



# **Årsrapport för dataskyddsarbetet 2023**

**Exploateringsnämnden**

2023-12-19

# Innehåll

|          |                                                                                             |           |
|----------|---------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Inledning .....</b>                                                                      | <b>3</b>  |
| 1.1      | Dataskyddsombud i Göteborgs Stad .....                                                      | 3         |
| <b>2</b> | <b>Särskilda iakttagelser 2023 .....</b>                                                    | <b>4</b>  |
| 2.1      | Stadenövergripande .....                                                                    | 4         |
| 2.1.1    | Förutsättningar för en hållbar digitalisering .....                                         | 4         |
| <b>3</b> | <b>Granskning av dataskyddsarbetet 2023.....</b>                                            | <b>5</b>  |
| 3.1      | Kontroll av fasta kontrollpunkter.....                                                      | 5         |
| 3.2      | Resultat från kontrollen 2023 .....                                                         | 5         |
| 3.2.1    | Kontrollpunkt 1: Dataskyddsorganisation .....                                               | 6         |
| 3.2.2    | Kontrollpunkt 2: Personuppgiftsincidenter .....                                             | 6         |
| 3.2.3    | Kontrollpunkt 3: Biträdesavtal och andra överenskommelser ..                                | 7         |
| 3.2.4    | Kontrollpunkt 4: Register över personuppgiftsbehandlingar ...                               | 8         |
| 3.2.5    | Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet                                 | 8         |
| 3.2.6    | Kontrollpunkt 6: Utbildning .....                                                           | 9         |
| 3.2.7    | Kontrollpunkt 7: Informationsplikt .....                                                    | 10        |
| 3.2.8    | Kontrollpunkt 8: E-post och dokumenthantering.....                                          | 10        |
| 3.2.9    | Kontrollpunkt 9: Konsekvensbedömning/samråd .....                                           | 11        |
| 3.2.10   | Kontrollpunkt 10: IT-projekt och upphandling .....                                          | 11        |
| 3.2.11   | Kontrollpunkt 11: IT-system och digitala verktyg .....                                      | 12        |
| 3.2.12   | Kontrollpunkt 12: Hantering av registrerades rättigheter .....                              | 12        |
| 3.3      | Uppföljning .....                                                                           | 12        |
| 3.3.1    | Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller ..... | 12        |
| <b>4</b> | <b>Rekommenderade fokusområden 2024 .....</b>                                               | <b>13</b> |
| <b>5</b> | <b>Bilagor .....</b>                                                                        | <b>14</b> |

# 1 Inledning

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. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

## 1.1 Dataskyddsombud i Göteborgs Stad

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Enligt lag ska dataskyddsombudet rapportera till högsta förvaltningsnivå och i Göteborgs Stad innebär det att dataskyddsombudet rapporterar direkt till nämnder och styrelser. Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är 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.

## 2 Särskilda iakttagelser 2023

### 2.1 Stadenövergripande

#### 2.1.1 Förutsättningar för en hållbar digitalisering

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen 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 inom Göteborgs Stad.

Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter. Verksamheterna behöver följa dataskyddslagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskyddsperspektivet förbises i digitaliseringsarbetet. Fokus behöver därför skiftas från att betrakta reglerna i dataskyddslagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt.

# 3 Granskning av dataskyddsarbetet 2023

## 3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts 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.

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.<sup>1</sup>

| Riskenivå | Beskrivning                                                                                                            | 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 bedriver ett systematiskt dataskyddsarbete. |         |

## 3.2 Resultat från kontrollen 2023

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. För beskrivning av respektive kontrollpunkt se bilaga 2.

<sup>1</sup> I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

### 3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar verksamhetens bedömning och anser att förvaltningen har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Exploateringsförvaltningen har kunskaps- och kompetensmässigt goda förutsättningar för att bedriva dataskyddsarbete.

Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

### 3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar verksamhetens bedömning och anser att förvaltningen har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Förvaltningens svar visar att verksamheten har dokumenterade arbetssätt på plats för att hantera personuppgiftsincidenter. Samtidigt är det förhållandevis få incidenter som rapporteras, detta är i sig ofta en indikation på en bristande medvetenhet kring vad en incident är och hur den ska hanteras snarare än att inga incidenter inträffar.

Dataskyddsombudet rekommenderar därför att:

- Förvaltningen fortsätter arbeta med frågan genom kontinuerliga kunskapshöjande insatser hos medarbetarna för att ge dessa verktyg för att upptäcka incidenter och veta hur de ska hanteras.

### 3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar verksamhetens bedömning och anser att förvaltningen har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Vid årsskiftet 2022/2023 upphörde fastighetskontoret och exploateringsförvaltningen inrättades i dess ställe. I samband med omorganiseringen förändrades verksamheten på ett sådant sätt att personuppgiftsbehandlingar upphörde och/eller tillkom på grund av förändringar i organiseringen för de stadsutvecklande nämnderna. För exploateringsförvaltningens del innebar omorganiseringen att flera av de rekommendationer som dataskyddsombudet lämnade inom ramen för sin fördjupade kontroll avseende dåvarande Fastighetskontorets hantering av biträdesavtal och andra överenskommelser, upphörde att vara relevanta. Dessa behandlingar utförs i stället inom andra NOS-förvaltningar.

De svar som verksamheten lämnat på dataskyddsombudets kontrollfrågor indikerar att förvaltningen har omhändertagit de kvarstående rekommendationerna.

Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. En förbättringsåtgärd som dataskyddsombudet identifierat utifrån förvaltningens svar handlar om dokumenterade arbetssätt för att bedöma och reglera situationer där det finns ett delat personuppgiftsansvar.

Dataskyddsombudet rekommenderar därför att förvaltningen:

- Tar fram arbetssätt för att bedöma om det föreligger ett gemensamt personuppgiftsansvar vid anlitande av leverantör/inledande av samarbeten, gärna i samarbete med övriga NOS-förvaltningar.

### 3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlings

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. Till exempel har det i dialog med verksamheten framkommit att förvaltningens dataskyddskontakt fortfarande upptäcker system och andra verktyg, i vilka det utförs personuppgiftsbehandlings, som inte framgår av registret. Förvaltningen har uppgett i dialog med dataskyddsombudet att man i arbetet med att ta fram uppdaterad och aktuell dokumenthanteringsplan (se kontrollpunkt 8) aktivt arbetar för att koppla ihop detta med behandlingsregistret för att på så sätt täcka upp eventuella luckor avseende personuppgiftsbehandlings som utförs. Dataskyddsombudet ser mycket positivt på detta och anser att det är ett effektivt arbetssätt.

### 3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där förvaltningen behöver genomföra åtgärder. Framför allt handlar det om att verksamheten behöver arbeta med att ta fram och implementera en övergripande strategi för dataskyddsfrågorna. I dialog med förvaltningen, genom dataskyddsombudets avstämningar, framkommer också att dokumenterade arbetssätt och styrande dokument finns på plats, men att följsamheten i organisationen lämnar en del att önska. Detta är inte ett helt ovanligt

problem, inte desto mindre är det viktigt att förvaltningen aktivt arbetar för att upprätthålla en hög följsamhet gentemot lagstiftningen, till exempel genom interna kontroller. Det är därför mycket positivt att förvaltningen uppger sig ha startat ett sådant internt arbete med utgångspunkt i det kontrollarbete som dataskyddsombudet utför.

Förvaltningen uppger också att man aktivt strävar efter att koppla ihop dataskydds- och informationssäkerhetsfrågor för att nå ut i verksamheten och använda resurser på ett effektivt och synergistiskt sätt, även detta är något som dataskyddsombudet ser mycket positivt på.

Dataskyddsombudet rekommenderar därför förvaltningen att:

- Ta fram och implementera en övergripande strategi för dataskyddsfrågorna.
- Fortsätta att regelbundet genomföra interna kontroller för att säkerställa följsamhet gentemot GDPR.

