutiner för hantering av personuppgifter i e-post rekommenderades bolaget åtgärda förra året, men eftersom skattningen fortfarande är låg kvarstår den rekommendationen.

### 2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd


Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

#### Dataskyddsombudets kommentarer:

Bolagets skattning på kontrollpunkten visar på höga risker kopplat till konsekvensbedömning/samråd. Eftersom bolaget hittills inte arbetat med konsekvensbedömningar, instämmer dataskyddsombudet i skattningen. Utifrån bolagets uppdrag ser dataskyddsombudet också att det är en stor brist att verksamheten inte vet om det finns några konsekvensbedömningar för några behandlingar, hur många framtagna och fastställda konsekvensbedömningar eller planerade konsekvensbedömningar bolaget har. Dataskyddsombudets uppfattning är att verksamheten inte genomfört någon konsekvensbedömning på grund av bristande kompetens och rutin och att det finns behandlingar som borde ha bedömts. Bolaget saknar helt rutiner kopplat till konsekvensbedömningar vilket

innebär stora risker. Bolaget rekommenderas att implementera arbetet med konsekvensbedömningar i sin övergripande strategi för dataskydd.

Dataskyddsombudet rekommenderar att bolaget utvärderar om/när konsekvensbedömningar behöver göras och om så är fallet säkerställer att konsekvensbedömningar också görs samt att dataskyddsombudet involveras.

### 2.4.10 Kontrollpunkt 10: IT-projekt och upphandling


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

#### Dataskyddsombudets kommentarer:

Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Eftersom dataskyddsombudet inte blivit involverad i några IT-projekt eller upphandlingar under året saknas insyn i hur verksamheten arbetar i dessa frågor. Dataskyddsombudet vill påminna bolaget om att dataskyddsombudet ska involveras i alla frågor som rör dataskydd. Dataskyddsombudet vill också lyfta, i och med att kunskapen om dataskydd generellt behöver höjas inom verksamheten, att det finns risker att dataskyddsperspektivet missas vid uppstart av IT-projekt och vid påbörjan av upphandlingar. Bolaget rekommenderas att säkerställa att hänsyn tas till dataskyddsperspektivet.

### 2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg


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

#### Dataskyddsombudets kommentarer:

Bolagets arbete med behörigheter och rutiner berörs i den fördjupade kontrollen och kommenteras inte vidare här.

Bolaget uppger att det är oklart om det finns rutiner för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratis applikationer och sociala medier. Dataskyddsombudet rekommenderar att bolaget dokumenterar sina kommunikationskanaler och ta fram rutiner samt instruerar sina medarbetare vad som gäller för användning av IT-system och applikationer i mobila enheter inklusive kontroll av användningen av dessa.

Bolaget rekommenderas att dokumentera vilka kommunikationskanaler som används i verksamheten samt se över eventuellt användande av cookies.

### 2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter


Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar i bolaget. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet tillsammans med verksamheten komma att följa upp arbetet under 2023.

