Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Miljöförvaltningen

2012-12-20

Innehåll

1 Dataskydd i kommunal verksamhet

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

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

1.1 Göteborgs Stads dataskyddsombud

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

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

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

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

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

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

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

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

2.2 Fördjupad kontroll

2.2.1 Kontroll av behörighetsstyrning 2022

Den fördjupade kontrollen har bestått av behörighetsstyrning. Resultatet av kontrollen presenteras i sin helhet i bilaga ”2”.Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och därför lämnat ett antal rekommendationer till verksamheten att vidta åtgärder.

- Förvaltningen rekommenderas att se över och dokumentera sitt arbetssätt för tilldelning av behörigheter.
- Förvaltningen rekommenderas att se över och dokumentera sitt arbetssätt för uppföljning av tilldelade behörigheter.
- Förvaltningen rekommenderas att införa åtkomstkontroll/loggуppföljning i form av regelbundna slumpmässiga stickprovskontroller.
- Förvaltningen rekommenderas att utreda och följa upp sekretessfrågor, kopplat till behörighetsstyrning, tillsammans med förvaltningsjurist.
- Förvaltningen rekommenderas att utreda behovet av att genomföra konsekvensbedömningar av behandlingarna i systemet, alternativt dokumentera varför sådana inte anses vara nödvändiga.

2.3 Årlig kontroll av dataskyddsarbetet

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

2.3.1 Metod och risknivåer

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

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	

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

Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Miljöförvaltningens dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet upplever att det finns en väl fungerande intern organisation och att verksamheten lyfter många och viktiga dataskyddsfrågor med dataskyddsombudet. Således instämmer dataskyddsombudet med den skattning som verksamheten gjort för kontrollpunkten.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Verksamheten har angett att man har goda förutsättningar för att hantera personuppgiftsincidenter i form av arbetssätt och rutiner. Dataskyddombudet instämmer i verksamhetens skattning. Under hösten 2022 inträffade en större personuppgiftsincident inom verksamheten. För en vidare diskussion om detta se avsnitt 3.5.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Dataskyddsombudets kommentarer:

Verksamheten har angett att det saknas tillräckliga rutiner för bedömningen om en ny leverantör är ansvarig eller biträde och för tecknandet av biträdesavtal. Personuppgiftsbiträdesavtal har tecknats med under eller upp till 75 % av verksamhetens anlitade personuppgiftsbiträden. Vidare anger förvaltningen att det saknas rutiner för att bedöma andra typer av överenskommelse/avtal som behövs upprättas avseende gemensam/ annan delad hantering av personuppgifter. Verksamheten har svarat att det saknas tillräckliga rutiner för att kontinuerligt genomföra efterlevnadskontroller och rutiner samt kompetens för att bedöma hela kedjan av underbiträden vid anlitandet av nya personuppgiftsbiträden. Dataskyddsombudets rekommendation är att förvaltningen tar fram heltäckande rutiner för alla delar som rör hanteringen av biträdesavtal och andra överenskommelser.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

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

Dataskyddsombudets kommentarer:

Verksamheten uppger att cirka 75% av samtliga behandlingar är införda i förvaltningens personuppgiftsregister, men att det delvis saknas rutiner för att säkerställa att nya behandlingar förs in i registret. Dataskyddsombudet rekommenderar att verksamheten för in samtliga behandlingar och att förvaltningen tar fram en rutin för att tillförsäkra att nya eller förändrade behandlingar upptas i registret.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Verksamheten har under denna punkt angett att man har en övergripande strategi för arbetet med dataskydd och att man arbetar systematiskt med att integrera dataskyddsfrågorna i informationssäkerhetsarbetet. Förvaltningen har identifierat och värderat under eller upp till 75% av sina informationstillgångar i enlighet med stadens styrande dokument och genomför regelbundna interna kontroller för att säkerställa följsamheten gentemot GDPR.

