Göteborgs Stad

# Årsrapport för dataskyddsarbetet 2022

## Göteborg & Co AB

2022-12-30

# 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 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 hantering av personuppgiftsincidenter under 2021

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om bolagets rutiner/handlingsplaner får önskat genomslag i praktiken. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen lämnat följande rekommendationer till verksamheten:

- Bolaget behöver ta fram en dokumenterad instruktion för hanteringen av personuppgiftsincidenter vilken bör, utöver den befintliga information som den idag innehåller, minst innehålla följande:
    - Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
    - Rutiner för hur medarbetarna inom organisationen ska agera om en incident inträffar.
    - Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten
    - Rutiner för anmälan av incident till Integritetsskyddsmyndigheten inom 72 timmar efter upptäckten.
    - Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- Komplettera rutinen med vem som beslutar gällande att bedöma om en anmälan till Integritetsskyddsmyndigheten ska göras.
- Se över bolagets kunskap gällande vad som är en personuppgiftsincident.
- Utbilda alla medarbetare om personuppgiftincidenter och hantering av dessa.

### 2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2021): Integritetspolicy

Verksamheten gavs följande rekommendationer:

- Ange samtliga rättigheter för den registrerade
- Upprätta en rutin för att säkerställa att informationen hålls uppdaterad
- Infoga en mer detaljerad beskrivning av de vanligaste behandlingarna

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med lämnade rekommendationer.

Exempel på åtgärder som vidtagits är att bolaget under året infört funktionen ”dataskyddskontakt”, och därmed har en person som ska kunna stötta bolaget i frågor som rör dataskyddsförordningen. Dataskyddskontakten har under året hjälpt till att uppdatera bolagets integritetspolicy och både den information som lämnas till externa besökare via hemsidorna och den som lämnas till bolagets medarbetare har uppdaterats. Bolaget anger att informationen särskilt uppdaterats gällande:

- Det finns en tydligare beskrivning av vanliga behandlingar som bolagets utför. Informationen är anpassad utifrån vilken målgrupp som bolaget tänker tar del av respektive information.
- Det finns en mer utförlig beskrivning av samtliga rättigheter som de registrerade har enligt dataskyddsförordningen.

- Det finns tydligare information om att bolaget omfattas av offentlighetsprincipen och den svenska arkivlagstiftningen, och hur detta påverkar de registrerade när bolaget behandlar deras personuppgifter.

Bolaget anger i uppföljningen att det ännu inte tagits fram en rutin för att säkerställa att integritetspolicyn uppdateras regelbundet, men att man fortsätter att arbeta för att få en sådan på plats. Skälet till att en sådan rutin inte ännu finns är för att bolaget har inväntat en organisationsförändring med personalförändringar som trädde i kraft i mitten av oktober 2022.

Utifrån bolagets svar bedömer dataskyddsombudet att fortsatt uppföljning kan ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

# 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. | |

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

## 2.4 Göteborg & Co:s 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 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:
Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men de bedöms inte vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker vad gäller att verksamheten ännu inte har en intern organisation för dataskyddsarbetet där roller, ansvar och beslutsmandat är tydligt definierade och att det inte heller finns rapporteringsvägar för dataskyddsfrågor som säkerställer att information når rätt nivå inom organisationen.

Bolaget har under året påbörjat arbetet med att etablera en intern dataskyddsorganisation, samt i december antagit en intern anvisning för dataskydd där roller och ansvar inom området beskrivs och tydliggörs. Framåt rekommenderas bolaget ge den interna dataskyddsorganisationen möjlighet att se över vilka resurser, vilken kompetens och vilka rutiner/anvisningar (kopplat till roller, ansvar och beslutsmandat) man behöver inom verksamheten för att kunna säkerställa dataskyddsperspektivet. Bolaget rekommenderas även fortsätta att regelbundet involvera dataskyddsombudet i dataskyddsfrågor.

### 2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter


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

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker framför allt vad gäller att dokumentera arbetssätt, följa upp incidenter och informera medarbetare

om vad en personuppgiftsincident är och vad medarbetare ska göra när en incident inträffar.