## 2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

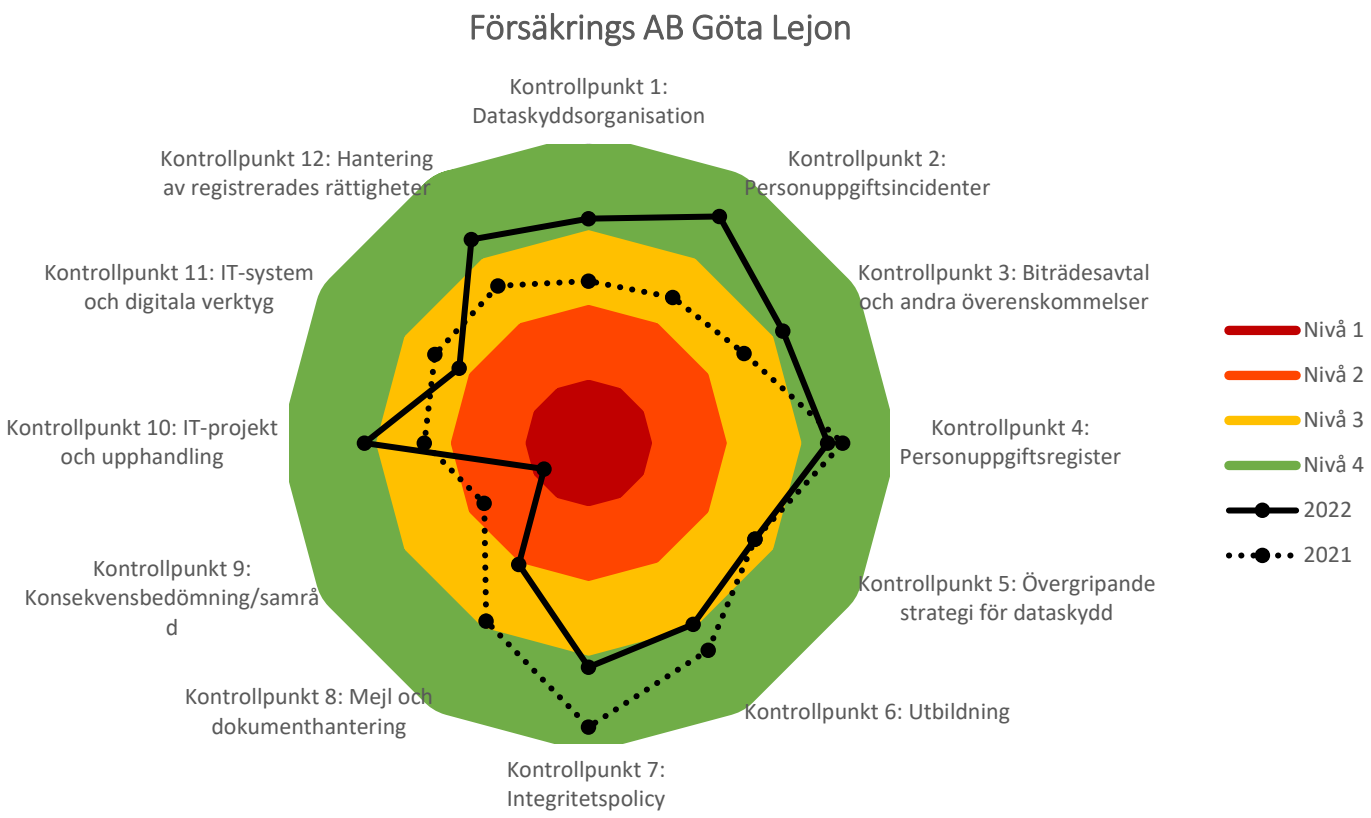
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Verksamheten rekommenderas implementera arbetet med konsekvensbedömningar i den övergripande strategi för dataskydd och säkerställa att konsekvensbedömningar genomförs där det är ett krav.
- Kontrollpunkt 8: Mejl och dokumenthantering
  Verksamheten rekommenderas att säkerställa att informationsklassificeringen är uppdaterad och att medarbetarna informeras om hur information i olika klasser får hanteras och vart.
- Kontrollpunkt 11: IT-system och digitala verktyg
  Verksamheten rekommenderas att se över sina kommunikationskanaler och säkerställa dataskyddsperspektivet vid införande och användande av kostnadsfria appar/tjänster.

# 3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 - behörighetsstyrning

# Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



# Fördjupad kontroll

Behörighetsstyrning - Göta Lejon

## Bakgrund

Den fördjupade kontrollen av behörighetsstyrning syftar till att se om verksamhetens hantering av personuppgifter är säker och korrekt utifrån både tekniska och organisatoriska åtgärder. Med utgångspunkt i artikel 32.2 har kontrollen granskat verksamhetens bedömning av lämplig säkerhetsnivå med hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Därför har fokus legat på behörighetsstyrning och hur det används för att begränsa vilka personuppgifter som medarbetarna får ta del av.

Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. I kontrollen ingick verksamhetens rutiner för tilldelning av behörigheter och åtkomster i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller.

## Iakttagelser från kontrollen

En medarbetare i en verksamhet ska enbart ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten ha rutiner för tilldelning av behörighet, uppföljning av behörigheter samt hur användningen av logg-/åtkomstkontroller sker.

