Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Nämnden för Intraservice

2023-12-21

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 Tidigare identifierade risker kopplat till avsaknaden av en intern dataskyddsorganisation kvarstår

Förvaltningens utmaningar kopplat till avsaknaden av tillräckliga resurser för dataskyddsarbetet har under året kvarstått. Då andra verksamheter inom Staden fortsätter att arbeta med, och utveckla, deras dataskyddsarbete medför det att skillnaderna mellan Intraservice och övriga blir allt tydligare. Förvaltningen ligger redan idag långt efter i dataskyddsarbetet, och om resurser inte tillsätts för det interna dataskyddsarbetet kommer skillnaden mellan verksamhetens leverans och kundernas förväntningar fortsätta öka.

Dataskyddsombudet bedömer att förvaltningen behöver avsätta resurser dels för arbetet med att hantera de krav och skyldigheter som kommer med nämndens utökade personuppgiftsansvar, dels för arbetet med att säkerställa att de tjänster som levereras uppfyller gällande lagkrav. Under året har förvaltningen fortsatt att utveckla och leverera tjänster utan att dessa först genomlysts utifrån ett dataskyddsperspektiv såväl som övrig lagstiftning. När kunder i Staden vid införandet ställer frågor och lämnar krav är dataskyddsombudets uppfattning att förvaltningen som regel inte kan redogöra för vilka bedömningar som gjorts eller tillhandahålla det underlag som efterfrågas. Då denna problematik inte är ny, utan tvärt emot är något som har lyfts regelbundet som en brist de senaste åren, ser dataskyddsombudet allvarligt på att inga åtgärder har vidtagits för att hantera bristerna. Samtidigt är dataskyddsombudets bedömning att en förutsättning för att dessa risker ska kunna hanteras är att det inom förvaltningen tillsätts en intern dataskyddsorganisation, med tillräckliga resurser och kompetens, som kan samordna och arbeta med frågorna.

Dataskyddsombudet vill i sammanhanget även lyfta att förvaltningen i dagsläget har en omfattande skuld när det gäller att följa dataskyddslagstiftningen, vilken de senaste åren bara har ökat. För att förvaltningen framåt ska ha förutsättningar att hantera denna behöver det omgående tillsättas resurser, så att förvaltningen får på plats de mest grundläggande delarna i form av en intern organisation och ett register över de personuppgiftsbehandlingar som nämnden är ansvarig för. Ytterligare en del som dataskyddsombudet bedömer nödvändig är att man inom verksamheten börjar arbeta aktivt med att bryta de vanor och förhållningssätt som bidrar till en leverans av tjänster där rättssäkerheten inte kan garanteras.

Bristerna i förvaltningens dataskyddsarbete har regelbundet lyfts från dataskydds-ombudet till både lednings- och nämndnivå de senaste åren. De åtgärder som vidtogs förra året i form av en handlingsplan har nu lett till att förvaltningen startat upp ett omfattande projekt kopplat till informationssäkerhet där dataskydd är en del. Projektet har många aktiviteter som ska möta upp till kraven inom både informationssäkerhet och dataskydd. Dataskyddsombudet vill därför understryka att åtgärder kopplat till den interna dataskyddsorganisationen behöver prioriteras för att förvaltningen på sikt ska ha möjlighet att komma i kapp i dataskyddsarbetet.

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.[1]

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.	

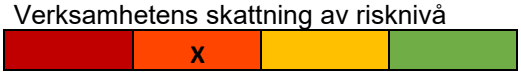
3.2 Resultat från kontrollen 2023

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.

[1] 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 det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad från verksamheten bedömningen att vissa av de identifierade riskerna är så höga att de kräver omgående insatser ifrån ledningsnivå.

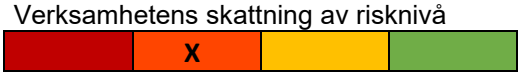
Dataskyddsombudet har i tidigare årsrapporter lyft att förvaltningen saknar en intern dataskyddsorganisation som praktiskt jobbar med dataskyddsfrågor. Eftersom förvaltningen inte har vidtagit några åtgärder för att förändra situationen kvarstår bristen och är i allra högsta grad en bakomliggande orsak till förvaltningens genomgående låga resultat på samtliga kontrollpunkter. Dataskydd kan inte vara en naturlig och integrerad del i arbetet i alla delar av verksamheten när det saknas någon/några som ansvarar för frågorna, samt arbetssätt/rutiner som säkerställer att alla medarbetare arbetar på samma sätt.