Datsskyddsombudet bedömer att verksamhetens arbete med personuppgiftsincidenter behöver utvecklas. De risker som identifierats medför att det finns ett behov av att både hitta långsiktigt hållbara sätt för att informera medarbetare, ta fram rutiner för de som arbetar med personuppgiftsincidenter såväl som att utveckla ett arbete med att systematiskt följa upp inträffade incidenter. Eftersom verksamheten har svarat att de inte fullt ut informerar medarbetare om vad personuppgiftsincidenter är, ser dataskyddsombudet risker med att incidenter inte identifieras och därmed heller inte dokumenteras och anmäls till tillsynsmyndigheten. Att bolaget inte haft någon incident under 2021 indikerar också att kunskapen om vad som utgör en personuppgiftsincident behöver öka inom verksamheten.

Bolaget rekommenderas utifrån svaren att fokusera på att informera medarbetare, ta fram rutiner för dem som arbetar med personuppgiftsincidenter samt utveckla ett arbete med att systematiskt följa upp inträffade incidenter.

I samband med genomgången av årsrapporten informerades dataskyddsombudet om att bolaget i november 2022 beslutat att dataskyddsenhetens e-utbildning ”Dataskydd på jobbet” ska tas upp på arbetsplatsträffar inom bolaget, samt att den ska vara obligatorisk för chefer att genomföra. Bolaget arbetar även med att ta fram en rutin för hanteringen av incidenter och planerar för utbildning av medarbetare framåt. Dataskyddsombudet kan se att de påbörjade åtgärderna ligger i linje med lämnade rekommendationer och uppmuntrar bolaget till att fortsätta med arbetet.

Fler rekommendationer lämnas inom ramen för den fördjupade kontrollen (se Bilaga 2).

### 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker framför allt vad gäller att genomföra efterlevnadskontroller av personuppgiftsbiträden och att

bedöma hela kedjan av underbiträden samt huruvida överenskommelser eller avtal behöver tecknas när en leverantör anlitas.

Utifrån skattningen rekommenderas bolaget att ta fram en rutin för utförandet av regelbundna efterlevandskontroller av anlitade personuppgiftsbiträden, en rutin/anvisning för att bedöma ansvarsförhållanden utifrån GDPR vid anlitande av nya leverantörer, eller när samarbeten sker, samt en rutin för att kontrollera hela kedjan av biträden och underbiträden vid anlitande av ny leverantör.

### 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 anger i enkäten att ca 25 % av bolagets personuppgiftsbehandlingar finns upptagna i nuvarande personuppgiftsbehandlingsregister. Avsaknaden av behandlingar innebär en risk då bolaget på grund av detta inte uppfyller dess skyldighet att föra register över personuppgiftsbehandlingar enligt artikel 30 GDPR. Enligt verksamhetens skattning finns även kvarstående risker framför allt vad gäller ansvarsfördelning och rutiner för att uppdatera personuppgiftsregister.

Vid genomgången av årsrapporten informerades dataskyddsombudet om att bolaget i september påbörjat ett arbete med att uppdatera registret, och att man nu bedömer att över 50 % av bolagets personuppgiftsbehandlingar nu finns registrerade. Man arbetar även med att ta fram en intern rutin för arbetet med registret.

Bolaget rekommenderas att under 2023 prioritera arbetet med att säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret, samt att färdigställa rutinen med ansvar och arbetssätt. Den interna dataskyddsorganisationen rekommenderas även fundera över på vilket sätt personuppgiftsregistret kan användas som del i det löpande dataskyddsarbetet.

### 2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd


Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker vad gäller att ha en övergripande strategi för arbetet med dataskydd och att arbeta systematiskt med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Verksamheten har ännu inte en informationssäkerhetspolicy för behandling av personuppgifter eller dokumenterade rutiner som hjälper till att säkerställa att de styrande dokument som reglerar personuppgiftsbehandlingar hålls uppdaterade. Verksamheten har heller inte dokumenterade rutiner för att efterleva kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster och genomför ännu inte regelbundna interna kontroller för att säkerställa följsamhet gentemot GDPR.

Sammantaget visar svaren att det saknas en överblick och en tydlig styrning i hur dataskyddsarbetet bedrivs, vilket innebär en risk eftersom man då bland annat riskerar att fokusera sina resurser på fel frågor. Det är viktigt att bolaget framåt identifierar vilka som är de största riskerna inom verksamheten och ser över hur arbetet med att hantera dessa ska prioriteras.