Hos Götalejon har kontrollen genomförts i verksamhetssystemet Insman, där försäkringsfrågor från hela staden behandlas. Systemet används inte bara av Götalejon utan även av andra inom staden. Det finns 271 registrerade användare med olika behörigheter, men alla kommer på något sätt åt personuppgifter. Antal ärenden med personskador i systemet är 433 och andra skador är 42 231. De personuppgifter som behandlas är namn, personnummer, adressuppgifter, telefonnummer, e-postadress, kontoinformation, hälsotillstånd, journalanteckningar och registreringsnummer.

### Behörighetsstruktur och roller i system

Behörigheter styrs genom olika grupper vars rättigheter sätts av systemadministratör. Beroende på vilken grupp en användare tillhör har den åtkomst till olika delar av systemet. En användare kan ingå i flera grupper, och utöver grupptillhörighet sätts också åtkomst till organisation på användarnivå. Till exempel grupper som tillhör område “kund” kan enbart se det som rör den egna organisationen. Detta tolkar dataskyddsombudet som att en användare i systemet från en annan verksamhet i staden (till exempel Lokalförvaltningen) enbart kan se uppgifter som härrör till Lokalförvaltningen. Däremot kan användare i systemet ifrån Göta Lejon få tillgång till även andra verksamheters uppgifter utifrån bolagets uppdrag.

### Tilldelning av behörighet utifrån bedömning

Grupptillhörighet bestäms utifrån vad olika användare ska göra i systemet. Nya grupper kan skapas om det inte finns någon som passar. Rättigheterna styrs således av arbetsuppgifterna. Behörigheter sätts så snävt det går, till exempel har en skadereglerare

som reglerar ansvarsskador enbart åtkomst till skador av typ ansvar. Behörighet går också att sätta på tidsperiod så att åtkomst till skador inom en viss period kan anges.

Vilka rättigheter en grupp har, beslutas vid uppstart av systemet och ses över löpande när ny release tas (mellan 3 och 6 gånger per år). Förändringar i behörigheter för grupper sker i samråd mellan ansvarig för grupp och IT-ansvarig.

### Beslut om behörighet

Respektive grupp har en ansvarig som har rätt att bestämma vem som ska ingå i respektive grupp. För att ge en ny användare behörighet till en grupp krävs att ansvarig för gruppen godkänner detta.

Dataskyddsombudet rekommenderar att bolaget tar fram rutiner/kriterier för när/under vilka förutsättningar en ny användare ska ges behörighet till systemet för att säkerställa att felaktiga behörigheter inte delas ut.

### Uppföljning av behörighet

Behov ska styra behörighet, vilket bland annat innebär att om någon byter roll eller arbetsuppgifter, begär tjänstledigt eller är föräldraledig ska behovet av behörighet ses över och justeras. Om någon avslutar sin anställning är det särskilt viktigt att omedelbart inaktivera behörighet och stoppa tillgång till system och information. Därför behövs rutiner både för ändrat behov under anställning och vid anställnings slut.

Uppföljning på gruppnivå görs löpande vid ny release av IT-ansvarig. Användare läggs till/tas bort från grupper löpande när ansvarig hör av sig. Årligen ses alla användare i systemet över av gruppansvarig och justeras vid behov.

Dataskyddsombudet rekommenderar att bolaget ser över behörighet så fort någon avslutar sin anställning eller byter arbetsuppgifter, för att minska risken för att obehöriga behörigheter ligger kvar i systemet. Dataskyddsombudets rekommendation är att bedömningen av behörighet ska göras per användare, även om tillgången kan ges på gruppnivå. Att ge tillgång till behörigheter på gruppnivå kan vara okej om det gjorts bedömningar utifrån vad som är nödvändigt för respektive grupp och bolaget bedömer att man gjort tillräckligt för att minimera riskerna för de registrerade. Bolaget uppger att behörigheter sätts så snävt som det går, vilket dataskyddsombudet anser är positivt. Eftersom en användare kan ingå i flera grupper, innebär det också att en användare kan ha flera behörigheter. Det är därför viktigt att det finns tydliga riktlinjer för vad en användare får göra i systemet utifrån respektive behörighet.

### Åtkomstkontroll/kontroll av loggar

Bolaget uppger att allting loggas och att det går att kontrollera om man vet vad eller vilken användare. Kontroll sker inte om det inte finns någon särskild händelse som gör att dessa behöver användas. IT-ansvarig/systemadministratör tillsammans med leverantören ansvarar för kontroll av loggarna. Någon definition av särskild händelse har inte bolaget då det hittills inte inträffat att man behövt kontrollera loggen. Men det skulle kunna ske om bolaget misstänker att något skett som inte borde ha skett.