Dataskyddsombudet bedömer att förvaltningen omgående behöver ta fram en organisation för dataskydd där utpekade roller har tillräckligt med tid och resurser för att faktiskt arbeta med frågorna. På grund av förvaltningens uppdrag såväl som stora skuld, i form av ogjort arbete, när det kommer till GDPR kommer det inte fungera att lägga arbetsuppgifterna på någon som redan har ett annat uppdrag i förvaltningen, utan förvaltningen bedöms behöva tillsätta ytterligare resurser.

En av de större bristerna som dataskyddsombudet har identifierat är att det också saknas särskilda befattningar/roller med utpekat ansvar och mandat att fatta beslut i olika typer av dataskyddsfrågor. Det innebär att, i de fall verksamheten faktiskt gör det som åligger dem enligt GDPR, till exempel genomför en konsekvensbedömning, så finns det ingen om kan ta ett beslut om att påbörja personuppgiftsbehandlingen. Utöver att fastställa och tillsätta en intern dataskyddsorganisation behöver förvaltningen därför även se över hur beslut kopplat till dataskyddsförordningen ska hanteras, och vilka beslutsmandat olika befattningar ska ha. Dataskyddsenheten har under 2023 tagit fram och tillhandahållit ett stödmaterial som förvaltningen kan utgå från i det arbetet.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar

verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudet har i tidigare årsrapporter lyft att förvaltningen bedöms ha stora risker när det kommer till hanteringen av personuppgiftsincidenter, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde. De risker som identifierats är både kopplade till medarbetares kunskaper och den praktiska hanteringen.

Utifrån gjorda iakttagelser under året bedömer dataskyddsombudet att den allmänna kunskapen om incidenter inom förvaltningen är låg, och att medarbetare inom förvaltningen saknar kunskap om vad en incident är och hur de ska omhändertas inom organisationen. Dataskyddsombudet har också kunnat se att det under året varit svårt för medarbetare att hitta rätt information om vad som ska göras när en incident inträffar eller upptäcks, då informationen kopplat till dataskydd/incidenthantering på intranätet är felaktig. Då den felaktiga informationen fortfarande kvarstår, trots att dataskyddsombudet uppmärksammat förvaltningen om detta, rekommenderas förvaltningen framåt vidta åtgärder för att uppdatera denna med syftet att ge medarbetare rätt förutsättningar i hanteringen.

Dataskyddsombudet har under året även noterat att förvaltningen, i rollen som biträde genom incidentkoordinatorerna, vidtagit ett antal åtgärder för att förbättra incidenthanteringsprocessen. Det är positivt att förvaltningen har arbetet med frågan under året för att förbättra och utveckla incidenthanteringen. Ytterligare rekommendationer och kommentarer kopplat till förvaltningens hantering av personuppgiftsincidenter lämnas i uppföljningen under punkt 3.3.1.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad från verksamheten bedömningen att vissa av de identifierade riskerna är så höga att de kräver omgående insatser ifrån ledningsnivå.

Utifrån gjorda iakttagelser och förvaltningens genomgående låga skattning inom kontrollpunkten bedömer dataskyddsombudet att det föreligger stora risker kopplat till förvaltningens hantering av biträdesavtal och andra överenskommelser.

Förvaltningen uppger i dialog med dataskyddsombudet att de låga resultaten hänvisar till biträdesavtal mellan Intraservice och verksamheter i staden, och inte mellan Intraservice och externa leverantörer. Dataskyddsombudet delar förvaltningens bedömning gällande att det finns stora risker med bristerna i den

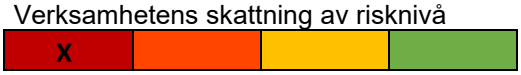
interna regleringen av ansvarsförhållanden, men ser samtidigt att denna fråga inte kommer kunna lösas förrän ansvaret för olika staden gemensamma personuppgiftsbehandlingarna har utretts. Förvaltningens möjligheter att ensamt hantera dessa frågor bedöms vara begränsade. Under året har dock förvaltningen tagit ett större ansvar för att, utifrån förutsättningarna, utreda och fastställa den egna nämndens personuppgiftsansvar för ett antal behandlingar. Även om ledning och samordning i frågan fortfarande saknas på central nivå i Staden, är det positivt att förvaltningen börjat agera i frågan. Dataskyddsombudet har även noterat att behovet av att utreda ansvarsförhållandena lyfts från både förvaltnings- och nämndnivå till stadsledningskontoret respektive kommunstyrelsen.