Vidare bör ett systematiskt dataskyddsarbete bedrivas utifrån övergripande strategier för verksamheten avseende både dataskydd och informationssäkerhet. Bolaget har i dialog med dataskyddsombudet angett att det inom verksamheten pågår ett arbete med att ta fram en policy för informationssäkerhet, men att man avvaktar att fastställa denna tills stadsrevisionen gjort klart sin granskning i frågan. Det är positivt att bolaget arbetar med frågan och bolaget rekommenderas innan informationssäkerhetspolicyn fastställs säkerställa att dataskyddsdelarna finns med.

### 2.4.6 Kontrollpunkt 6: Utbildning


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

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker vad gäller regelbundet utbilda och informera medarbetarna inom dataskydd. Verksamheten har ännu inte kartlagt vilken nivå av dataskyddskunskap som olika befattningars arbete kräver för att planera utbildningsinsatser eller infört rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetarna efter genomförda utbildningar.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Verksamheten rekommenderas därför fortsätta ge medarbetarna möjlighet att delta i utbildningar för att höja den allmänna kunskapsnivån inom dataskydd. Den

interna dataskyddsorganisationen bör också ges rätt förutsättningar för att kunna genomföra informationsinsatser.

Vidare, för att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser, rekommenderas verksamheten att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

Bolaget rekommenderas även se över hur man internt inom verksamheten framåt skulle kunna arbeta regelbundet med att utbilda och informera medarbetare i dataskydd.

### 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:
Informationskravet utgör en av grunderna i GDPR och handlar om att den registrerade ska få information hur hens personuppgifter behandlas.

Enligt verksamhetens skattning finns kvarstående risker framför allt vad gäller att se till att integritetspolicyn uppfyller kraven på information enligt GDPR och att de registrerade på ett enkelt sätt kan nå integritetspolicyn från samtliga av verksamhetens digitala kanaler. Skattningen visar även att verksamheten inte bedömer att integritetpolicyn uppfyller kraven på information enligt GDPR, och därmed uppfyller inte bolaget sin informationsplikt.

För att bolaget ska kunna uppfylla sin informationsplikt rekommenderas bolaget framåt prioritera arbetet med att se över integritetspolicyn och uppdatera den så att informationen uppfyller kraven enligt artikel 13 och 14 GDPR.

### 2.4.8 Kontrollpunkt 8: E-post och dokumenthantering


Kontrollpunkten avser verksamhetens rutiner för e-post 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker vad gäller rutiner för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut. Vidare saknas anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Det finns också risker vad gäller avsaknad av rutiner och anvisningar för hantering av personuppgifter i e-post och verksamheten anger även att man inte informerar de registrerade om hur deras personuppgifter hanteras direkt i samband med upprättande av kontakt.

Utifrån svaren bedömer dataskyddsombudet att verksamhetens arbete med e-post och dokumenthantering behöver utvecklas och rekommenderar bolaget att ta fram anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas, samt för hur personuppgifter ska hanteras i e-post. Bolaget rekommenderas även ta del av Göteborg Stads mall för e-postsignatur, där det framgår att en länk till hanteringen av verksamhetens personuppgifter ska infogas i signaturen, och lägga till en sådan länk i bolagets e-postsignatur.

### 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:
Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Det är därför mycket viktigt att verksamheten säkerställer att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingar och att det finns rutiner för att genomföra och dokumentera konsekvensbedömningar.

Verksamhetens resultat visar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Verksamheten har bland annat angett att inte någon av verksamhetens personuppgiftsbehandlingar har riskbedömts (tröskelanalys) eller varit föremål för en konsekvensbedömning utifrån att höga risker identifierats. Enligt verksamhetens skattning finns det även risker utifrån att fastställda rutiner och arbetssätt för att arbeta med konsekvensbedömningar i stora delar saknas.