### 3.2.6 Kontrollpunkt 6: Utbildning



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som förvaltningen bedömningen att de inte är omfattande, brådskande eller allvarliga.

Förvaltningen uppger att man arbetar aktivt med frågan genom att dataskyddskontakt medverkar på APT:er och håller gemensamma utbildningsinsatser avseende GDPR/OSL/IT, med mera. Sammantaget så gör verksamheten en hel del för att uppnå och bibehålla en god kunskapsnivå. Dataskyddsombudet ser detta som positivt. All kunskap behöver också bibehållas, därför är det av vikt att olika utbildningsinsatser kontinuerligt följs upp.

Med ledning av verksamhetens svar rekommenderas förvaltningen att:

- Ta fram dokumenterade arbetssätt för att för att följa upp och bibehålla kunskapsnivån hos medarbetare efter genomgångna utbildningar.

### 3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Efter avstämning med förvaltningen i december 2023 uppger verksamheten att man vidtagit åtgärder avseende aktualiteten för de personuppgiftsbehandlingar som finns med i integritetspolicyn på goteborg.se, samt att man har för avsikt att göra informationen mer användarvänlig och lättillgänglig. Några särskilda rekommendationer lämnas därför inte, men dataskyddsombudet kommer följa upp frågan inom ramen för ordinarie avstämningsmöten med verksamheten under 2024.

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

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och som kräver omgående åtgärder. I dialog med verksamheten framkommer det att arbetet med att ta fram en uppdaterad dokumenthanteringsplan pågår och att resurser är avsatta för att utföra arbetet.

Dataskyddsombudet rekommenderar förvaltningen att:

- Prioritera arbetet med att ta fram en aktuell och fastställd dokumenthanteringsplan som omfattar samtliga av verksamhetens processer och i vilken det framgår hur handlingar som innehåller personuppgifter ska hanteras.
- Ta fram dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut.
- Ta fram dokumenterade arbetssätt för att informera medarbetare om dokumenthantering och gallring kopplat till kraven enligt GDPR.
- Utreda för hur stor andel av de personuppgiftsbehandlingar som har informationsklassificerats som informationen är aktuell och ta fram

dokumenterade arbetssätt som säkerställer att informationen uppdateras i takt med förändringar

### 3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudet är tveksam till förvaltningens uppgift om att 75% av verksamhetens riskfyllda behandlingar har bedömts. Framför allt avseende HR-området saknas det bedömningar, men även för administrativa processer som registrering och utlämnande av allmänna handlingar, för att nämna några exempel

Dataskyddsombudet rekommenderar därför att förvaltningen:

- Gör en översyn av vilka behandlingar med höga risker man inte gjort någon konsekvensbedömning för och i steg två inleder arbetet med att ta fram bedömningar för dessa.
- Tar fram dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas.
- Tar fram dokumenterade arbetssätt för att följa upp de åtgärder som beslutats att genomföras för att hantera de risker som identifierats i en konsekvensbedömning.
- Fastställer ett dokumenterat arbetssätt för att, i de fall det bedöms lämpligt, kunna inhämta de registrerades synpunkter (på en behandling).

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

Verksamhetens skattning av risknivå



#### Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten

har gjort avseende risknivå. Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

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

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

### 3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

## 3.3 Uppföljning

### 3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Exploateringsnämnden inrättades den förste januari 2023 som ett led i den nya organiseringen av de stadsutvecklande nämnderna. Eftersom nämnden utgör en ny förvaltningsmyndighet sker ingen uppföljning av tidigare utförda kontroller.

## 4 Rekommenderade fokusområden 2024

Utifrån höga föreliggande risker för de registrerades fri- och rättigheter har dataskyddsombudet identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa listas i punktform enligt nedan. Detta är områden som dataskyddsombudet särskilt kommer att följa upp framåt. Uppföljningen kommer ske löpande under det kommande året, i dialog med verksamheten.

