Yttrande	M, D, L, KD
2024-03-06	Ärende nr 2

Yttrande angående – Årsrapport för dataskyddsarbetet 2023 för kommunstyrelsen.

Yttrandet

Stadsledningskontoret har det övergripande ansvaret för att driva på digitaliseringen i Göteborgs Stad. Utifrån ‘Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning” har kommunstyrelsen ett särskilt ansvar via den strategiska samordningsgruppen.

Dataskyddsombudets bedömning är att det identifierats ett behov att involvera dataskyddsombudet i större utsträckning om frågor som berör dataskydd. En bedömning är att kommunstyrelsen behöver tydliggöra för förvaltningen inom vilka verksamheter som det behövs vidtas åtgärder, detta för att säkerställa information till medarbetare om det lagkrav som finns om att involvera dataskyddsombudet i alla frågor som avser dataskydd.

Med anledning av ovanstående vill vi lyfta behovet av att arbetet sker skyndsamt för att säkerställa att dataskyddsombudet i Göteborgs Stad involveras och kan genomföra sitt arbete på ett effektivt sätt.

Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2024-02-05
Ärendenummer SLK-2024-00042

Handläggare
Anders Rosvall
Telefon: 031-368 00 52
E-post: anders.roswall@stadshuset.goteborg.se

Årsrapport för dataskyddsarbetet 2023 för kommunstyrelsen

Förslag till beslut

I kommunstyrelsen:

Årsrapport för dataskyddsarbetet 2023 för kommunstyrelsen antecknas.

Ärendet

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. Rapporten redogör för det kontrollarbete som genomförts och de iakttagelser som gjorts. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

För 2023 kontrollerade dataskyddsombudet verksamhetens dataskyddsarbete utifrån tolv fasta kontrollpunkter. Kontrollpunkterna har genomförts genom en enkät där förvaltningen har gjort en självskattning. Av rapporten framgår förvaltningens självskattning tillsammans med dataskyddsombudets bedömning. Enkäten spänner över de viktigaste delarna inom dataskyddsarbetet och metoden syftar till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

I de delar där dataskyddsombudets bedömning avviker från förvaltningens självskattning ges rekommendationer kring vad som behöver hanteras. Stadsledningskontoret kommer i det fortsatta utvecklingsarbetet att utgå från lämnade rekommendationer, med start i de för förvaltningen mest angelägna åtgärderna. Rapporten följer även upp den granskning som gjordes 2022 och kontoret arbetar vidare med att hantera de rekommendationer som återstår.

Bilaga

Årsrapport för dataskyddsarbetet för kommunstyrelsen 2023

Anders Roswall	Eva Hessman
Chef område kontorsledning	Stadsdirektör

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Kommunstyrelsen

2024-01-05

Innehåll

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 dataskydds-lagstiftningen 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 dataskydds-perspektivet 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.

2.2 Verksamhetsspecifika

2.2.1 Risker kopplat till att dataskyddsombudet ej involveras och/eller utestängs

Dataskyddsombudet har identifierat risker inom förvaltningen kopplat till bristande kunskaper inom dataskydd, som innebär att dataskyddsombudet ej involveras i och/eller utestängs från förvaltningens arbete. Bristerna i dataskyddskunskaper bedöms vara genomgående inom förvaltningens olika delar, och dataskyddsombudet har under åren varit med om flera situationer där olika funktioner från förvaltningen lämnat felaktiga råd och/eller information utifrån dataskyddslagstiftningen till bolag och förvaltningar i Staden. Utifrån det merarbete som detta innebär, både för dataskyddsombudet och verksamheterna som får olika svar från stadsledningskontoret och dataskyddsombudet, är det olyckligt att förvaltningen inte stämmer av och/eller hänvisar verksamheterna till dataskyddsombudet i stället.

Dataskyddsombudet har identifierat två områden där bristerna bedöms vara extra allvarliga och där konsekvenserna drabbar övriga Stadens verksamheter.

Inom ärendeberedningen och i utredningsarbetet

I beredningen av ärenden till kommunstyrelsen, till exempel vid utredning av politiska yrkanden eller uppdrag, behöver stadsledningskontoret involvera dataskyddsombudet i det fall frågan gäller en behandling av personuppgifter. När så inte görs innebär det dels att kommunstyrelsen inte uppfyller sina skyldigheter att involvera dataskyddsombudet, dels att underlaget riskerar att sakna viktiga perspektiv. Då kommunstyrelsens beslut som regel har en direkt påverkan på andra nämnder/bolag är det av särskild vikt att de beslut som fattas är väl underbyggda och ger verksamheter förutsättningar för att ta ansvar och följa gällande lagstiftning. I det fall ärenden påverkar Stadens eller en verksamhets behandling av personuppgifter bör beslutsunderlaget innehålla både en bedömning av huruvida förslaget är förenligt med gällande dataskyddslagstiftning och en ansvarsutredning utifrån gällande förutsättningar, tillsammans med dataskyddsombudets rekommendationer. I dagsläget är det dock inte fallet, utan i stället för att involvera dataskyddsombudet rådfrågas andra funktioner, något som dataskyddsombudet bedömer har medfört beslutsunderlag som helt saknar de registrerades perspektiv och/eller där dataskyddsombudet inte delar de gjorda analyserna.[1] Det är anmärkningsvärt, och bedöms utgöra en allvarlig brist, att stadsledningskontoret ej kunnat säkerställa att dataskyddsombudet involveras i arbetet med frågor kopplat till dataskyddslagstiftningen.