Utifrån de höga risker som föreligger inom kontrollpunkten bedömer dataskyddsombudet att verksamhetens arbete med konsekvensbedömningar under 2023 behöver prioriteras. Verksamheten rekommenderas i arbetet fokusera på att kontrollera verksamhetens personuppgiftsbehandlingar utifrån höga risker och

bedöma för vilka behandlingar konsekvensbedömningar behöver genomföras, samt ta fram en plan för arbetet framåt. Inom ramen för arbetet ingår också delar som att se över hur uppföljning av de åtgärder som beslutats att genomföras för att hantera de risker som identifierats i en konsekvensbedömning ska hanteras, samt tydliggöra vem/vilka befattningar som har mandat att fatta beslut inom ramen för arbetet med konsekvensbedömningar och hur dessa beslut ska dokumenteras.

### 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att inga direkta risker är identifierade. Då dataskyddsombudet under året enbart blivit involverad i någon enstaka fråga, och då i ett sent skede i processen, rekommenderas verksamheten framåt se över hur det kan säkerställas att dataskyddsombudet involveras i ett tidigt skede i uppstart av nya IT-projekt, vid införande av nya system/tjänster eller i samband med upphandlingar.

### 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men dessa bedöms inte vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker vad gäller målgruppsanpassad information för digitala verktyg samt rutiner för att systematiskt följa upp och kontrollera att användningen av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policys. Vidare saknas en dokumenterad och tydlig överblick över kommunikationskanaler och rutiner för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.

Utifrån svaren rekommenderas bolaget kartlägga de kommunikationskanaler som används inom bolaget, samt ta fram rutiner för att systematiskt följa upp och

kontrollera att användningen av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policys. Bolaget rekommenderas även se över hur dataskyddsperspektivet ska kunna säkerställas vid införandet och användandet av kostnadsfria tjänster så som gratis appar och sociala medier.

Därtill noterar dataskyddsombudet att bolaget använder flera sociala medier. Dataskyddsombudet vill därför lyfta att denna hantering strider mot de rekommendationer som dataskyddsombudet lämnat gällande användningen av sociala medier (med amerikanska moderbolag). Frågan om användning av sociala medier bör även i grunden ses över. I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även Instagram och Youtube är exempel på sociala medier som överför personuppgifter till USA. Ingen av dessa plattformar har angett att de vidtagit några extra skyddsåtgärder och utifrån det saknar alla överföringar som görs inom dessa tjänster laglig grund. När det gäller användningen av sociala medier rekommenderar dataskyddsombudet att bolaget kartlägger dessa behandlingar och genomför en konsekvensbedömning för att kontrollera att behandlingarna är förenliga med GDPR. Dataskyddsombudet avråder bolaget från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

### 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder. Enligt verksamhetens skattning finns kvarstående risker eftersom det inom verksamheten ännu inte finns en utbredd medvetenhet om vilka rättigheter de registrerade har, när de registrerades rättigheter begränsas eller rutiner för hur dessa situationer ska hanteras. Det saknas även rutiner för att bedöma en registrerads invändning mot en personuppgiftsbehandling, hantera tillbakadragande av samtycke från en registrerad så väl för att hantera en begäran om registerutdrag. Verksamheten har inte heller en dokumenterad process för att kunna hitta/få tillgång till efterfrågad information vid en begäran om registerutdrag.

Utifrån skattningen bedömer dataskyddsombudet att verksamhetens arbete med hantering av registrerades rättigheter behöver prioriteras under 2023, och rekommenderar bolaget att som ett första steg ta fram en rutin för att hantera en begäran om registerutdrag. Utöver det rekommenderas bolaget arbeta med att stärka medarbetares kunskap om registrerades rättigheter, samt ta fram en rutin för att hantera situationen då ett samtycke från en registrerad dras tillbaka.