Dataskyddsombudet bedömer dock att förvaltningen har risker även kopplat till avtalsrelationer med externa leverantörer, vilket i sig medför risker för övriga Staden utifrån förvaltningens roll som tjänsteleverantör. I rollen som tjänsteleverantör är förvaltningen ansvarig för de personuppgiftsbiträdesavtal som ingås med leverantörer för de tjänster som övriga verksamheter använder, för vilka förvaltningen agerar ”mellanhand” mellan verksamheter i staden och leverantören. Då verksamheter i staden saknar insyn, och inte kan påverka vilka leverantörer som väljs eller hur avtalen hanteras, åligger det ett stort ansvar på förvaltningen att säkerställa avtalens innehåll och hantering, såväl som efterlevnad.

Förvaltningen rekommenderas utifrån ovan, kopplat till externa leverantörer, att ta fram arbetssätt/rutiner för hantering av personuppgiftbiträdesavtal och andra överenskommelser. I ett sådant dokument bör det bland annat framkomma när avtal/överenskommelser ska tecknas, vem som är behörig att göra detta, vilka krav som ska uppfyllas, samt hur regelbunden uppföljning och kontroll av hela kedjan av underbiträden ska genomföras.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser av ledning och/eller övriga verksamheten. Dataskyddsombudet delar verksamhetens bedömning om att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Förvaltningen behöver ta ett omtag i arbetet med behandlingsregistret och starta om från början med att kartlägga de personuppgiftsbehandlingar som förekommer inom verksamheten. Ett sådant arbete är omfattande och kräver resurser både för samordning och identifiering. För att registret ska kunna bli heltäckande behöver även alla olika delar av förvaltningen involveras i och bidra till arbetet.

En grundläggande förutsättning för att förvaltningen ska kunna åtgärda bristerna och upprätta, samt underhålla, ett behandlingsregister som uppfyller lagkraven är att det finns en intern dataskyddsorganisation på plats. Dataskyddsombudet rekommenderar därför förvaltningen att innan arbetet med behandlingsregistret påbörjas först säkerställa att det finns en fastställd intern dataskyddsorganisation, med tillräckliga resurser, mandat och kompetens, som kan samordna och arbeta med frågorna inom förvaltningen.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande behandlingsregistret enligt GDPR. Då förvaltningen saknar dataskyddsorganisation deltog ingen från Intraservice på de informationsinsatser som dataskyddsenheten genomförde under våren 2023. I samband med informationsinsatsen tillhandahölls skriftligt underlag för stadens samtliga verksamheter. Förvaltningen kan med fördel använda sig av underlaget som stöd i arbetet framåt.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

	X		

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad från verksamheten bedömningen att vissa av de identifierade riskerna är så höga att de kräver omgående insatser ifrån ledningsnivå.

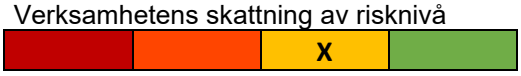
De risker som identifierats av såväl dataskyddsombudet som förvaltningen under de senaste åren är återkommande. En av dessa risker är att det saknas styrning och stöd när det kommer till dataskyddsfrågor inom förvaltningen. Konsekvenserna av detta påverkar både enskilda medarbetare, som tvingas arbeta i stuprör eftersom det inte finns ledning i hur man ska gå till väga, och förvaltningen som helhet, då förvaltningen inte kan arbeta riskbaserat. Även brister i styrningen bedöms vara sammankopplat till avsaknaden av en intern dataskyddsorganisation. Förvaltningen kan inte arbeta riskbaserat eftersom det inte finns någon intern funktion som har ett helhetsgrepp över allt som sker på förvaltningen. Det finns därför ingen överblick kring vilka behandlingar som sker idag och vilka som planeras, varför det inte går att prioritera utifrån risker.

Avsaknad av styrning innebär också att förvaltningen inte har kontroll på hur dataskyddsfrågorna hanteras inom verksamhetens olika delar. Här bedömer dataskyddsombudet att det föreligger stora risker då tjänsteutveckling och initiativ kan fortlöpa obehindrat utan någon kvalitetssäkring utifrån lagkrav. Dataskydds-ombudets uppfattning är att man inom stora delar av verksamheten fortfarande har mer fokus på att kunna leverera nya funktioner/teknik än att kontrollera så att dessa är förenliga med de lagar som styr verksamheten.