[1] Se exempel; ”Redovisning av uppdrag att utreda inrättandet av en trygghets- och larmcentral med befogenhet att samordna stadens larm, kameror, trygghetsvärdar och ordningsvakter” (dnr 1440/22), ”Redovisning av uppdrag om stadens rutiner vid nyanställning för att förhindra rekrytering av personer med konstaterad koppling till organiserad brottslighet eller våldsbejakande extremism” (dnr 1365/20), samt pågående arbete med uppdraget enligt yrkande från S, V och MP att i samverkan med stadsmiljönämnden förstärka samarbetet med Polismyndigheten för att effektivisera processen kring uppförandet av kameror på prioriterade platser där dessa behövs i brottsförebyggande och brottsuppklarande syfte (dnr SLK-2023-00866).

Inom arbetet med digitalisering och innovation

Med stadsledningskontorets övergripande ansvar att driva digitalisering i Göteborg Stad, kommer också ett ansvar för att säkerställa att arbetet bedrivs utifrån de regler och krav som styr verksamheterna som påverkas. Dataskyddsombudet bedömer att en genomgående brist i hur arbetet bedrivs, kopplat till Stadens styrning i digitaliserings- och innovationsfrågor, är att dataskyddsperspektivet saknas.

Utifrån riktlinjen (”Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning”) har kommunstyrelsen ett särskilt ansvar genom den strategiska samordningsgruppen som leds av stadsledningskontoret. En del i gruppens uppdrag är att värdera och prioritera gemensamma tjänster och digital infrastruktur, och de beslut som fattas/eller föreslås av den strategiska samordningsgruppen kommer således ha en direkt påverkan på förvaltningar och bolag inom Göteborgs Stad. Rimligen bör därför den beredningsgrupp som finns inom stadsledningskontoret ta ansvar för att alla perspektiv belyses, samt att dataskyddsombudet involveras då frågorna som gruppen hanterar ofrånkomligen kommer ha påverkan på hur personuppgifter hanteras. Utifrån gruppens sammansättning är dock så inte fallet, och dataskyddsombudet har inte på något sätt blivit involverad i beredningsarbetet. Konsekvensen av detta är att kommunstyrelsen inte uppfyller sin skyldighet att involvera dataskyddsombudet i alla frågor som gäller dataskydd.

Insatser krävs från högsta ledningsnivå

Utifrån den dialog som varit med förvaltningen kopplat till stadsledningskontorets uppdrag, och särskilt gällande dess rådgivande/stödjande funktioner, ser dataskyddsombudet ett behov av att understryka att förvaltningen inte kan göra skillnad på det interna och externa dataskyddsarbetet. Även de funktioner som arbetar utåt i Staden, men organisatoriskt tillhör stadsledningskontoret, omfattas av förvaltningens ansvar och behöver säkerställa att deras arbete och de råd/rekommendationer som lämnas är förenliga med dataskyddslagstiftningen. Dessa funktioner, till exempel inom ärendeberedning/juridik, informationssäkerhet och digitalisering/innovation, är också skyldiga att involvera dataskyddsombudet.

Sammantaget bedömer dataskyddsombudet att det inom förvaltningen finns ett stort behov av att tydliggöra att det är ett krav enligt lagstiftningen att involvera dataskyddsombudet i frågor som gäller dataskydd. Då problematiken med att dataskyddsombudet inte har, eller ges, insyn i förvaltningens arbete och att andra funktioner rådfrågas i stället fortfarande kvarstår, bedömer dataskyddsombudet att det krävs insatser från högsta ledningsnivå för att situationen ska förändras. Kommunstyrelsen bedöms behöva tydliggöra för förvaltningen att det inom verksamheten behöver vidtas åtgärder för att säkerställa att medarbetare informeras om att det är ett lagkrav att involvera dataskyddsombudet i alla frågor som gäller dataskydd. Detta rekommenderas hanteras genom riktade utbildningsinsatser inom förvaltningen med syftet att stärka den allmänna kunskapsnivån inom verksamheten. Vidare rekommenderas förvaltningen även ta fram interna

dokumenterade arbetssätt som tydliggör när och hur dataskyddsombudet ska involveras i förvaltningens arbete.

2.2.2 Risker kopplat till hanteringen av uppdraget att utreda hur ett ändamålsenligt och stadengemensamt dataskydd kan organiseras

Dataskyddsombudet ställde med anledning av att ärendet ”Redovisning av uppdrag att utreda hur ett ändamålsenligt och stadengemensamt dataskydd kan organiseras” (dnr SLK-2023-00556) skulle behandlas på kommunstyrelsens sammanträde 2023-11-08 en särskild skrivelse till kommunstyrelsen.[2] Skrivelsen gällde risken att kommunstyrelsen skulle bryta mot artikel 38:2 och 38:3 i dataskyddsförordningen (GDPR) om beslut fattades i enlighet med förslaget. Detta utifrån de ställningstaganden som gjorts i utredningen om dataskyddsombudets ställning och uppgifter, samt då den föreslagna hanteringen i praktiken skulle innebära att dataskyddsombudet avsätts eller utsätts för repressalier för att ha utfört sina lagstadgade uppgifter. Beslut i ärendet fattades av kommunstyrelsen 2023-11-22 (§ 825), samt av kommunfullmäktige 2023-12-07 (§ 85).

Dataskyddsombudet bedömer att den identifierade risken kvarstår, och att det fattade beslutet riskerar att bryta mot artikel 38:2 och 38:3 i dataskyddsförordningen (GDPR).

[2] Dataskyddsombudets skrivelse med anledning av ”Redovisning av uppdrag att utreda hur ett ändamålsenligt och stadengemensamt dataskydd kan organiseras” (dnr SLK-2023-00556), 2023-11-06.

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.[3]

Risknivå	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.	