Utifrån identifierade risker är dataskyddsombudets sammanfattande rekommendationer till nämnden/bolaget att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 8: E-post och dokumenthantering

Förvaltningen bör prioritera arbetet med att ta fram en aktuell och fastställd dokumenthanteringsplan som omfattar samtliga av verksamhetens processer och i vilken det framgår hur handlingar som innehåller personuppgifter ska hanteras.

I samband med detta bör man också ta fram dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Förvaltningen rekommenderas att göra en översyn av vilka behandlingar med höga risker man inte gjort någon konsekvensbedömning för och i steg två inleda arbetet med att ta fram bedömningar för dessa.

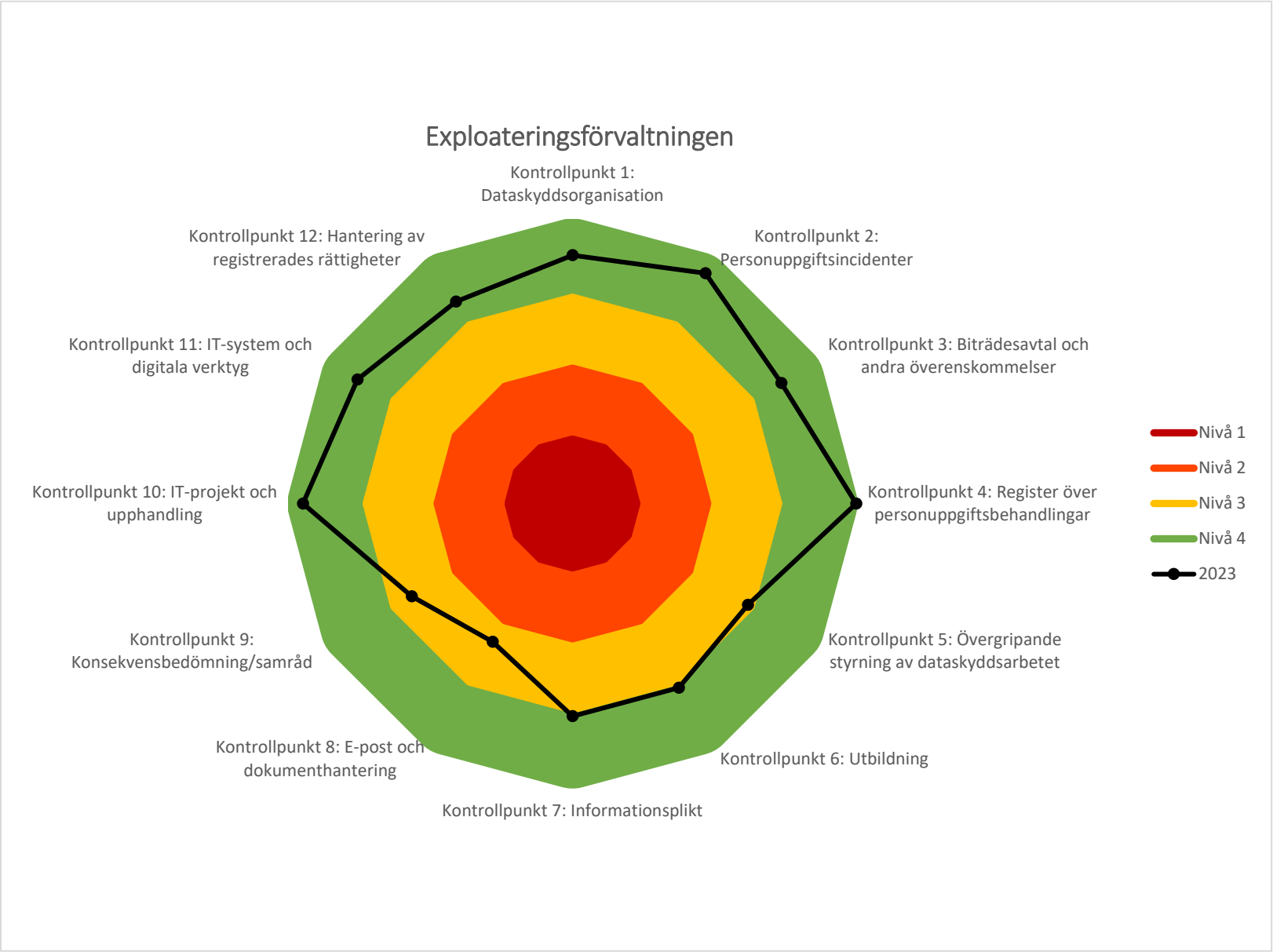
I samband med detta bör förvaltningen också ta fram dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas, samt dokumenterade arbetssätt för att följa upp de åtgärder som beslutats att genomföras för att hantera de risker som identifierats i en konsekvensbedömning.

