Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Äldre samt vård- och omsorgsförvaltningen

2022-12-23

Innehåll

1 Dataskydd i kommunal verksamhet

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

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

1.1 Göteborgs Stads dataskyddsombud

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

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

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

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

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 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

Under 2022 har dataskyddsombudet genomfört en fördjupad kontroll där delar av verksamhetens arbete med behörighetsstyrning i IT-systemet Treserva har granskats. Syftet med kontrollen är att granska om dataskyddsombudet ser risker i verksamhetens arbete med behörighetsstyrning utifrån kraven i artikel 32 i GDPR. Kontrollen har avgränsats till att endast omfatta tilldelning och kontroll av behörigheter för chefer och medarbetare vid avdelning Myndighet Hisingen och Sydväst.

Dataskyddsombudet har lämnat följande rekommendationer till förvaltningen:

- Se över och dokumentera ert arbetssätt för tilldelning av behörigheter.
- Se över ert arbetssätt för uppföljning av tilldelade behörigheter.

- Fortsätt arbetet med att ta fram en rutin för loggranskning och gör dessa rutiner kända bland medarbetarna.
- Ge personuppgiftsbiträdet Intraservice dokumenterade instruktioner.
- Ta arbetet vidare med ny profil för avvikelsehantering och motverka kvarstående risker.
- Se över utformningen av de behörigheter som tilldelas medarbetare i Treserva, med hänsyn till risker för klienters integritet.
- Gör en bedömning av om aktuella personuppgiftsbehandlingar behöver konsekvensbedömmas.

Den fördjupade kontrollen kan läsas i sin helhet i bilaga 2.

2.2.2 Uppföljning av tidigare genomförda kontroller

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

Kontroll (2021):

Verksamheten gavs följande rekommendationer:

Att se över sin dataskyddsorganisation och övergripande strategi för dataskydd genom att:

- Säkerställa att dataskyddsarbetet integreras i det övergripande informationssäkerhetsarbetet.
- Säkerställa och bevaka att de personer som involveras i dataskyddsarbetet, särskilt de som har ålagts det operativa arbetet, har tillräckligt med tid och förutsättningar.
- Inkludera eller komplettera med en metod för att identifiera och bedöma risker utifrån de registrerades rättigheter och vad identifierade risker skulle medföra för eventuella konsekvenser för organisationen, såsom ekonomisk skada eller förlust av förtroende.

Kommentarer:

Uppföljningen visar att verksamheten har vidtagit vissa åtgärder gällande de organisatoriska förutsättningarna för dataskyddsarbetet. Fortsatt uppföljning från dataskyddsombudets sida kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat. Dataskyddsombudets rekommendationer i frågan framgår ur kontrollpunkt 1 (se längre ner vid 2.4.1).

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in

en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

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

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Äldre samt vård- och omsorgsförvaltningens 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

X

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.

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens egen skattning av sin dataskyddsorganisation ligger den kvar på ungefär samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Likt föregående år uttrycker förvaltningen att organisationen behöver mer resurser för att ha förutsättningar att utföra ett fullgott dataskyddsarbete. Dataskyddsorganisationen var föremål för den fördjupade kontrollen under våren 2021.

Förvaltningen har under hösten 2022 anställt en ny dataskyddskontakt som har tagit över efter den tidigare dataskyddskontakten. Rekrytering av en ytterligare resurs till dataskyddsorganisationen är på gång. Dataskyddsombudet vill uppmuntra den nya dataskyddskontakten i det fortsatta arbetet med att bygga upp och stärka förvaltningens dataskyddsorganisation. Positivt är att det verkar finnas flera personer i olika roller inom förvaltningen som redan har viss kompetens och medvetenhet kring dataskyddsrelaterade frågor. En möjlig utvecklingspotential är därför att få fler personer involverade i förvaltningens interna dataskyddsorganisation. För att en nivåhöjning ska vara möjligt är det också viktigt att dataskyddsorganisationen ges stöd och tilldelas tillräckliga resurser från ledningen.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av arbetet med personuppgiftsincidenter ligger det kvar på ungefär samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Mot bakgrund av att förvaltningen är så pass stor och har så pass omfattande och känslig personuppgiftsbehandling är det relativt sett få personuppgiftsincidenter som dataskyddsombudet fått kännedom om under året. Detta kan ställas i relation till andra förvaltningar som har en jämförelsevis ”starkare” dataskyddsorganisation och som rapporterar fler incidenter per år. Möjligen indikerar detta att förvaltningen behöver bli bättre på att identifiera personuppgiftsincidenter. Utifrån förvaltningens svar rekommenderar dataskyddsombudet att förvaltningen ser över de aktuella rutinerna för personuppgiftsincidenter. Detta med särskilt fokus på att klargöra hanteringen kring när information ska ges till registrerade samt frågan om uppföljning av inträffade incidenter. Dataskyddsombudet uppmuntrar förvaltningen att höja medvetenheten kring frågan i den interna organisationen genom