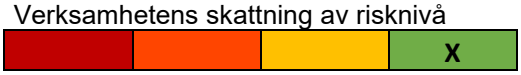
3.2 Resultat från kontrollen 2023

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.

[3] 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 inte verksamhetens bedömning utan anser tvärtom att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Utifrån skattningen kan det utläsas att förvaltningen i år bedömer att den interna dataskyddsorganisationen har tillräckliga resurser för att kunna bedriva ett systematiskt dataskyddsarbete, samt att det finns definierade rapporteringsvägar i dataskyddsfrågor. När det gäller huruvida dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten anger förvaltningen, likt 2022, att detta inte stämmer. Förvaltningen anger även ett sämre värde på frågan ifall dataskyddsombudet regelbundet involveras i alla frågor som gäller dataskydd gentemot tidigare år.

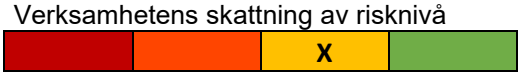
I årsrapporten för 2022 lyfte dataskyddsombudet att förvaltningens interna dataskyddsorganisation upplevdes splittrad och att det saknades samordning eller planering på en övergripande nivå. Det lyftes även att det fanns en osäkerhet kring ifall utpekad dataskyddskontakt fick tillräcklig information från övriga verksamheten, vilket i sin tur bedömdes påverka dataskyddsombudet möjligheter till insyn negativt. Dataskyddsombudet bedömde då att förvaltningen inte involverade dataskyddsombudet i alla frågor, och påminde i årsrapporten därför förvaltningen om lagkravet på att i alla frågor som rör dataskydd involvera dataskyddsombudet. Vidare lyftes i årsrapporten för 2022 att dataskyddsombudet inte bedömde att den interna dataskyddsorganisationen hade tillräckliga resurser för att kunna arbeta med dataskyddsfrågorna i den takt som de dyker upp och i enlighet med lagstiftningen. Utifrån detta rekommenderades förvaltningen att se över dåvarande organisation och hur denna skulle kunna utvidgas. Förvaltningen rekommenderades även att vidta åtgärder för att säkerställa dataskyddsombudets involvering framåt.

Under 2023 bedömer dataskyddsombudet att förvaltningen vidtagit flera åtgärder kopplat till den interna dataskyddsorganisationens resurser och omfattning, vilka ligger i linje med den rekommendation som lämnades 2022. Att förvaltningen arbetat med frågan och utökat organisationen med kontaktpersoner ute på avdelningarna bedöms vara mycket positivt. Dataskyddsombudet bedömer också att förvaltningens dataskyddskontakter involverat dataskyddsombudet i verksamhetens dataskyddsarbete under året. Vid genomgången av årsrapporten uppger förvaltningen att dataskyddsombudet under året blivit involverad i alla de dataskyddsfrågor som dataskyddskontakterna har fått kännedom om, vilket överensstämmer med dataskyddsombudets uppfattning.

Utifrån de åtgärder som vidtagits under året kopplat till den interna dataskyddsorganisationen vill dataskyddsombudet därför särskilt poängtera att de höga risker som dataskyddsombudet identifierat inom kontrollpunkten inte gäller den interna dataskyddsorganisationen. De identifierade riskerna handlar i stället om verksamhetens brister kopplat till att göra dataskydd till en naturlig och integrerad del i verksamheten, samt en upplevd ovilja att involvera dataskyddsombudet. Då dessa delar tillsammans bedöms medföra höga risker för Stadens verksamheter som helhet har dataskyddsombudet valt att lyfta detta som en verksamhetsspecifik iakttagelse under avsnitt 2.2.1. Under avsnitt 2.2.1 lämnas även de rekommendationer som bedöms behöva vidtas av högsta ledningsnivå för att riskerna ska kunna hanteras.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

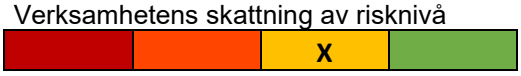
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar verksamhetens bedömning om att det inom kontrollpunkten föreligger risker, men kan utifrån förvaltningens svar ej göra en bedömning om huruvida dessa kräver omgående åtgärder eller ej.

De risker som kan identifieras utifrån förvaltningens skattning är att det inte bedöms finnas dokumenterade arbetssätt som säkerställer att alla inträffade personuppgiftsincidenter dokumenteras och att dokumentationen uppfyller kraven enligt GDPR, samt att det inom verksamheten inte regelbundet sker ett arbete med att informera medarbetare om vad personuppgiftsincidenter är och vad man som medarbetare ska göra när en incident upptäcks/inträffar. På dessa frågor har förvaltningen i år angett ett lägre värde än för 2022. Störst skillnad på svaret är för frågan om verksamheten har dokumenterade arbetssätt som säkerställer att alla inträffade personuppgiftsincidenter dokumenteras och att dokumentationen uppfyller kraven enligt GDPR. Vid genomgången av årsrapporten framkom att det lägre värdet beror på att förvaltningen i år gjort en intern bedömning att det högsta svarsalternativ som kan användas utifrån hur frågan är formulerad är 3 (”Ja, stämmer bra”) och därför valt att svara 2 (”Nej, stämmer inte bra”). Dataskyddsombudet delar inte förvaltningens bedömning gällande att frågans utformning begränsar vilka svarsalternativ som kan användas, och vill framhålla att frågan är formulerad på samma sätt som tidigare år.

I årsrapporten 2022 identifierade dataskyddsombudet en risk för underrapportering kopplat till ett lågt antal incidenter, och förvaltningen rekommenderades därför säkerställa att alla medarbetare får tillräcklig utbildning och information om incidenter och incidenthantering. Utifrån skattningen i år bedömer dataskyddsombudet att tidigare lämnad rekommendation om att utbilda och informera medarbetare om incidenter och incidenthantering kvarstår.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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.