Verksamheten anger vidare att förvaltningen har antagit ett riskbaserat arbetssätt men att det saknas en informationssäkerhetspolicy som övergripande beskriver hur organisationen ska hantera personuppgifter avseende skydd av IT-system och andra digitala enheter. Verksamheten anser att inte heller att det finns tillräckliga rutiner som säkerställer att de styrande dokument som reglerar personuppgiftsbehandlingar hålls uppdaterade. Dataskyddsombudet rekommenderar att verksamheten ser över dessa lågt självskattadeområden och vidtar åtgärder/ tar fram rutiner som behövs

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i verksamhetens bedömning men rekommenderar att förvaltningen tar fram rutiner för att kunna följa upp och bibehålla kunskapsnivån hos medarbetare som genomgått utbildningar.

2.4.7 Kontrollpunkt 7: Integritetspolicy

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

Dataskyddsombudets kommentarer:

Verksamheten har genomgående besvarat enkätfrågorna inom kontrollpunkten med höga värden. Dataskyddsombudet instämmer dock inte i verksamhetens bedömning och anser att det saknas väsentliga delar i policyn, bland annat avseende hantering av cookies. Men att informationen även brister i andra avseenden rörande de krav på information till de registrerade som följer av artikel 13 och 14 i GDPR. Förvaltningen har tagit fram ett uppdaterat förslag till policy och Dataskyddsombudets rekommendation är därför att verksamheten tillsammans med dataskyddsombudet tittar på vilka delar av policyn som behöver kompletteras och genomför dessa uppdateringar för att kraven i dataskyddsförordningen ska kunna efterlevas. Kontrollpunkten kommer att följas uppunder 2023.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

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

Dataskyddsombudets kommentarer:

Verksamheten har skattat att 100 % av förvaltningens personuppgiftsbehandlingar har informationsklassificerats och att de registrerade informeras direkt i samband med kontakt om hur verksamheten behandlar personuppgifter. Det som däremot saknas är en fastställd dokumenthanteringsplan och rutiner för att kontrollera att handlingar innehållandes personuppgifter gallras enligt gällande beslut. Dataskyddsombudets rekommendation är att förvaltningen tar fram en uppdaterad dokumenthanteringsplan och rutiner för att säkerställa att gallring sker enligt gällande gallringsbeslut.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Dataskyddsombudets kommentarer:

Verksamhetens enkätsvar indikerar att det finns flera förbättringsområden inom kontrollpunkten, även om den når upp till nivå ”gul”. Skattningen visar att flera rutiner saknas för konsekvensbedömningar. Att genomföra

konsekvensbedömningar är i många fall ett absolut krav och om detta inte genomförs riskerar förvaltningen att missa att vidta åtgärder som behövs för att säkerställa de registrerades rättigheter.

Den interna dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet av en konsekvensbedömning. Det är även av vikt att verksamheten har rutiner för att följa upp identifierade risker. Förvaltningen rekommenderas att klargöra och ta fram dokumenterade rutiner och processer för hur arbetet med konsekvensbedömningar inom verksamheten ska gå till. Vidare rekommenderas miljöförvaltningen att kartlägga samtliga behandlingar där det förekommer höga risker och genomföra konsekvensbedömningar där så krävs. Det rekommenderas också att förvaltningen tydliggör vilka som har mandat att fatta beslut i frågor rörande konsekvensbedömningar och riskacceptans.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

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

Dataskyddsombudets kommentarer:

Verksamheten har inte identifierat några stora risker kopplade till kontrollpunkten och dataskyddsombudet har ingen anledning att göra någon annan bedömning än den skattning som förvaltningen själva har gjort.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

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

Dataskyddsombudets kommentarer:

Verksamheten har på denna punkt skattat sitt arbete högt, men det är stor spridning på svaren. Utifrån de svar som lämnats av förvaltningen så rekommenderar dataskyddsombudet att förvaltningen tar fram rutiner för att systematisk kunna följa upp och kontrollera att användningen av digitala verktyg följer antagna

riktlinjer, samt att verksamheten tar fram rutiner för att säkerställa att dataskyddsperspektivet beaktas vid införandet och användandet av kostnadsfria tjänster som gratisappar och sociala medier.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

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

Dataskyddsombudets kommentarer:

Den sammantagna bedömningen utifrån verksamhetens skattning är att förvaltningen har goda möjligheter att tillvarata de registrerades rättigheter, en bedömning som dataskyddsombudet delar. Förvaltningen rekommenderas dock att kontinuerligt fortsätta informera medarbetare om de registrerades rättigheter.