Förvaltningen rekommenderas att ta fram en övergripande strategi och styrning för dataskyddsarbetet. Utöver att strategin behöver omfatta förvaltningens arbete framåt med de grundläggande delarna kopplat till register, incidenthantering och informationsplikten behöver den även sätta ramarna för förvaltningens tjänsteutveckling och relatera till det ansvar som förvaltningen har i egenskap av tjänsteleverantör. För att den övergripande strategin ska vara ändamålsenlig och skapa förutsättningar för att dataskyddsarbetet ska bli en integrerad och naturlig del av hela verksamheten behöver strategin omfatta förvaltningens ansvar både i egenskap av personuppgiftsansvarig och personuppgiftsbiträde.

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 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 möter regelbundet medarbetare inom förvaltningen som saknar kunskap om dataskyddslagstiftningen och, utifrån de dialoger som dataskyddsombudet haft inom verksamheten, bedöms intresset för att följa gällande lagstiftning ibland som lågt. Det är förekommer att man försöker skjuta ifrån sig ansvaret och inte tycker att man som enskild medarbetare behöver lära sig eller ta ansvar för att följa reglerna.

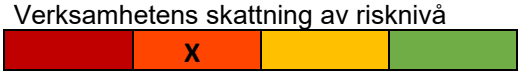
Utifrån gjorda iakttagelser bedöms det inom förvaltningen finnas ett stort behov av utbildning i dataskyddsfrågor. Behovet av att höja kunskapsnivån inom förvaltningen har lyfts i tidigare årsrapporter, och dataskyddsombudet vill därför igen påminna förvaltningen om att dataskyddsenheten tillhandhåller utbildningar samt kan genomföra riktade informationsinsatser.

Dataskyddsombudet vill i sammanhanget uppmärksamma att olika medarbetare kan ha olika behov av utbildnings- och informationsinsatser utifrån sin roll och sina arbetsuppgifter. För att säkerställa att resurser sätts in där det främst behövs rekommenderas förvaltningen kartlägga vilken nivå av dataskyddskunskaper som olika befattningar behöver ha och säkerställa att medarbetare löpande utbildas därefter. På så sätt ges medarbetarna rätt förutsättningar att integrera dataskyddsperspektivet i sitt dagliga arbete och att hantera personuppgifter korrekt utifrån sin roll inom förvaltningen.

Då förvaltningen har ett stort antal konsulter inom verksamheten bedöms det även viktigt att denna grupp erbjuds utbildning i dataskydd och närliggande lagstiftning.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad från verksamheten bedömningen att vissa av de identifierade riskerna är så höga att de kräver omgående insatser ifrån ledningsnivå.

Eftersom förvaltningen saknar översyn och kunskap kring de behandlingar som faktiskt sker i verksamheten bedömer dataskyddsombudet att förvaltningen i dagsläget inte har möjlighet att uppfylla informationsplikten gentemot de registrerade. En grundläggande förutsättning för att förvaltningen ska kunna åtgärda bristerna är att det finns ett behandlingsregister, vilket i sin tur kräver att det finns en intern dataskyddsorganisation på plats. Dataskyddsombudet rekommenderar därför förvaltningen att innan arbetet med informationsplikten påbörjas först säkerställa att det finns en fastställd intern dataskyddsorganisation med tillräckliga resurser, mandat och kompetens. När den interna organisationen är på plats och arbetet med att ta fram ett behandlingsregister påbörjats, kan även delarna kopplat till informationsplikten tas med i arbetet.

Förvaltningen behöver i det arbetet se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I detta arbete är integritetspolicyn en del och förvaltningen rekommenderas även att framåt säkerställa att de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande informationsplikten enligt GDPR. Då förvaltningen saknar dataskyddsorganisation deltog ingen från Intraservice på de informationsinsatser som dataskyddsenheten genomförde under våren 2023. I samband med informationsinsatsen tillhandahölls skriftligt underlag för stadens samtliga verksamheter. Förvaltningen kan med fördel använda sig av underlaget som stöd i arbetet framåt.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar

verksamhetens bedömning om att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Utifrån den egna skattningen rekommenderas förvaltningen att vidta följande åtgärder:

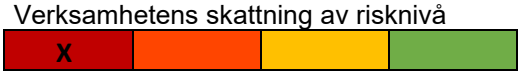
- Ta fram dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut.
- Ta fram dokumenterade arbetssätt som säkerställer att medarbetare informeras om dokumenthantering och gallring kopplat till kraven enligt GDPR.
- Att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.
- Att ta fram dokumenterade arbetssätt och information om hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas.
- Att ta fram dokumenterade arbetssätt och information som beskriver hur personuppgifter får hanteras e-post.