I skattningen anger förvaltningen, likt 2022, låga värden på frågor kopplat till arbetet med kontinuerliga efterlevnadskontroller och för rutiner och kompetens kopplat till att bedöma biträden/underbiträden, samt för att säkerställa att andra överenskommelser tecknas när så krävs. De rekommendationer som lämnades 2022 gällande att ta fram rutiner och tillse att det finns rätt kompetens inom förvaltningen för genomförandet av arbetet kvarstår därför.

De höga risker som dataskyddsombudet identifierat, utifrån gjorda iakttagelser inom ramen för kontrollpunkten, är relaterade till förvaltningens arbete med att utreda ansvarsförhållanden för personuppgiftsbehandlingar gemensamma för förvaltningar och bolag inom Staden. I årsrapporten 2022 lyfte dataskyddsombudet att arbetet inom denna kontrollpunkt är kopplat till behovet av att utreda kommunstyrelsens personuppgiftsansvar och att det framåt sannolikt kommer behöva upprättas överenskommelser gällande gemensam/annan delad hantering av personuppgifter med stadens förvaltningar och bolag. Behovet av att utreda ansvarsförhållandena lyftes även som en särskild iakttagelse i årsrapporten.

Dataskyddsombudet har under 2023 inte blivit involverad i något arbete med att utreda ansvarsförhållandena för stadengemensamma personuppgiftsbehandlingar från stadsledningskontorets sida. I stället har frågan lyfts och drivits på av förvaltningen för Intraservice som i egenskap av tjänsteleverantör bedömt att ansvarsförhållandena för personuppgiftsbehandlingar behöver klarläggas för att tjänster, och de IT-stöd som utgör behandlingarnas informationsbärare, ska kunna levereras. Ett exempel på det arbete som genomförts på initiativ av Intraservice, med stöd av dataskyddsombudet, är utredningen av personuppgiftsansvaret för den behandling som genomförandet av Göteborgs Stads medarbetarundersökning innebär. Kartläggningen av behandlingen visade på att det är kommunstyrelsen som, genom att ha fattat beslut med påverkan på hela Staden, bestämt förutsättningarna (i form av ändamål och medel) för behandlingen och därför är personuppgiftsansvarig. En avgörande del för att personuppgiftsansvaret kunde fastställas var att det på stadsledningskontoret fanns förståelse för att ansvaret regleras utifrån de faktiska förutsättningarna, och att kommunstyrelsen kan ha ett personuppgiftsansvar för behandlingar som man tidigare antagit ligger hos respektive verksamhet.

Dataskyddsombudet är mycket positiv till att kommunstyrelsen, genom stadsledningskontoret, nu har tagit ansvar för denna behandling. Utöver att det stärker Stadens förutsättningar att uppfylla sina skyldigheter enligt dataskyddslagstiftningen, har det även medfört en minskad administrativ börda ute i verksamheterna då endast en konsekvensbedömning behövt genomföras hos stadsledningskontoret. Vidare bedömer dataskyddsombudet att denna behandling, och dess förutsättningar, kan fungera som ett referensfall för bedömningen av personuppgiftsansvaret för andra stadengemensamma behandlingar där kommunstyrelsen, genom beslut, fastställt ändamål och medel.

Dataskyddsombudet bedömer dock, utifrån den dialog som varit och de iakttagelser som gjorts, att det inom stadsledningskontoret finns en ovilja att ta ansvar för arbetet med att utreda ansvarsförhållandena kopplat till gemensamma personuppgiftsbehandlingar i Staden. Vad detta grundar sig på har dataskyddsombudet inte någon inblick i, men kan däremot se att samma inställning gäller för arbetet med att hantera de grundläggande problem som de senaste åren regelbundet har varit föremål för diskussioner kopplat till styrningen av hur och vilka behandlingar som ska genomföras samt vilka informationsbärare som ska användas. Dataskyddsombudet lyfte i årsrapporten för 2022 att stadsledningskontoret borde ta ansvar för att utreda frågorna utifrån förvaltningens roll, samt då förvaltningen ansvarar för stadens styrmodell och frågeställningen egentligen redan borde ha utretts. Dataskyddsombudets bedömning i dessa delar kvarstår oförändrade.

Dataskyddsombudet rekommenderar att kommunstyrelsen, genom stadsledningskontoret, tar ansvar för att driva frågan om att utreda ansvarsförhållanden för stadengemensamma personuppgiftsbehandlingar. Det finns ett stort antal kvarstående behandlingar där kommunstyrelsen sannolikt har ett större personuppgiftsansvar än vad som tidigare bedömts. Dataskyddsombudet rekommenderar att arbetet prioriteras under 2024 då nuvarande situation bedöms innebära att kommunstyrelsen ej kan uppfylla sina skyldigheter enligt dataskyddslagstiftningen.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå

		X	

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, och bedömer vidare att dessa främst är kopplade till de risker som lyfts under kontrollpunkt 3 gällande outrett personuppgiftsansvar.