2.5 Särskilda iakttagelser under året

2.5.1 Personuppgiftsincident avseende serveringstillstånd

Under oktober 2022 upptäcktes en personuppgiftsincident avseende personuppgifter som på ett eller annat sätt kunde kopplas till miljöförvaltningens register över serveringstillstånd. Dataskyddsombudet tänker inte i detalj gå in på incidenten, då nämnden under hösten 2022 fått separat information från förvaltningen om det inträffade. Dataskyddsombudet vill ändå passa på att delge några reflektioner kring det inträffade. Den inträffade incidenten är allvarlig, både på grund av dess omfattning med närmare 27 000 registrerade totalt, men också på grund av känsligheten i uppgifterna, då ett 50-tal registrerade med olika typer av skyddade personuppgifter omfattas av incidenten. Händelsen visar på vikten av ett fungerande dataskyddsarbete i organisationens alla delar.

Av central betydelse är att organisationen har full koll på samtliga sina IT-lösningar och personuppgiftsbehandlingar för att kunna förstå vilka risker som finns förknippade med varje enskild behandling och eller IT-lösning. Det är den proaktiva delen. Den innefattar att det finns ett fungerande arbete med ett fullständigt register över verksamhetens alla personuppgiftsbehandlingar och att förvaltningen kontinuerligt arbetar med att säkerställa att både nya och äldre system och IT-lösningar uppfyller kraven på tillräcklig säkerhet, både för personuppgifter och annan information. Ett led i detta är rutiner både för upphandling/införande av nya lösningar, samt för efterlevnadskontroll av redan

driftsatta system och att verksamheten aktivt arbetar med konsekvensbedömningar för att korrekt kunna bedöma risker.

Incidenten visar också på vikten av en fungerande incidenthantering när något väl har skett, att det finns rutiner och arbetssätt för att förstå och upptäcka en incident, utreda incidenten och ta ställning till om och hur den ska anmälas till IMY. Den visar också på vikten av fungerande rutiner för kontakt med de registrerade. När och hur ska de registrerade informeras, vilken information som ska lämnas och hur eventuella anspråk på skadestånd ska hanteras. Dataskyddsombudets bedömning är att miljöförvaltningen har en god kompetens i dessa frågor med många välfungerande rutiner. Förvaltningen har enligt dataskyddsombudets uppfattning hanterat incidenten på ett förtjänstfullt sätt. Det innebär inte att allt har varit fläckfritt. Men genom enträget arbete är ändå den samlade bedömningen att arbetet med incidenthanteringen har flutit på bra. Förvaltningen har dragit många lärdomar och erfarenheterna från händelsen har lett till att rutiner och arbetssätt som saknades före det inträffade har tagits fram och adderats till befintliga rutiner. Det innebär till exempel att förvaltningen som första verksamhet i Göteborgs Stad har en fungerande hantering av skadestånd till de registrerade. Flera lärdomar från det inträffade är av sådan art att det kommer komma hela Staden till nytta, inte minst då det omfattande utredningsarbete som miljöförvaltningen gjort angående den nyss nämnda skadeståndsfrågan.

Sammantaget är dataskyddsombudets förhoppning att förvaltningen fortsätter arbeta vidare med dataskyddsfrågorna på ett organiserat sätt och drar nytta av de erfarenheter som incidenten gett i det arbetet.