Dataskyddsombudet rekommenderar att bolaget definierar vad misstanke kan bestå av och när loggar får kontrolleras, för att säkerställa att övervakning av anställda inte sker i

onödan. Eftersom det kan finnas integritetskänslig information i systemet, så som uppgifter om sjukdom, är det viktigt att dessa personuppgifter behandlas på ett korrekt sätt. Stickprovskontroller får dock inte utföras om Göta Lejon inte informerat de anställda om detta och klargör vilken rättslig grund man lutar sig på för behandlingen.

**Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen**
Inte aktuellt enligt bolaget.

Utifrån uppgifternas art är dataskyddsombudet osäker på om det inte finns särskilda regler kopplat till försäkring/skador som gäller. Till exempel sekretessregler. Dataskyddsombudet rekommenderar att bolaget undersöker detta.

**Andra risker och åtgärder**
Bolaget uppger att systemet driftas av Intraservice och att åtgärder som vidtas för att skydda servern bestäms av dem. Informationen om huruvida Intraservice ska anses vara personuppgiftsbiträde är enligt dataskyddsombudet motstridigt. Å ena sidan uppger bolaget att Intraservice inte är biträde eftersom de inte ska behandla några personuppgifter. Å andra sidan hänvisar man till att ett personuppgiftsbiträdesavtal finns på plats med hänvisning till Göteborg Stads generella regler för kommungemensamma interna tjänster, bilaga 1. Dataskyddsombudet rekommenderar bolaget att reda ut vilken åtkomst Intraservice har och om de är biträde eller ej. Om de är biträde bör instruktioner finnas för hur de får behandla personuppgifter. Eftersom bolaget uppger att loggkontroll görs tillsammans med leverantören tolkar dataskyddsombudet det som att leverantören har eller kan få tillgång till personuppgifter. Bolaget har också svarat att systemadmin och personal på Götalejon har åtkomst till personskador där känsliga uppgifter kan förekomma. Relationen måste regleras om det inte är gjort.

Bolaget har inte genomfört någon konsekvensbedömning på grund av att kunskap och resurser saknas. Dataskyddsombudet skulle, utifrån personuppgifternas art och behandlingens omfattning, rekommendera bolaget att undersöka ifall en konsekvensbedömning krävs.

Bolaget har själva identifierat ett antal risker med nuvarande hantering av behörigheter men även den riskminimerande åtgärd som behövs.

En identifierad risk är att administratör registrerar fel grupp eller organisation på en användare. Åtgärd för detta uppger bolaget är att kontroll av behörighet sker minst årligen. En annan risk är att användare väljer ett för enkelt/samma lösenord som till ett annat system, vilket gör det lättare att logga in med annans användaruppgifter. Som åtgärd har bolaget tagit fram riktlinjer för vad lösenordet ska innehålla samt att arbetet med att införa tvåfaktorsautentisering har startat. Bolaget har också identifierat en risk för att behörigheter förändras i samband med ny release och att detta inte uppmärksammas vid testning. Därför ska testning genomföras av minst två personer och ev. behörighetsförändring i ny release ska stämmas av inför varje release. Slutligen har bolaget identifierat att det finns en risk att användare slutar och inloggning ändå finns kvar, men att man åtgärdar detta genom årlig kontroll av behörigheter.

Dataskyddsombudet anser att det är positivt att bolaget själva identifierat risker och åtgärder, men vill uppmana bolaget att säkerställa så att dessa åtgärder faktiskt vidtas.

## Sammanfattade rekommendationer (punktform)

- Verksamheten rekommenderas att, utöver nuvarande rutiner, även se över behörigheter vid avslut av tjänst och ändring av tjänst.
- Gör konsekvensbedömning för behandlingar i systemet där det krävs och kontrollera hur behörigheterna påverkas av bedömningen.
- Red ut relationen med Intraservice och ta fram instruktioner i de fall det behövs (om Intraservice är personuppgiftsbiträde).
- Se över om det inte finns annan lagstiftning (till exempel sekretess) som påverkar hur behörigheter bör sättas.