Utifrån förvaltningens skattning noterar dataskyddsombudet att förvaltningen även i år anger att ca 75 % av förvaltningens behandlingar finns med i registret och att ca 75 % av dessa bedöms innehålla den information som ska finnas med enligt artikel 30 i GDPR. Dataskyddsombudet har under året haft en dialog med förvaltningen om det pågående arbetet med att gå igenom och uppdatera behandlingsregistret. Förvaltningen har i dialogen angett att man tar ett omtag och i arbetet framåt kommer utgå från den mall som dataskyddsenheten tagit fram, tillsammans med några tillägg som man bedömer kommer underlätta det interna dataskyddsarbetet. Vidare har det i dialogen uttryckts att förvaltningen bedömer att arbetet med att kartlägga stadsledningskontorets interna personuppgiftsbehandlingar kommer ”spilla över” till arbetet med att identifiera de behandlingar som är gemensamma för Staden och där kommunstyrelsen sannolikt har ett ansvar. Dataskyddsombudet är mycket positiv till det kartläggningsarbete som stadsledningskontoret påbörjat och har efterfrågat att få delta vid möten med de avdelningar som bedöms hantera stora mängder personuppgifter och/eller genomföra behandlingar med höga risker, till exempel kopplat till trygghets- och säkerhetsarbete eller statistik på stadenövergripande nivå. Förvaltningen rekommenderas för 2024 prioritera det påbörjade arbetet med att inom verksamheten identifiera de interna personuppgiftsbehandlingar som ligger inom kommunstyrelsens ansvar.

I sammanhanget vill dataskyddsombudet lyfta att även om det interna kartläggningsarbetet kan bidra till att identifiera behandlingar som är gemensamma i Staden, kommer det finnas behandlingar som inte täcks in i detta. Då nuvarande situation bedöms innebära att kommunstyrelsen inte kan uppfylla sina skyldigheter enligt dataskyddslagstiftningen rekommenderas förvaltningen därför parallellt att driva frågan om att utreda ansvarsförhållanden för stadengemensamma personuppgiftsbehandlingar (se kontrollpunkt 3).

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. För denna punkt gör dataskyddsombudet olika bedömningar avseende risknivån kopplat till den interna respektive externa styrningen. Medan riskerna för den externa styrningen bedöms vara omfattande, visar förvaltningens skattning på att det internt finns styrning i form av styrdokument och dokumenterade arbetssätt.

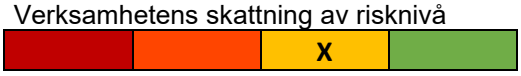
Kopplat till den interna styrningen visar förvaltningens egen skattning att det kvarstår ett behov av att se över hur det inom verksamheten kan genomföras regelbundna interna kontroller för att säkerställa följsamhet gentemot GDPR.

Dataskyddsombudet kan vidare, utifrån förvaltningens skattning och efter genomgång av styrande dokument, se att det finns flera styrdokument framtagna som på olika sätt, direkt eller indirekt, reglerar hanteringen av personuppgifter. För att tillförsäkra sig om att de utformade arbetssätten är ändamålsenliga rekommenderas förvaltningen att framledes genomföra interna kontroller för att följa upp och kontrollera så att de styrande dokument som finns får genomslag i praktiken.

För den externa styrningen är dataskyddsombudets bedömning att det på staden övergripande nivå föreligger risker utifrån bristande styrning från stadsledningskontoret i dataskyddsfrågor. Det saknas idag från stadsledningskontorets håll helt någon form av samordning eller styrning inom dataskyddsområdet. Utifrån kommunstyrelsens uppdrag att samordna och styra Stadens verksamheter borde rimligen ett större ansvar kunna tas i det gemensamma dataskyddsarbetet. Dataskyddsombudets uppfattning är att den nya enheten som ska inrättas på stadsledningskontoret ska arbeta med bland annat detta, vilket är positivt. Samtidigt gör dataskyddsombudet bedömningen att många av de frågor och den osäkerhet som föreligger inom dataskyddsområdet i Staden är direkt kopplade till att ansvarsförhållanden inte utretts. En förutsättning för att bristerna med den externa styrningen ska kunna åtgärdas är därför att kommunstyrelsen, genom stadsledningskontoret, tar ansvar för att driva frågan om att utreda ansvarsförhållanden för stadengemensamma personuppgiftsbehandlingar.

3.2.6 Kontrollpunkt 6: Utbildning

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 inte verksamhetens bedömning, utan gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är betydande och kräver omgående åtgärder.

Av förvaltningens svar kan utläsas att den allmänna kunskapsnivån inom förvaltningen bedöms ha stärkts från föregående år, och att det nu regelbundet ges möjlighet för medarbetare att delta i utbildningar inom dataskydd. Det högre resultatet i dessa delar indikerar att förvaltningen under året arbetat med frågan, vilket är positivt. Samtidigt visar skattningen att de risker som föregående år identifierades kopplat till interna utbildningsinsatser och upprätthållande av kompetens fortfarande kvarstår. De rekommendationer som lämnades i årsrapporten 2022 gällande att kartlägga utbildningsbehov kopplat till olika befattningar, att ta fram en utbildningsplan och rutiner för genomförande samt uppföljning, kvarstår därför.

I årsrapporten 2022 bedömde dataskyddsombudet, utifrån gjorda iakttagelser, att det fanns brister i den allmänna kunskapsnivån inom förvaltningen. Vidare rekommenderades förvaltningen prioritera arbetet med att stärka den allmänna kunskapsnivån inom förvaltningen utifrån det arbete kopplat till kommunikation, innovation och digitalisering som drivs för hela Staden. Även om förvaltningen i år bedömer att den allmänna kunskapsnivån förbättrats, är dataskyddsombudets bedömning att det kvarstår ett stort behov av riktade utbildningsinsatser inom förvaltningen, bland annat för funktioner som arbetar med att utreda/bereda ärenden till politiken, inom informationssäkerhet samt med innovation och digitalisering. Förvaltningen rekommenderas därför fortsätta arbeta med att stärka den allmänna kunskapsnivån inom verksamheten.