## 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:

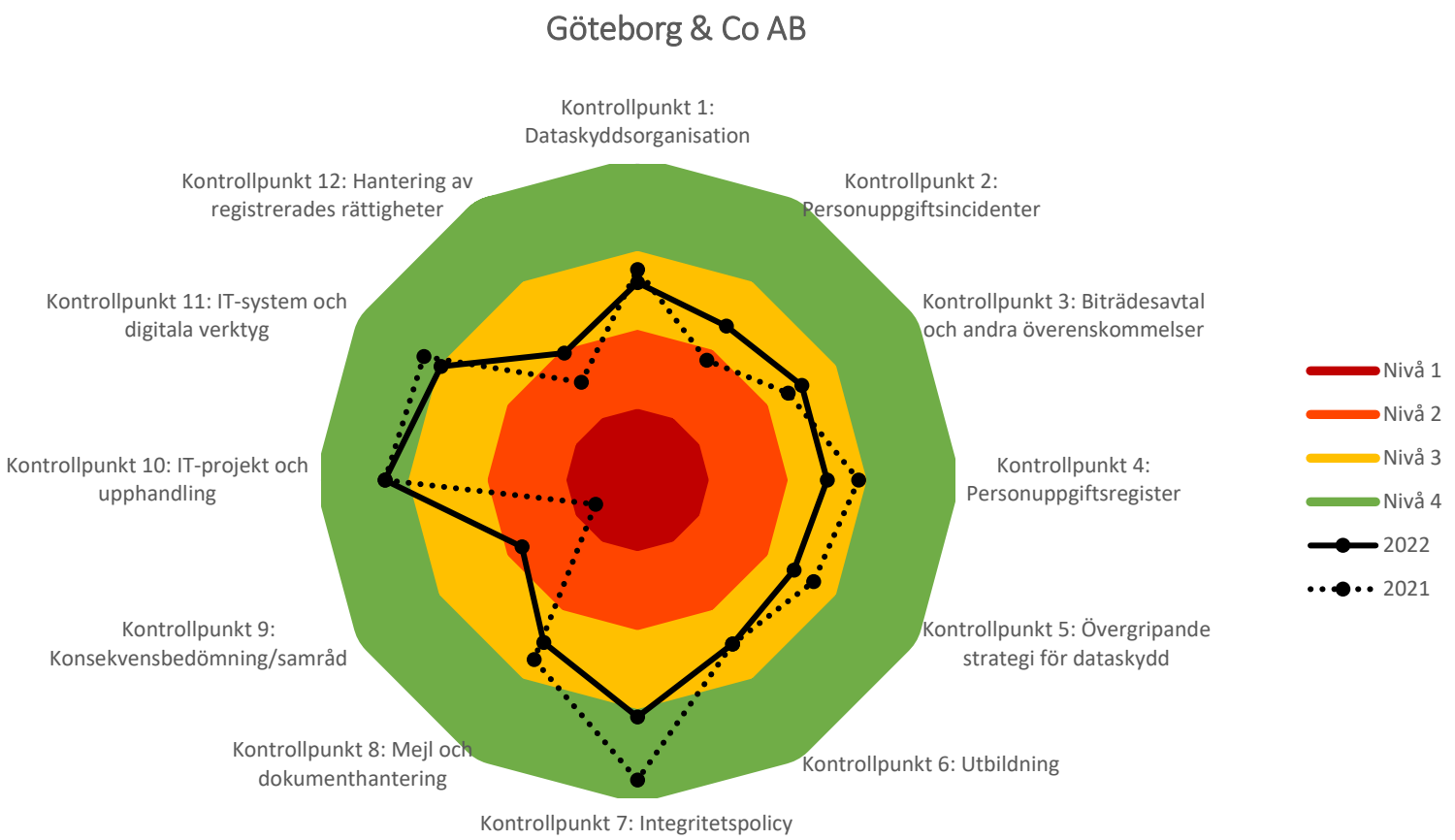
- Kontrollpunkt 4: Personuppgiftsregister
  : Se över och komplettera registret med de behandlingar som saknas för att uppfylla bolagets skyldighet att föra register över personuppgiftsbehandlingar enligt artikel 30 GDPR.
- Kontrollpunkt 6: Utbildning
  : Öka den generella kunskapsnivån inom dataskydd hos medarbetare, inkl. hantering av personuppgiftsincidenter.
- Kontrollpunkt 9: Konsekvensbedömningar/Samråd
  : Kontrollera verksamhetens personuppgiftsbehandlingar utifrån höga risker och planera för genomförandet av konsekvensbedömningar för de behandlingar detta krävs.
- Kontrollpunkt 12: Hantering av registrerades rättigheter
  : Ta fram en rutin för att hantera en begäran om registerutdrag från en registrerad.

# 3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022

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



# Fördjupad kontroll 2022

Hantering av personuppgiftsincidenter under 2021

## Bakgrund

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om bolagets rutiner/handlingsplaner får önskat genomslag i praktiken. Kontrollen har genomförts i två delar där del ett har bestått av att verksamheten har ombetts att skicka in dokumentation av rutiner/handlingsplaner för hanteringen av incidenter och dokumentation över inträffade incidenter under 2021. Del två har bestått av frågor kopplade till organisationens incidenthantering.