Vid genomgången av årsrapporten anger förvaltningen att det alldeles nyligen tagits fram en uppdaterad dokumenthanteringsplan. Dataskyddsombudet ser positivt på det och rekommenderar förvaltningen att säkerställa att alla medarbetare och konsulter inom förvaltningen har kännedom om dokumenthanteringsplanen.

Utifrån vad som anges av förvaltningen vid genomgången av årsrapporten är dataskyddsombudets uppfattning att den gjorda skattningen på vissa frågor inom kontrollpunkten kan vara felaktig. Förvaltningen rekommenderas därför se över hur svaren förhåller sig till de faktiska förutsättningarna, med syftet att kunna utröna om, och i så fall vilka, av ovan angivna åtgärder som kan behöva vidtas.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser av ledning och/eller övriga verksamheten. Dataskyddsombudet delar verksamhetens bedömning om att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Dataskyddsombudets bedömning är att det saknas förvaltningsövergripande arbetssätt kopplat till konsekvensbedömningar. Medarbetare i förvaltningen vet inte hur, när och varför en konsekvensbedömning ska genomföras. Om en konsekvensbedömning faktiskt genomförs, saknas information om hur den ska tas vidare och vem som har mandat att fatta beslut utifrån underlaget.

Förvaltningen rekommenderas att ta ett omtag kring arbetet med konsekvensbedömningar. Det gäller både intern kompetensutveckling för de funktioner som ska arbeta med frågan, och information och utbildning till övriga verksamheten. Dataskyddsenheten har sedan tidigare tagit fram ett mallstöd och en mall för arbetet med konsekvensbedömningar vilka förvaltningen rekommenderas att utgå från i arbetet. Förvaltningen rekommenderas också att säkerställa att dataskyddsombudet involveras i god tid vid arbetet med konsekvensbedömningar. Detta är ett absolut krav enligt GDPR.

Då förvaltningen inte arbetar, eller har arbetat, aktivt med dataskydd föreligger en stor skuld när det kommer till genomförandet av konsekvensbedömningar enligt GDPR. Det finns även ett stort antal behandlingar, vilka sannolikt innebär höga risker för de registrerade, som inte riskbedömts. Att behandlingarna inte säkerställts genom en riskbedömning och/eller konsekvensbedömning innebär att personuppgifter riskeras att behandlas felaktigt eller utan tillräckliga skyddsåtgärder. Dataskyddsombudet bedömer att en genomgående brist inom förvaltningen är att det i tjänsteleveransen inte kan säkerställas tillräckliga skyddsåtgärder för att upprätthålla skyddet för de personuppgifter som behandlas.

En konsekvensbedömning ska vara ett verktyg för att bedöma risker med en personuppgiftsbehandling. Det finns även vissa delar som ett underlag ska innehålla för att kunna anses uppfylla kriterierna för en godtagbar konsekvensbedömning enligt GDPR. Idag förekommer det att medarbetare inom förvaltningen gör konsekvensbedömningar på tjänster utan att veta vilka behandlingar som ingår i tjänsterna. Denna hantering bedömer dataskyddsombudet vara fel, och medför problem samt förvirring när underlagen sedan skickas ut i Staden. Det finns i vissa fall behov av att ta fram material som beskriver en tjänst och vilka risker (för personuppgifter) som användningen av denna kan innebära. Det är viktigt att förvaltningen skiljer detta underlag (”tjänstebeskrivning/specifikation”) från vad som utgör en konsekvensbedömning. Konsekvensbedömningar kan förvaltningen ej genomföra för hela staden, utan enbart för den egna behandlingen som förvaltningen är personuppgiftsansvarig för. Förvaltningen rekommenderas därför att sluta ta fram ”konsekvensbedömningar” eller liknande underlag för tjänster, och i stället ta fram nya arbetssätt för tillhandahållandet av information kopplat till förvaltningens skyldigheter som personuppgiftsbiträde.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser av ledning och/eller övriga verksamheten. Dataskyddsombudet delar verksamhetens bedömning om att det inom

kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Dataskyddsombudet anser att det är anmärkningsvärt att en förvaltning som ansvarar för Stadens digitala infrastruktur och vars uppdrag är att ta fram och utveckla IT-tjänster bedömer sig ha så stora risker kopplat till IT-projekt och upphandling. Utifrån det stora, och till stor del staden övergripande, ansvar som åligger förvaltningen inom området borde rimligen förvaltningen ligga i framkant i dessa delar.