Att medarbetare, utifrån sin roll och sina arbetsuppgifter, har tillräckliga kunskaper om GDPR är en grundläggande förutsättning för ett fungerande dataskyddsarbete. Dataskyddsombudet vill även lyfta att olika medarbetare kan ha olika behov av utbildnings- och informationsinsatser utifrån sin roll och sina arbetsuppgifter. Genom att kartlägga vilken nivå av dataskyddskunskaper som olika befattningar behöver ha, och säkerställa att medarbetare löpande utbildas därefter, ges medarbetarna rätt förutsättningar att integrera dataskyddsperspektiv i sitt dagliga arbete och att hantera personuppgifter korrekt utifrån sin roll inom förvaltningen.

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. Resultaten på denna punkt är lägre än tidigare år, och bland annat anges i år ett betydligt lägre värde på frågan om verksamhetens integritetsinformation uppfyller kraven på information enligt GDPR.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, och ser att resultatet på denna punkt är beroende av det arbete som behöver göras med att kartlägga verksamhetens personuppgiftsbehandlingar och bedöma ansvarsförhållandena för dessa. En förutsättning för att förvaltningen ska kunna uppfylla informationsplikten är att verksamhetens personuppgifts-behandlingar är dokumenterade och att kommunstyrelsens personuppgiftsansvar utretts. Dataskyddsombudets uppfattning är att den lägre skattningen visar på en ökad medvetenhet i frågan och om de krav som ställs på information i GDPR.

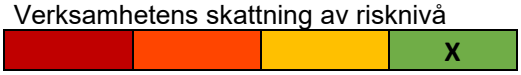
Framåt, i takt med att kartläggningen färdigställs och registret uppdateras, rekommenderas förvaltningen att se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som förvaltningen tillämpar för att säkerställa att informationsplikten gentemot de registrerade uppfylls. Inom ramen för detta arbete behöver förvaltningen omhänderta de rekommendationer som

tidigare lämnats inom ramen för den fördjupade kontroll som genomfördes 2022 gällande förvaltningens integritetspolicy (se avsnitt 3.3.1).

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande informationsplikten enligt GDPR. Förvaltningen kan med fördel utgå från denna i arbetet.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå



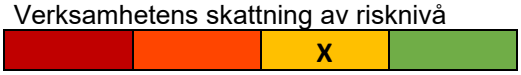
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året ej involverats i någon fråga kopplat till kontrollpunkten, varför ingen bedömning kan göras.

Förvaltningens egen skattning visar en förbättring inom flera områden, samt att rekommendationen som lämnades föregående år gällande att ta fram dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut omhändertagits. Då det även inom verksamheter med låga risker krävs kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas, rekommenderas förvaltningen att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

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 betydande risker som kräver omgående åtgärder.

Under året har dataskyddsombudet involverats i ett antal konsekvensbedömningar och tröskelanalyser. Kvaliteten på underlagen har varit varierande, där några inte bedömts uppfylla kriterierna för en godtagbar konsekvensbedömning. I flera fall har även konsekvensbedömningarna gjorts för sent och efter det att beslut om att inleda behandlingarna tagits, till exempel för införandet av Digitala Navet och Ciceron. Dataskyddsombudet ställer sig utifrån hanteringen frågande till förvaltningens ingång i arbetet med konsekvensbedömningarna och det förväntade

resultatet av dessa. Med anledning av de iakttagelser som gjorts under året inom ramen för förvaltningens arbete med konsekvensbedömningar ser dataskyddsombudet anledning att ifrågasätta förvaltningens bedömning att det finns dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas. Om sådana arbetssätt fanns på plats borde förutsättningarna för det arbete som genomförts under året varit annorlunda. Ytterligare risker som dataskyddsombudet identifierat, vilket även visas av förvaltningens egen skattning, är att det enbart finns framtagna och fastställda konsekvensbedömningar för en liten del av verksamhetens personuppgiftsbehandlingar, samt att det till stor del saknas en planering för genomförandet framåt.

Vid genomgången av årsrapporten anger förvaltningen att arbetet med konsekvensbedömningar och tröskelanalyser som avser interna behandlingar, vilka stadsledningskontoret själva styr över, har hanterats i tid. Däremot har det arbete som skötts utanför förvaltningen, till exempel gällande Digitala Navet och Ciceron, inte kunnat hanteras i tid. Förvaltningen bedömer sig inte ha getts förutsättningar för att hantera dessa frågor i tid.

Dataskyddsombudet har under året identifierat en särskild risk kopplat till förvaltningens hantering av konsekvensbedömningen för behandlingarna inom ramen för det nya intranätet ”Digitala Navet”. Förvaltningen framförde ett tjänsteutlåtande[4] till kommunstyrelsens sammanträde 2023-08-23 där det framkom att en konsekvensbedömning genomförts, men resultatet av konsekvens-bedömningen presenterades inte. Då syftet med en konsekvensbedömning är att kartlägga risker med en behandling, är det också av största vikt att den som är ytterst ansvarig för behandlingen får all tillgänglig information innan beslut fattas om att påbörja behandlingen. I fallet med Digitala Navet framkom det i konsekvensbedömningen, men inte i tjänsteutlåtandet, att förvaltningen genom att påbörja behandlingen, riskerade att bryta mot GDPR genom en otillåten tredjelandsöverföring. I underlaget till kommunstyrelsen angav förvaltningen att man antagit ett riskbaserat arbetssätt, men nämnde inte att det riskbaserade arbetssättet innebar att man valde att gå vidare och inleda en behandling som (vid tidpunkten) saknade rättsliga förutsättningar. Att förvaltningens bedömning i frågan avvek från såväl praxis som dataskyddsombudets rekommendationer framgick inte heller i tjänsteutlåtandet. Utifrån detta är dataskyddsombudets bedömning att stadsledningskontoret ej tillhandahöll kommunstyrelsen ett fullständigt underlag i ärendet. Då ärendet vid sammanträdet enbart hanterades som ett informationsärende är det för dataskyddsombudet även otydligt hur, samt med vilket mandat, beslut om att inleda behandlingen fattades.