## Iakttagelser från kontrollen

Personuppgiftsincidenter kan leda till allvarliga konsekvenser för registrerade personer och det är av stor vikt att de hanteras på ett korrekt sätt. Enligt dataskyddsförordningen ska vissa typer av personuppgiftsincidenter anmälas till tillsynsmyndigheten och i vissa fall ska även de registrerade informeras. Även de personuppgiftsincidenter som inte behöver anmälas till tillsynsmyndigheten ska dokumenteras.

### IMY:s checklista vid personuppgiftsincidenter

Integritetsskyddsmyndigheten (IMY) har på sin hemsida publicerat en checklista för personuppgiftsansvariga att använda i sitt arbete med personuppgiftsincidenter. Den består bl.a. av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter och vad som behöver göras vid redan inträffade incidenter. IMY lyfter att det av rutinerna bör framgå hur en bedömning av riskerna för de registrerade ska gå till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten. Det bör också framgå hur man bedömer om de registrerade ska informeras, hur det ska gå till och vad informationen ska innehålla.

### Göteborg & Co. AB:s hantering av personuppgiftsincidenter

Rutiner och handlingsplaner

Göteborg & Co. AB (bolaget) har en processbeskrivning för hantering av personuppgiftsincidenter som gäller för alla anställda på bolaget. Beskrivningen innefattar en process för hantering av personuppgiftsincidenter. I beskrivningen framgår det att om en incident identifieras ska IT-chef och systemansvarig informeras omgående. En rapport ska upprättas och bedömning gällande incidenten ska ske. Beroende på dess omfattning ska, enligt beskrivningen, dataskyddsombud och Integritetsskyddsmyndigeten informeras. Incidenten ska enligt beskrivningen sedan lösas och dokumenteras.

Beskrivningen innehåller vilken information som ska rapporteras till tillsynsmyndigheten i de fall incidenten ska anmälas till Integritetsskyddsmyndigheten.

### Personuppgiftsincidenter under 2021

Av det inskickade underlaget framgår att bolaget under år 2021 inte gjort någon bedömning av om en händelse är en personuppgiftincident.

### Information till anställda

Bolaget uppger att man inte vidtagit några åtgärder för att säkerställa att bolagets anställda vet vad en personuppgiftsincident är och hur de ska gå till väga vid en inträffad personuppgiftincident.

## Dataskyddsombudets rekommendationer

### Rutiner och handlingsplaner

Bolaget har en processbeskrivning som förklarar arbetsgången vid hantering av en personuppgiftincident. Det saknas dock mycket information som kan vara bra att en rutin innehåller. För att göra hanteringen mer lättillgänglig för verksamheten kan det enligt dataskyddsombudet finnas skäl att utöka rutinen med fler konkreta beskrivningar av vad en personuppgiftincident är samt mer konkreta beskrivningar av hur en incident och risken för de registrerade ska bedömas.

Sammantaget rekommenderar dataskyddsombudet att bolaget konkretiserar sin rutin och kompletterar den med en instruktion eller stödmaterial/metod som anger hur en incident och risken för de registrerade kan bedömas. Rutinen bör även innehålla vem eller vilka inom bolaget som ska bedöma risker och besluta om hanteringen av personuppgiftsincidenter.

### Personuppgiftsincidenter under 2021

Bolaget har angett att de inte haft någon personuppgiftincident under 2021. Inom en verksamhet är det normalt att det sker ett flertal incidenter varje år och det är troligt att så även har skett hos bolaget, trots att det inte upptäckts, dokumenterats och bedömts. Ett felskickat mejl är exempelvis den vanligast förekommande personuppgiftsincidenten, vilket inte hade varit förvånande om bolaget hade haft vid ett eller flera tillfällen under året 2021. Att bolaget därför inte dokumenterat någon incident under 2021 visar på bristande kunskap om och hantering av incidenter inom bolaget.