Dataskyddsombudet bedömer att riskerna beror på att det saknas rutiner och processer för hur lagkrav både kopplat till dataskydd, informationssäkerhet och angränsande lagstiftning, ska omhändertas vid uppstart av nya IT-projekt och vid upphandlingar. Det bedöms vara mer en regel än ett undantag att förvaltningen utvecklar eller säljer en tjänst utan att man har säkerställt följsamhet till gällande lagstiftning. Som nämns under kontrollpunkt 5 bedöms avsaknaden av styrning medföra att tjänsteutveckling och initiativ kan fortlöpa obehindrat utan någon kvalitetssäkring utifrån lagkrav. Då denna problematik inte är ny, utan tvärt emot är något som har lyfts regelbundet som en brist de senaste åren, ser dataskydds-ombudet allvarligt på att inga åtgärder har vidtagits för att hantera bristerna. Dataskyddsombudet har i tidigare årsrapporter rekommenderat förvaltningen att internt tydliggöra att det inte är valfritt för medarbetare att följa de lagar och regler som gäller för verksamheten, utifrån gjorda iakttagelser under året bedöms det även fortsatt finnas behov av detta.

Utifrån ovan rekommenderas förvaltningen att omgående vidta följande åtgärder för att hantera bristerna som föreligger inom kontrollpunkten:

- Ta fram dokumenterade arbetssätt som säkerställer att dataskyddsperspektivet omhändertas vid uppstart av nya digitaliseringslösningar.
- Ta fram dokumenterade arbetssätt som säkerställer att riskbedömningar görs vid arbete med utveckling och upphandling av nya system och tjänster.
- Ta fram dokumenterade arbetssätt som säkerställer att dataskyddsperspektivet omhändertas vid kravställning i upphandling så att inbyggt dataskydd och dataskydd som standard uppfylls.
- Ta fram dokumenterade arbetssätt som säkerställer att dataskyddsombudet involveras från start vid nya IT-projekt, upphandlingar och/eller införandet av nya tjänster där personuppgifter kommer att hanteras.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

	X		

Dataskyddsombudets bedömning

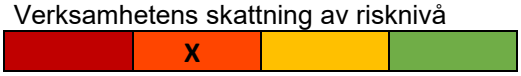
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Utifrån den egna skattningen rekommenderas förvaltningen att vidta följande åtgärder:

- Ta fram dokumenterade arbetssätt för tilldelning av behörigheter och åtkomster i alla IT-system, som säkerställer att medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter.
- Ta fram dokumenterade arbetssätt som säkerställer att uppföljning av behörigheter och åtkomster sker.
- Ta fram dokumenterade arbetssätt för att systematiskt kunna följa upp och kontrollera så att användning av system och/eller andra digitala verktyg följer antagna styrande dokument.
- Ta fram dokumenterade arbetssätt som säkerställer att dataskyddsperspektivet omhändertas vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.
- Ta fram en heltäckande dokumentation över alla IT-system och digitala verktyg som används inom organisationen.
- Ta fram målgruppsanpassad information för de digitala verktyg som används/tillhandahålls.
- I den mån förvaltningen har en egen hemsida, säkerställ att hanteringen av cookies uppfyller gällande lagkrav. Säkerställ också att de medarbetare som ansvarar för stadens hemsida har kunskap om gällande lagstiftning.
- Ta fram en dokumentation över samtliga kommunikationskanaler och säkerställ att användningen följer GDPR.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet har enbart involverats i någon enstaka fråga kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

De risker som föreligger inom kontrollpunkten bedöms vara nära sammankopplade med avsaknaden av ett behandlingsregister, då en överblick av verksamhetens

behandlingar är en förutsättning för att de registrerades rättigheter ska kunna hanteras korrekt. Dataskyddsombudet vill därför särskilt lyfta att medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och de behandlingar som görs i verksamheten. Utan överblick av alla behandlingar som sker inom verksamheten, ser dataskyddsombudet en risk att förvaltningen missar behandlingar som görs inom verksamheten vid handläggning av registerutdrag. Det medför även risk för att alla begäran inte kan behandlas likartat och att de registrerade därmed inte får samma information i registerutdragen, till exempel gällande ändamålen med behandlingen.