2.6 Sammanfattande rekommendationer

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

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

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Verksamheten rekommenderas att se över nuvarande hantering och ta fram rutiner för anlitande av biträden och uppföljning av ingångna biträdesavtal

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamheten rekommenderas att ta fram rutiner och processer för hur arbetet med konsekvensbedömningar inom förvaltningen ska bedrivas

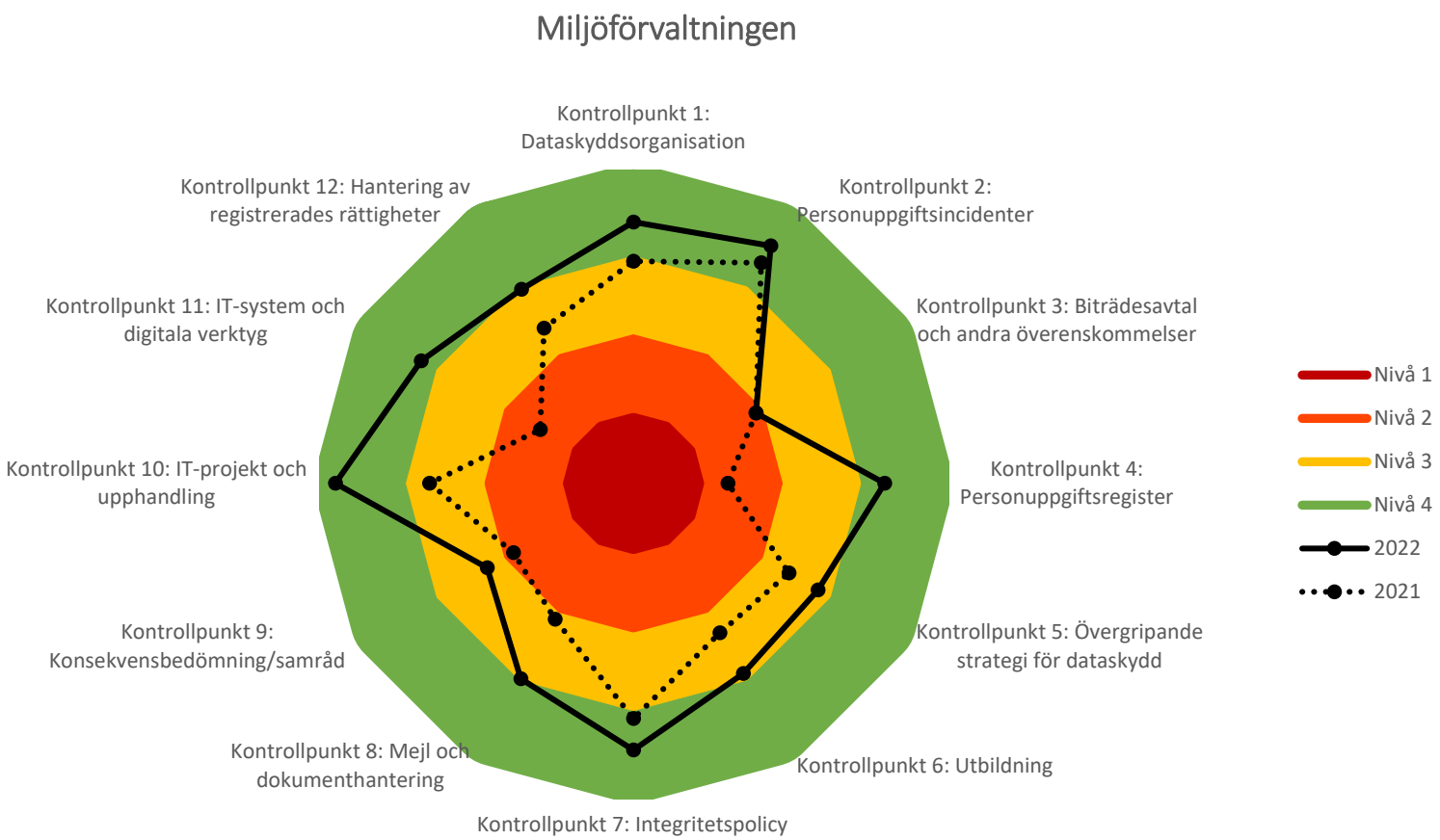
Verksamheten rekommenderas att ta fram rutiner för riskacceptans och att tydliggöra vem som har mandat att fatta beslut i frågor som rör konsekvensbedömningar.