Dataskyddsombudet ser det dock som positivt att bolaget i sitt svar framhåller att det troligtvis inträffat en eller flera personuppgiftincidenter trots att detta inte fångats upp av deras nuvarande rutiner. Det är också positivt att bolaget uppger att man under hösten 2021 påbörjat ett arbete med att se över rutinen för hantering av personuppgiftincidenter.

### Information till anställda

Bolaget har inte vidtagit några åtgärder för att utbilda sina anställda i vad en personuppgiftincident är och hur de ska hantera en inträffad incident. Bolaget uppger att man kommer påbörja ett arbete med att utbilda bolagets chefer och medarbetare.

Den bristande rutin som finns gällande hantering av personuppgiftincidenter och de faktum att man inte utbildat anställda i vad en personuppgiftincident är eller hur den ska hanteras visar att anställda saknat kännedom om vad en personuppgiftincident är och hur den ska hanteras vid upptäckt.

Dataskyddsombudet rekommenderar att bolaget ser över sin rutin samt utbildar sina anställda i vad en personuppgiftsincident är och hur den ska hanteras, för att säkerställa att incidenter inte missas.

## Sammanfattning

- Bolaget behöver ta fram en dokumenterad instruktion för hanteringen av personuppgiftsincidenter vilken bör, utöver den befintliga information som den idag innehåller, minst innehålla följande:
    - Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
    - Rutiner för hur arbetstagarna inom organisationen ska agera om en incident inträffar.
    - Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten
    - Rutiner för anmälan av incident till Integritetsskyddsmyndigheten inom 72 timmar efter upptäckten.
    - Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- Komplettera rutinen med vem som beslutar gällande att bedöma om en anmälan till Integritetskyddsmyndigheten ska göras.
- Se över medarbetares kunskap gällande vad som är en personuppgiftsincident.
- Utbilda alla medarbetare om personuppgiftincidenter och hantering av dessa.

## Bilagor

- Information om fördjupad kontroll 2022.
- Frågeunderlag fördjupad kontroll 2022, del 1 och del 2.

# Information om fördjupad kontroll 2022

## Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Personuppgiftsansvariga och personuppgiftsbiträden ska arbeta medvetet och proaktivt för att förhindra personuppgiftsincidenter. Om det ändå sker en incident ska det finnas förutsättningar för att hantera den snabbt och på rätt sätt. Den personuppgiftsansvarige är enligt artikel 33.5 GDPR skyldig att dokumentera samtliga inträffade incidenter, oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 GDPR, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska innefatta omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om det inte är osannolikt att en inträffad personuppgiftsincident medför en risk för registrerades fri- och rättigheter ska, enligt artikel 33 GDPR, den personuppgiftsansvarige anmäla incidenten till Integritetsskyddsmyndigheten inom 72 timmar efter det att personuppgiftsansvarig fått vetskap om incidenten. Den personuppgiftsansvarige behöver vid varje inträffad incident bedöma i vilken utsträckning som den uppkomna incidenten påverkar de registrerades fri- och rättigheter.

## Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumentation av rutiner/handlingsplaner för att hantera incidenter samt er dokumentation avseende redan inträffade personuppgiftsincidenter. I del två ombeds ni att svara på ett antal frågor kopplade till er incidenthantering.

Dataskyddsombudet kommer sedan att sammanställa underlaget i årsrapporten.

# Fördjupad kontroll 2022

## Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Del 1: Dokumentation för er att skicka in till dataskyddsombudet:

1. Rutiner/handlingsplaner/instruktioner för att hantera personuppgiftsincidenter
2. Dokumentation av inträffade personuppgiftsincidenter
    a. Dokumentation av incidenter som har anmälts till tillsynsmyndigheten
    b. Dokumentation av incidenter som endast har dokumenterats internt
3. Dokumentation av utredningar kring potentiella personuppgiftsincidenter

Underlaget ska ha inkommit till dataskyddsombudet **senast den 15 mars 2022.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.

# Fördjupad kontroll 2022

## Hantering av personuppgiftsincidenter under 2021

**Del 2**

Frågor att besvara:

1. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
2. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida incidenten ska anmälas till tillsynsmyndigheten.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
3. Hur ni säkerställer att era anställda vet vad en personuppgiftsincident är och hur de ska gå tillväga vid inträffade personuppgiftsincidenter.

Svaren ska ha inkommit till ert dataskyddsombud **senast den 10 juni 2022.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.