Förvaltningen rekommenderas framåt se över vilka åtgärder som behöver vidtas för att registrerade ska kunna utöva sina rättigheter i enlighet med förordningen. Dataskyddsombudet bedömer att det sannolikt främst bör handla om åtgärder kopplat till utbildning (kontrollpunkt 6) och behandlingsregistret (kontrollpunkt 4).

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 (2022): Integritetspolicy

Verksamheten gavs följande rekommendationer:

- Ta fram verksamhetsspecifik information (intern integritetspolicy) som fokuserar på de behandlingar som omfattar anställda.
- Utreda hur policyn bättre kan formuleras, t.ex. med hjälp av skiktad integritetspolicy, eller hur det annars kan säkerställas att information lämnas till de registrerade.
- Se över informationen om tredjelandsöverföring.
- Ange precis lagringstid för uppgifterna (inte ange "så länge det är nödvändigt för de berättigade ändamålen").
- Om samtycke används som rättslig grund rekommenderas det att informationen kompletteras med uppgifter om hur ett samtycke kan återkallas.
- Se över språket för att uppfylla kravet på ett klart och tydligt språk.
- Ta bort hänvisning till intranätet eftersom informationen där är ej åtkomlig för utomstående och inte kan fungera som ett komplement till integritetspolicyn.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Förvaltningen har i skrivande stund vidtagit åtgärder i form av att

lyfta in rekommendationerna i projektet EPA (etablera processer och arbetssätt för styrning och uppföljning för informationssäkerhet). Någon konkret tidsplan för specifika aktiviteter kopplat till rekommendationerna i den fördjupade kontrollen har inte tillhandahållits dataskyddsombudet.

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.

Kontroll (2021): Personuppgiftsbiträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

- Förvaltningen bör utforma och bilägga instruktioner till de personuppgiftsbiträdesavtal där det saknas.
- Förvaltningen bör ta fram rutin eller tydliggöra hur redan existerande stöddokument ska användas vid säkerställande/uppföljning av ett biträdes tekniska och organisatoriska säkerhetsåtgärder.
- Förvaltningen bör utreda behov av att ta fram rutin för avtalsuppföljning.
- Förvaltningen bör överväga att i så stor utsträckning som möjligt använda egen mall för personuppgiftsbiträdesavtal för att minimera risken för ofördelaktiga avtalsvillkor.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Åtgärder som har vidtagits är att en egen mall för personuppgiftsbiträdesavtal är framtagen samt att rutiner för avtalshantering och uppföljning är under framtagande.

Då de kvarstående rekommendationerna inom kontrollen bedöms överlappa med de rekommendationer som lämnas under kontrollpunkt 3 kommer den fortsatta uppföljningen ske inom ramen för fasta kontrollpunkter.

Särskild uppföljning (2021): Intraservice hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Förvaltningen rekommenderas göra en översyn av rutiner och processer för att säkerställa att incidenter inte missas.
- Förtydliga rutinen med när och hur dataskyddsombudet ska involveras.
- Utreda hur tiden mellan att förvaltningen får kännedom om en incident och rapportering till personuppgiftsansvariga sker kan minska.
- Ta fram tydliga instruktioner för vilken information som ska kommuniceras.

- Säkerställa tillräcklig kompetens och möjlighet till utbildning hos berörda parter.

Kommentarer och rekommendationer:

I uppföljningen anger förvaltningen att följande åtgärder vidtagits för att hantera de rekommendationer som lämnats av dataskyddsombudet:

- Rutin för utbildning av nyanställd personal i incidentprocessen.
- Ny rutin där information om incidenter sänds till Dataskyddsenhetens funktionsbrevlåda med kopior på alla incidenter. Dataskyddsombud har tillgång till Servicenow.
- Förtydligande information till PUA gällande tid och vilken information som ska lämnas.
- Incidentteamet går på Dataskyddsenhetens utbildningar samt i möjligaste mån externa utbildningar.
- I EPA projektet finns planerade aktiviteter för utbildning och ytterligare förändring av incidenthanteringsprocessen.

Det är positivt att förvaltningen har arbetat med frågan och att flera åtgärder vidtagits. Dataskyddsombudet bedömer dock att det fortfarande föreligger risker kopplat till själva incidenthanteringsprocessen, den låga kunskapsnivån inom förvaltningen samt kopplat till dokumentationen av incidenter. Det är för dataskyddsombudet även oklart hur prioriterad denna fråga är inom ramen för EPA-projektet. Ytterligare uppföljning kommer därför att göras under 2024.