## Bilagor

1. Informationsutskick fördjupad kontroll behörighetsstyrning
2. Frågeutskick del 1
3. Frågeutskick del 2

# Information om fördjupad kontroll 2022

## Kontrollpunkt 11: Behörighetsstyrning

För att säkerställa säkerheten och en korrekt personuppgiftshantering inom en verksamhet behöver både tekniska och organisatoriska åtgärder vidtas. Exempel på tekniska säkerhetsåtgärder är att system utformas så att endast behöriga personer kan göra sökningar och att det finns behörighetskontrollsystem. En viktig och effektiv organisatorisk åtgärd i en verksamhet är behörighetsstyrning.

I artikel 32.2 i dataskyddsförordningen ställs krav på att den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå ska ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Obehörig är den som inte har legitim anledning att ta del av en handling eller uppgift i sin tjänsteutövning. Bestämmelser om sekretess utgör ofta men inte alltid en utgångspunkt för vilka uppgifter som någon får ta del av. Genom en ändamålsenlig behörighetsstyrning kan det säkerställas att ingen obehörig åtkomst sker inom verksamheten. Behörighetsstyrning sker genom att bland annat bedriva ett arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en medarbetare med en viss funktion eller roll ska ha. Det är viktigt att behörigheterna är anpassade och begränsade till det som är nödvändigt och i enlighet med gällande rättslig reglering. Dessutom behöver behörigheterna löpande kontrolleras och följas upp samt att åtkomstkontroller genomförs. En felaktig eller bristfällig behörighetsstyrning kan leda till exempelvis inskränkningar av den enskildes integritet eller personuppgiftsincidenter.

Den fördjupade kontrollen avser undersöka hur behörighetsstyrning används för att begränsa vilka uppgifter som medarbetarna får ta del av. Verksamhetens rutiner för tilldelning av behörigheter och åtkomster i IT-system kommer att granskas. Kontrollen kommer även omfatta verksamhetens uppföljning av medarbetares behörigheter och åtkomst till personuppgifter i IT-system samt om logg-/åtkomstkontroller används för att upptäcka och motverka obehörig åtkomst.

Syftet med den fördjupade kontrollen är att undersöka om medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter, att åtkomstkontroller genomförs och att därmed risken för obehörig åtkomst inom verksamheten minimeras.

## Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att besvara ett antal frågor samt att skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Insman. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i maj/juni.

**Obs!** Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

# Fördjupad kontroll 2022

## Kontrollpunkt 11: Behörighetsstyrning (del 1)

Del 1: Ni ombeds besvara frågorna nedan samt skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Insman.

- Beskriv systemets behörighetsstruktur och olika roller i systemet.
- Vilka roller får vilka behörigheter och vad baseras den bedömningen på?
- Vem beslutar om vilka som ska ha vilken behörighet?
- Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?
- Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.
- När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?
- Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?
- Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka?
- Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?
- Har verksamheten identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter?

**Obs!** Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 10 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

# Fördjupad kontroll 2022

## Kontrollpunkt 11: Behörighetsstyrning (del 2)

Del 2: Utifrån vad som framkommit i del 1 av den fördjupade kontrollen ombeds ni besvara frågorna nedan.

- Vad är det för personuppgifter som behandlas i systemet?
- Hur många registrerades personuppgifter hanteras i systemet?
- Hur många personer har behörigheter (inom aktuella enheter, men inklusive personuppgiftsbiträde, administratörer)?
- Föreligger det inbyggda svårigheter i aktuellt systemstöd att begränsa behörigheterna på så vis att personer enbart kan se sådana uppgifter som härrör till den egna förvaltningen? Varför/varför inte?
- Är Intraservice personuppgiftsbiträde för behandlingen/systemet och finns i sådana fall ett personuppgiftsbiträdesavtal? Om inte, varför?
- Hur kontrolleras personuppgiftsbiträdets, i detta fall Intraservice, behörigheter i systemet?
- Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
- Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
- Har ni identifierat specifika risker kopplat till nuvarande hantering av behörigheter? Varför/varför inte? Beakta såväl risker inifrån organisation som utanför (ex, intrång) för de registrerades rättigheter.
- Kan ni ge exempel på vad en ”särskild händelse” är som gör att ni behöver kontrollera loggarna? Vem bestämmer om kontroll ska ske?

**Obs!** Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.