## 5 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

**Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.**





# Exploaterings- förvaltningen

## Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

# Innehåll

|          |                                       |          |
|----------|---------------------------------------|----------|
| <b>1</b> | <b>Bakgrund</b>                       | <b>3</b> |
| 1.1      | Ny utformning av kontrollarbetet      | 3        |
| <b>2</b> | <b>Kontrollarbetet 2023–2024</b>      | <b>4</b> |
| 2.1      | Kontrollarbetets delar                | 4        |
| 2.2      | Tidplan för kontrollarbetet 2023–2024 | 5        |
| <b>3</b> | <b>Kontroller</b>                     | <b>5</b> |
| 3.1      | Fasta kontrollpunkter                 | 5        |
| 3.2      | Fördjupad kontroll                    | 6        |
| 3.3      | Uppföljning av genomförda kontroller  | 6        |
| <b>4</b> | <b>Rapportering</b>                   | <b>7</b> |
| 4.1      | Årsrapport                            | 7        |
| 4.2      | Särskilt yttrande                     | 7        |
| <b>5</b> | <b>Kontakt</b>                        | <b>7</b> |

# 1 Bakgrund

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. 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 personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskyddsombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

## 1.1 Ny utformning av kontrollarbetet

För att ytterligare stärka kvaliteten i verksamheternas dataskyddsarbete kommer dataskyddsombudets kontrollarbete att framgent löpa över tvåårsperioder. Tidigare har kontrollarbetet planerats årsvis, vilket ändras från och med år 2023. För att också underlätta verksamheternas egen planering kommer en ny kontrollplan att skickas ut varje år, som omfattar både innevarande och nästkommande kalenderår.

Kontrollarbetet kommer även fortsättningsvis bestå av tre delar, men frekvensen för den fasta respektive fördjupade kontrollen ändras. Framåt kommer dessa kontroller att ske vartannat år och under 2023 kommer en kontroll av de fasta kontrollpunkterna att genomföras. Genom att alternera den fasta respektive fördjupade kontrollen mellan åren får verksamheterna mer tid till att omhänderta resultaten från kontrollerna, vilket bedöms kunna bidra till ökad kvalitet på vidtagna åtgärder såväl som lagefterlevnad. Detta ligger också i linje med önskemål från flera verksamheter som har signalerat att tätt liggande kontroller gör det svårt att hinna med att arbeta med de lämnade rekommendationerna.

Den nya utformningen innebär även att tid frigörs för dataskyddsombudet, vilken kommer att läggas på att ytterligare stärka arbetet med informations- och utbildningsinsatser för stadens förvaltningar och bolag.

## 2 Kontrollarbetet 2023–2024

Dataskyddsbudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av dataskyddslagstiftningen görs i Göteborgs stad genom ett antal kontroller. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2023 och 2024. Enligt GDPR ska dataskyddsbudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsbudets bedömning avseende risker kopplat till personuppgiftsbehandlingar i verksamheten.