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

Fastställ och tillsätt en intern dataskyddsorganisation, med tillräckliga resurser, mandat och kompetens, som kan samordna och arbeta med frågorna inom förvaltningen.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Ta fram ett personuppgiftsbehandlingsregister. Gå igenom verksamhetens personuppgiftsbehandlingar, se över hur dessa ska definieras och dokumentera respektive behandling utifrån kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

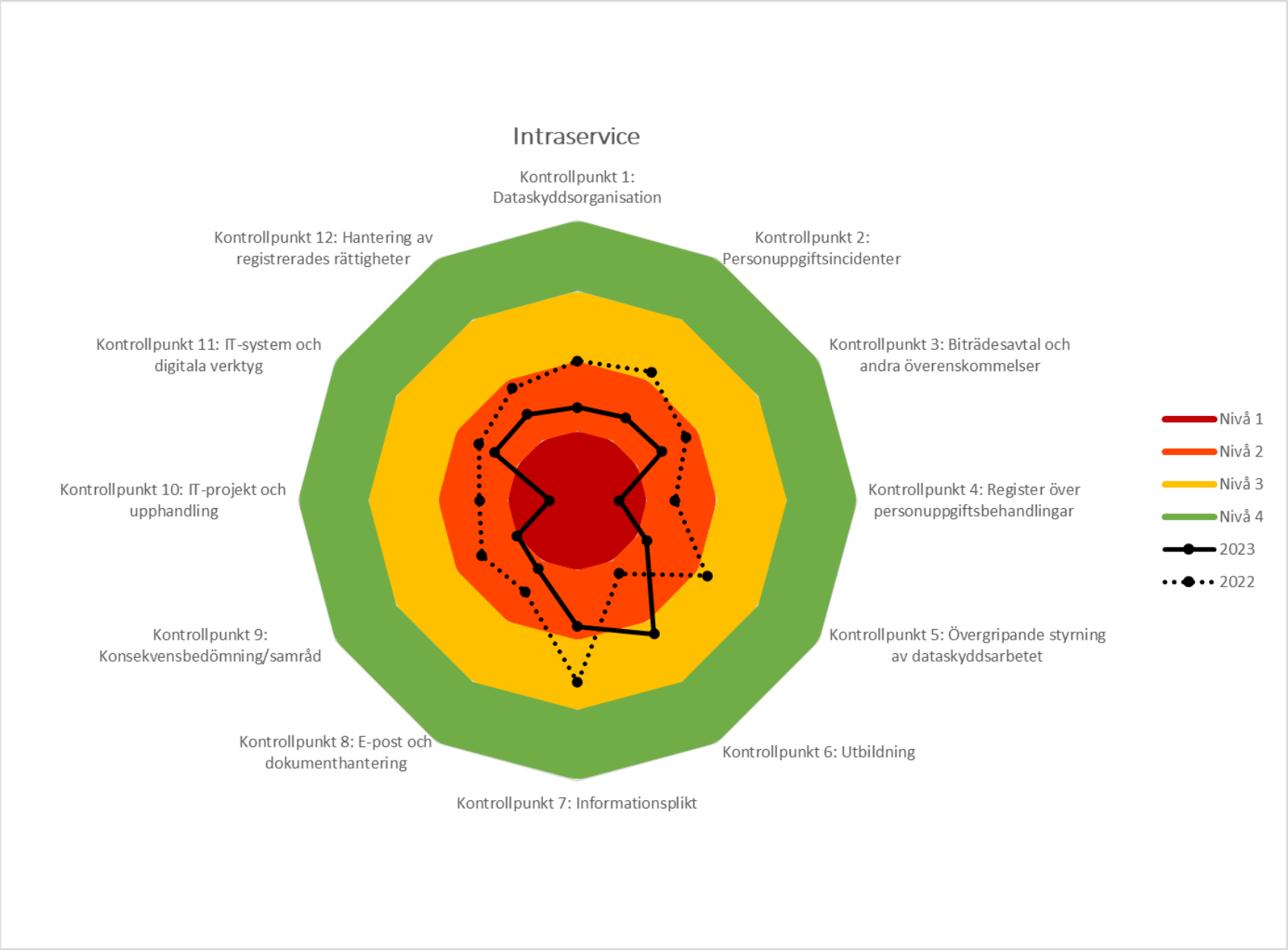
Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

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

Intraservice

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.