3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022

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



Fördjupad kontroll

Kontrollpunkt 11: Behörighetsstyrning Miljöförvaltningen, EDP Vision

Bakgrund

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

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

En medarbetare i en verksamhet bör endast ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. Verksamheten bör därför överväga behovet av att dokumentation sitt arbetssätt för tilldelning av behörighet, uppföljning av behörighet samt överväga behovet av dokumentation för uppföljning av användningen genom logg-/åtkomstkontroller.

Iakttagelser från kontrollen

Förvaltningen har uppgett att 271 personer har behörighet i systemet varav sju personer har hög administratörsbehörighet. Antalet registrerade vars personuppgifter behandlas i systemet uppskattas vara mellan 100 000 och 400 000.

Behörighetsstruktur och roller i system

Utifrån den beskrivning som förvaltningen har gett uppfattar dataskyddsombudet det som att behörigheterna kan anpassats utifrån olika roller och arbetsuppgifter som man kan ha inom förvaltningen. Systemet är uppbyggt kring behörighetsgrupperna ”grundbehörigheter” samt ”tilläggsbehörigheter”. Användare tilldelas en grundbehörighet och sedan kan tilläggsbehörigheter läggas till. Dataskyddsombudet ser det som positivt att strukturen för behörighetstilldelning är uppbyggd kring grundbehörighet och tilläggsbehörigheter, eftersom strukturen verkar möjliggöra en mer individuellt anpassad tilldelning av behörigheter.

Tilldelning av behörighet utifrån bedömning

Behörigheterna är kopplade till förvaltningens organisatoriska struktur. Handläggare får grundbehörighet utifrån var de jobbar och tilläggsbehörigheter baseras på om specifika handläggare har behov av att kunna utföra vissa arbetsuppgifter utöver vad den grundläggande behörigheten ger tillgång till.

Dataskyddsombudet ser det som positivt att förvaltningen har en tanke kring hur man ska bedöma tilldelningen av behörigheter, nämligen att tilldelningen ska ske utifrån organisatorisk tillhörighet och utifrån behovet av att kunna utföra sina arbetsuppgifter. Dataskyddsombudet rekommenderar förvaltningen att överväga behovet av att se över och dokumentera sitt arbetssätt för tilldelning av behörigheter. Dokumentationen blir ett led i att uppfylla ansvarsskyldigheten enligt artikel 5.2 i dataskyddsförordningen, eller med andra ord ett sätt för er att visa att ni följer reglerna kring personuppgiftsbehandling.

Beslut om behörighet

Förvaltningen har uppgett att det är den anställdes chef (informationsägaren) som bestämmer vilken behörighet den anställde ska ha i EDP Vision. Om chefen bestämmer att den anställde ska ha tillgång till Vision tilldelas behörighet utifrån organisatorisk tillhörighet och roll. Dataskyddsombudet har inget att invända mot denna ordning. Att det är chefen som beslutar om behörigheter kan lämpligen framgå ur dokumentationen kring arbetssätt för tilldelning av behörigheter (se rekommendationen i stycket ovan).

Uppföljning av behörighet

Förvaltningen har uppgett att befintliga behörigheter justeras i samband med att medarbetare får nya arbetsuppgifter eller byter avdelning/enhet. Det sker under förutsättning att IT-funktionen meddelas ändringen. I samband med att en medarbetare slutar tas behörigheterna bort. Det är IT-funktionen som sköter det praktiska med att tilldela och ta bort behörigheterna i EDP Vision genom att lägga till eller ta bort användarna ur tillgängliga behörighetsgrupper. IT-funktionen går även regelbundet igenom och rensar felaktiga behörigheter som ligger kvar. Uppbyggnad av behörighetsgrupperna i sig hanteras av en utpekad person på avdelningen för ärende- och informationshantering.