Som lyftes i årsrapporten för 2022 bör arbetet med konsekvensbedömningar vara en del av den övergripande strategin för dataskyddsarbetet i verksamheten, och den interna dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet

[4] ”Information om att Digitala navet ersätter nuvarande intranät i kommunstyrelsens egen förvaltning/stadsledningskontoret” (dnr 0608/23)

av en konsekvensbedömning. Utifrån de brister som identifierats i arbetet under året kvarstår den rekommendation som lämnades i årsrapporten 2022 gällande att kartlägga behandlingar, identifiera vilka behandlingar (med höga risker) som kräver en konsekvensbedömning samt ta fram en planering för genomförandet. Förvaltningen rekommenderas även att framåt involvera dataskyddsombudet i ett tidigare skede av konsekvensbedömningsarbetet.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

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 har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

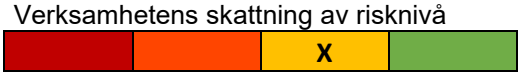
I årsrapporten för 2022 rekommenderades förvaltningen dels säkerställa rutiner för att involvera dataskyddsombudet från start vid införande av nya IT-projekt och införande av nya tjänster, dels utreda om insatser behöver genomföras för att säkerställa att dataskydd beaktas i tillräcklig utsträckning. Utifrån förvaltningens skattning i år kan utläsas att det bedöms ha skett en förbättring i båda avseendena.

Utifrån de risker som identifierats kopplat till den allmänna kunskapsnivån (kontrollpunkt 6) bedömer dataskyddsombudet dock att det föreligger risker inom kontrollpunkten, men att hanteringen av dessa är beroende av insatser inom ramen för andra kontrollpunkter. Förbättringar i den allmänna kunskapsnivån, såväl som en ökad medvetenhet kopplat till förvaltningens ansvar, skulle sannolikt kunna hantera de risker som identifierats inom ramen för förvaltningens arbete med digitalisering och innovation.

Inom ramen för kontrollpunkten rekommenderas förvaltningen framåt arbeta med att säkerställa att dokumenterade arbetssätt för att involvera dataskyddsombudet vid uppstart av nya IT-projekt och/eller införandet av nya tjänster där person-uppgifter kommer att hanteras blir kända inom samtliga delar av verksamheten.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

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 har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Den risk som kan utläsas utifrån förvaltningens egen skattning är kopplad till uppföljning av efterlevnad gentemot styrande dokument. Förvaltningen rekommenderas därför, likt 2022, ta fram arbetssätt för att kunna följa upp att användningen av system och digitala verktyg följer antagna styrande dokument.

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 fått några direkta indikationer som medför en annan bedömning än den som förvaltningen gör, men har inte heller kontrollerat hanteringen särskilt.

Även om dokumenterade arbetssätt för hanteringen finns på plats visar förvaltningens egen skattning på att det fortfarande finns ett stort behov av att öka medvetenheten gällande registrerades rättigheter inom verksamheten. Utifrån detta rekommenderas förvaltningen framåt ta med frågan i de utbildnings- och informationsinsatser som förvaltningen rekommenderas genomföra för att stärka den allmänna kunskapsnivån inom dataskydd i verksamheten.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2021): Hantering av personuppgiftsincidenter under 2020

Verksamheten gavs följande rekommendationer:

- Justera formuleringen i rutinen från ”Innebär incidenten allvarlig skada?” till ”Är det sannolikt att incidenten utgör en risk för en enskild persons rättigheter och friheter?”.
- Justera rutinen så att bedömningen om det är en teknisk incident kommer tidigare i processen.

- Säkerställ så att även de fall där man gjort bedömningen att det inte rör sig om en personuppgiftsincident dokumenteras.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit ett par åtgärder utifrån rekommendationerna, samt att det pågår ett arbete med att skapa en ny process kopplat till dokumentation där incidentdokumentationen utgör en del.

Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

Kontroll (2022): Integritetspolicy

Verksamheten gavs följande rekommendationer:

- Kartlägga vilka behandlingar som den externa policyn är tänkt att omfatta samt komplettera informationen så att det för samtliga behandlingar anges bl.a. ändamål, rättslig grund och lagringstid.
- Säkerställa att information om övriga behandlingar som förvaltningen utför (som inte omfattas av den externa policyn) ges till registrerade på andra sätt, samt säkerställa att denna är komplett och korrekt.
- Kartlägga kanaler och kontaktvägar samt säkerställa att de registrerade får information om hur deras personuppgifter behandlas i rätt tid vid deras kontakter med förvaltningen.
- Ta fram förvaltningsspecifik information om hur anställdas personuppgifter behandlas.
- Komplettera den externa policyn och den interna informationen med konkret information om hur länge personuppgifterna lagras.
- Se över språkbruket i den externa policyn och den interna informationen och säkerställa att det är konkret, exakt och enkelt.
- Ta fram rutin som säkerställer att informationen som ska ges uppdateras vid behov.

Kommentarer och rekommendationer:

Uppföljningen visar att förvaltningen påbörjat arbetet med att omhänderta rekommendationerna, och att detta är nära sammankopplat med förvaltningens pågående arbete med att uppdatera behandlingsregistret. Förvaltningen anger att det pågår ett arbete med att identifiera samtliga behandlingar och att nästa steg är att uppdatera informationstexter till registrerade. Parallellt med detta större arbete uppger förvaltningen också att det löpande tagits fram informationstexter för ett antal specifika behandlingar.