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

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

### 2.1 Kontrollarbetets delar

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

| Del                   | Beskrivning                                                                                                                                            | Frekvens                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Fasta kontrollpunkter | En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter. | Vartannat år fr.o.m. 2023 |
| Fördjupad kontroll    | En fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.                                                                  | Vartannat år fr.o.m. 2024 |
| Uppföljning           | Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.                                                                 | Årligen                   |

## 2.2 Tidplan för kontrollarbetet 2023–2024

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2023–2024 för stadens förvaltningar och bolag.

| 2023                | Aktivitet                                                 |
|---------------------|-----------------------------------------------------------|
| Januari - april     | Årsrapport 2022 presenteras för nämnd/styrelse.           |
| Januari - februari  | Kontrollplan för 2023–2024 lämnas till nämnd/bolag.       |
| September           | Utskick av enkät för fasta kontrollpunkter.               |
| November - december | Genomgång av innehåll i årsrapport med förvaltning/bolag. |
| December            | Fastställd årsrapport översänds till förvaltning/bolag.   |

| 2024                | Aktivitet                                                 |
|---------------------|-----------------------------------------------------------|
| Januari - april     | Årsrapport 2023 presenteras för nämnd/styrelse.           |
| Januari - februari  | Kontrollplan för 2024–2025 lämnas till nämnd/bolag.       |
| Augusti - november  | Fördjupad kontroll.                                       |
| November - december | Genomgång av innehåll i årsrapport med förvaltning/bolag. |
| December            | Fastställd årsrapport översänds till förvaltning/bolag.   |

## 3 Kontroller

### 3.1 Fasta kontrollpunkter

De fasta kontrollpunkterna utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

De fasta kontrollpunkterna kontrolleras genom en enkät som framöver kommer att vara återkommande vartannat år. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av

påståenden och/eller skattningsfrågor. Det är verksamheten som ansvarar för att enkäten fylls i. För att uppskattningarna ska bli så korrekta som möjligt kan det krävas att olika personer från olika delar i verksamheten deltar i arbetet med att fylla i enkäten. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som även åskådliggör de förändringar som vidtas över tid.

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

| <b>Fasta kontrollpunkter</b>                  |
|-----------------------------------------------|
| 1. Dataskyddsorganisation                     |
| 2. Personuppgiftsincidenter                   |
| 3. Biträdesavtal och andra överenskommelser   |
| 4. Register över personuppgiftsbehandlingar   |
| 5. Övergripande styrning av dataskyddsarbetet |
| 6. Utbildning                                 |
| 7. Informationsplikt                          |
| 8. E-post och dokumenthantering               |
| 9. Konsekvensbedömning/samråd                 |
| 10. IT-projekt och upphandling                |
| 11. IT-system och digitala verktyg            |
| 12. Hantering av registrerades rättigheter    |

## 3.2 Fördjupad kontroll

Den fördjupade kontrollen ska utgå från verksamhetens specifika risker och kommer framöver att genomföras vartannat år. Dataskyddsombudet kommer att fastställa fokusområde för den fördjupade kontrollen i dialog med verksamheten.

Information om fokusområde för 2024 kommer att tillhandahållas nämnd/bolag i kontrollplanen för 2024–2025.

## 3.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer och utvecklat sitt dataskyddsarbete inom varje kontrollpunkt.

# 4 Rapportering

## 4.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig presenteras årsrapporten för nämnd/styrelse vid sammanträde/möte.

## 4.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

# 5 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till verksamhetens huvudansvariga kontaktperson inom dataskyddsenheten.

Frågor kan också alltid ställas till [dso@intraservice.goteborg.se](mailto:dso@intraservice.goteborg.se).

# Bilaga 1 - Beskrivning av fasta kontrollpunkter

## Kontrollpunkt 1: Dataskyddsorganisation

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

## Kontrollpunkt 2: Personuppgiftsincidenter

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

## Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

## Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 register innefattas.

## Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

## Kontrollpunkt 6: Utbildning

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

### Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

### 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 dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

### Kontrollpunkt 9: Konsekvensbedömning/samråd

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

### Kontrollpunkt 10: IT-projekt och upphandling

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

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

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

### Kontrollpunkt 12: Hantering av registrerades rättigheter

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