Förvaltningen har uppgett att inga medarbetare hos personuppgiftsbiträdet Intraservice är upplagda som användare i systemet och att de därför inte har någon behörighet som omfattar hantering av personuppgifter. Utifrån de svar som lämnats av förvaltningen uppfattar dataskyddsombudet det som att förvaltningen inte har lämnat några särskilda instruktioner till personuppgiftsbiträdet. Förvaltningen hänvisar istället till den generella överenskommelsen gällande kommungemensamma system. Dataskyddsombudet vill påminna förvaltningen om att även om Intraservices anställda inte har tilldelats behörigheter i systemet så har Intraservice uppenbarligen i egenskap av personuppgiftsbiträde någon slags del i personuppgiftsbehandlingen. Mot bakgrund av att detta är det därför viktigt att förvaltningen ger dokumenterade instruktioner till personuppgiftsbiträdet (se 28.3 a dataskyddsförordningen).

Förvaltningen har uppgett att systemleverantören EDP Consult AB:s har åtkomst till systemet och att förvaltningen regelbundet kontrollerar att de som tilldelats behörighet fortsatt har en roll och ska behålla sin åtkomst till systemet.

Dataskyddsombudet rekommenderar att förvaltningen överväger behovet av att se över och dokumentera sitt arbetssätt för uppföljning av tilldelade behörigheter.

Åtkomstkontroll/kontroll av loggar

Förvaltningen har uppgett att systemet har olika loggningsfunktioner. Utöver en ren teknisk loggning så finns ”GDPR-loggning”, loggning av sekretessändringar samt loggning av

historik vid ändringar i systemet. GDPR-loggningen visar om någon har tittat på eller sökt på poster som innehåller personuppgifter. För att kunna granska dessa loggar krävs en priviligierad åtkomst och användning av tredjepartsprogramvara. Vad gäller loggning av ändringar i sekretessmarkeringar så är detta något som är tillgänglig direkt i ärendebilden för behöriga handläggare. Specialbehörigheter för att se alla sekretessmarkerade handlingar ges till registratorer och vissa chefer. Loggning av historik och förändring av poster kan ses av behörig handläggare till posten. Förvaltningen har uppgett att det inte sker någon systematisk och regelbunden genomgång av loggar.

Dataskyddsombudet rekommenderar att förvaltningen överväger behovet av att införa åtkomstkontroll/logguppföljning i form av regelbundna slumpmässiga stickprovskontroller. Dataskyddsombudet vill understryka att nyttan med loggkontroller inte endast är att man kan kontrollera riktighet/korrekthet av registrerade uppgifter, men att loggkontrollerna också kan fylla en viktig funktion vad gäller kontroll av åtkomst i systemet och säkerställandet av konfidentialitet. Dataskyddsombudet vill påminna om vikten av att det finns tydliga rutiner för logguppföljning och att berörda medarbetare informeras om gällande strukturer. Kontrollerna bör inte inskränka medarbetarnas integritet på ett oproportionerligt sätt.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

Förvaltningen har angett att offentlighets- och sekretesslagen (2009:400) (OSL) är relevant för behörighetstilldelningen. Förvaltningen har inte uppgett vilka lagrum som blir tillämpbara, men har förklarat att åtkomsten till sekretessmarkerade uppgifter begränsas.

Dataskyddsombudet ser det som positivt att det finns begränsningar vad gäller åtkomst till sekretessmarkerade uppgifter. I 10 kapitlet OSL finns regler kring sekretess för miljöinformation och geografisk miljöinformation. Som bekant finns även sekretessbestämmelser i OSL som gäller till skydd för fysiska personers personliga förhållanden, skyddade personuppgifter, hälsa m.m. och för den här typen av uppgifter (som också är personuppgifter) gäller även dataskyddsförordningen. Eftersom det finns olika typ av sekretess kan det därför vara relevant att särskilja mellan sekretess som gäller för fysiska personer och sekretess som gäller för annan typ av information (information som inte har med fysiska personer att göra). Eftersom sekretessfrågor inte sällan överlappar dataskyddsrelaterade frågor rekommenderar dataskyddsombudet att förvaltningen överväger behovet av att följa upp sekretessreglernas påverkan på frågan om behörighetsstyrning med en förvaltningsjurist.

Andra åtgärder

Förvaltningen har uppgett att de arbetar löpande för att förhindra oriktig hantering (inklusive obehörig åtkomst) av personuppgifter, bland annat genom:

- Introduktion av nya medarbetare i systemet och i regelverk som berör GDPR och informationssäkerhet.
- Utbildningsinsatser riktade till chefer och medarbetare. Löpande dialog med lokala systemansvariga i verksamheten kring frågor som rör GDPR och systemets användning.
- Rutiner och manualer för hantering av personuppgifter.