För att ta ett helhetsgrepp i förvaltningens arbete med informationsplikten kommer fortsatt uppföljning av arbetet ske inom ramen för de fasta kontrollpunkterna. Under kontrollpunkt 7 lämnas rekommendationer för arbetet framåt, och där framgår att förvaltningen som en del i arbetet rekommenderas omhänderta de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn.

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 att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

Inom ramen för denna kontrollpunkt inkluderas rekommenderade åtgärder för att hantera de risker som identifierats under avsnitt 2.2.1 kopplat till att dataskyddsombudet ej involveras och/eller utestängs.

1) Vidta åtgärder för att säkerställa att medarbetare informeras om att det är ett lagkrav att involvera dataskyddsombudet i alla frågor som gäller dataskydd.

2) Genomför riktade utbildningsinsatser inom förvaltningen med syftet att stärka den allmänna kunskapsnivån (i dataskydd) inom verksamheten.

3) Ta fram interna dokumenterade arbetssätt som tydliggör när och hur dataskyddsombudet ska involveras i förvaltningens arbete.

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Ta ansvar för att driva frågan om att utreda ansvarsförhållanden för stadengemensamma personuppgiftsbehandlingar.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

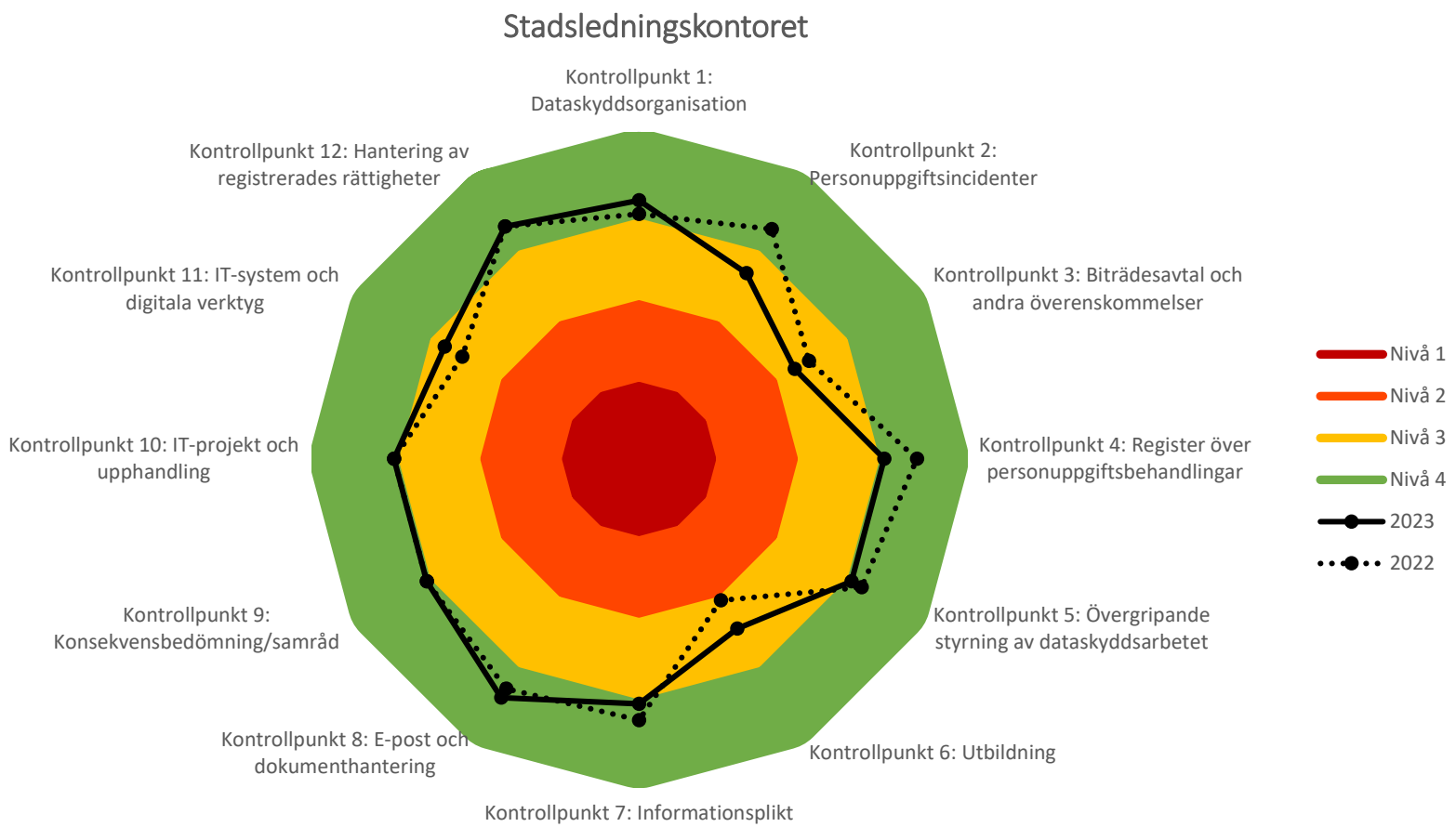
Fortsätt det påbörjade arbetet med att inom verksamheten identifiera de interna personuppgiftsbehandlingar som ligger inom kommunstyrelsens ansvar.

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.



Göteborgs Stad

Stadsledningskontoret

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

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 dataskydds-ombudets 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

Dataskyddsombudets 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 dataskyddsombudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsombudets 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 dataskyddsombud 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.

Fasta kontrollpunkter
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.

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 personuppgiftincidenter. 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.