- Förvaltningen har begränsat antalet personer som är systemadministratörer med möjlighet att lägga upp nya användare i systemet.
- Rutiner för hur och när man skapar nya användare till systemet inklusive autentiseringskontroll (ID-kontroll). Förvaltningen arbetar aktivt med systemkonfiguration för att minimera onödig hantering av personuppgifter, t.ex. genom att låsa eller dölja fritextfält i systemet och styra vilka sorters uppgifter som kan registreras i vilka fält.

Förvaltningen har uppgett att man ligger efter i arbetet med konsekvensbedömningar och att någon konsekvensbedömning därmed inte har gjorts för behandlingarna i systemet. Förvaltningen har underrättat dataskyddsombudet om detta sedan tidigare. Dataskyddsombudet rekommenderar förvaltningen att följa upp och undersöka behovet av att genomföra konsekvensbedömningar.

Förvaltningen har uppgett att man har genomfört en kartläggning och riskanalys kopplat till hanteringen av behörigheter avseende informationssäkerhet. Dataskyddsombudet noterar utifrån underlaget som förvaltningen skickat in att det är oklart huruvida kartläggningen och riskanalysen också omfattar hanteringen av personuppgifter. Dataskyddsombudet rekommenderar därför förvaltningen att ser över om kartläggningen och riskanalysen omfattar personuppgiftsbehandling

Sammanfattade rekommendationer

- Förvaltningen rekommenderas att se över och dokumentera sitt arbetssätt för tilldelning av behörigheter.
- Förvaltningen rekommenderas att se över och dokumentera sitt arbetssätt för uppföljning av tilldelade behörigheter.
- Förvaltningen rekommenderas att införa åtkomstkontroll/loggуppföljning i form av regelbundna slumpmässiga stickprovskontroller.
- Förvaltningen rekommenderas att utreda och följa upp sekretessfrågor, kopplat till behörighetsstyrning, tillsammans med förvaltningsjurist.
- Förvaltningen rekommenderas att utreda behovet av att genomföra konsekvensbedömningar av behandlingarna i systemet, alternativt dokumentera varför sådana inte anses vara nödvändiga.

Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022 Behörighetsstyrning (del 1)
3. Fördjupad kontroll 2022 Behörighetsstyrning (del 2)

Bilaga 1

Information om fördjupad kontroll

Kontrollpunkt 11: Behörighetsstyrning

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

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

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

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

Tillvägagångssätt

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

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

Rosenlundsgatan 4 dso@intraservice.goteborg.se
403 31 Göteborg 031-365 00 00 (kontaktcenter) goteborg.se

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

Bilaga 2

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 1)

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

o Beskriv systemets behörighetsstruktur och olika roller i systemet.

o Vilka roller får vilka behörigheter och vad baseras den bedömningen på?

o Vem beslutar om vilka som ska ha vilken behörighet?

o Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?

o Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.

o När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?

o Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?

o Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka? o Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?

o Har verksamheten identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet. Underlaget ska ha inkommit till dataskyddsombudet senast den 10 mars 2022. Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Bilaga 3

Fördjupad kontroll 2022

Kontrollpunkt 11 Behörighetsstyrning (del 2)

1. Hur många personer har behörighet i systemet?

2. Hur många har behörigheten ”Administratör Hög”?

3. Hur kontrolleras personuppgiftsbiträdets behörigheter i systemet?

4. Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?

5. Hur många registrerades personuppgifter hanteras i systemet?

6. Har ni konsekvensbedömt behandlingarna i systemet?

7. Har ni identifierat specifika risker kopplat till den nuvarande hanteringen av behörigheter? Varför/varför inte? Beakta såväl risker som uppkommer inifrån den egna organisationen som utanför (exempelvis intrång) för de registrerades rättigheter.

8. På vilket sätt är offentlighets- och sekretesslagen relevant i behörighetsstyrningen?