utbildnings- och informationsinsatser. Förvaltningen har som tidigare nämnts uppgett att man har en nyrekrytering på gång. Dataskyddskontakten har uppgett att denna resurs initialt kommer att arbeta fokuserat med att just skickliggöra organisationen på området personuppgiftsincidenter. Mot bakgrund av detta ser dataskyddsombudet att det finns goda förutsättningar för förvaltningen att göra framsteg på den här punkten framöver.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamheten

s 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:

Enligt förvaltningens skattning av arbetet med biträdesavtal och andra överenskommelser ligger det kvar på ungefär samma nivå som vid förra årets enkät. Dataskyddsombudet har inget att invända mot denna bedömning. Resultatet indikerar att det finns risker som bedöms vara omfattande och/eller som omgående kräver åtgärder.

Eftersom förvaltningen har skattat sig lågt vad gäller rutiner för kontinuerlig kontroll av efterlevnad hos personuppgiftsbiträden och vad gäller rutiner kring uppföljning av underbiträden, rekommenderar dataskyddsombudet att förvaltningen framöver prioriterar arbete med dessa frågor. I enkätsvaret har förvaltningen uppgett att personuppgiftsavtal finns upprättade till 50 %. Förvaltningen har dock förklarat muntligen att det förmodligen finns fler personuppgiftsavtal upprättade, men att det finns brister i diarieföringen. Med andra ord verkar utmaningen vara att man inte har överblick på alla personuppgiftsavtal. Dataskyddsombudet rekommenderar förvaltningen att fortsätta arbetet med att skapa överblick på existerande personuppgiftsbiträdesrelationer och att säkerställa att personuppgiftsbiträdesavtal finns på plats.

Vidare indikerar svaren från förvaltningen att förvaltningen behöver arbeta med frågan kring delat och gemensamt personuppgiftsansvar. Förvaltningen har berättat att utmaningarna delvis kan ha sin grund i att det ibland finns lite ”udda” samarbeten (t.ex. när ÄVO levererad mat till skolor) där man kanske inte intuitivt vet hur man ska hantera dem. I andra fall, uttrycker förvaltningen, kan utmaningen ligga i att en samarbetspartner kanske inte går in och tar fullt ansvar och det kan

finnas information som bara samarbetspartnern har tillgång till. Utmaningar vad gäller delat och gemensamt personuppgiftsansvar finns både internt inom staden, och externt exempelvis i relation till Västra Götalandsregionen.

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:

Enligt förvaltningens skattning av arbetet med personuppgiftsregister ligger det kvar på samma nivå som vid förra årets enkät. Dataskyddsombudet har inget att invända mot denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet rekommenderar förvaltningen att prioritera arbetet med att göra personuppgiftsregistret mer komplett i enlighet med reglerna i artikel 30 i GDPR. Förutom att det är fråga om lagefterlevnad så vill dataskyddsombudet poängtera att den praktiska nyttan med ett utförligt personuppgiftsregister är att det är ett användbart hjälpmedel i dataskyddsarbetet och att förvaltningen med hjälp av registret kommer att få bättre koll på sina personuppgiftsbehandlingar.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av förvaltningens övergripande strategi för dataskydd ligger den kvar på ungefär samma nivå som vid förra årets enkät (aningen högre skattning i år jämfört med förra året). Dataskyddsombudet har inget att invända mot denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Strategi för dataskydd är en fråga som hänger samman med dataskyddsorganisationen och som tidigare nämnts var dataskyddsorganisationen och den övergripande strategin föremål för den fördjupade kontrollen under våren 2021.

Dataskyddskontakten har muntligen förklarat att man i dagsläget inte genomför intern kontroll av efterlevnad av GDPR. Den långsiktiga planen och strategin är istället att först fokusera på att bygga upp kompetensen i organisationen. Dataskyddskontakten har uppgett att man upplever att det finns en god vilja och medvetenhet kring dataskyddslagstiftningen i organisationen och att dataskyddsrelaterade frågor löpande lyfts av medarbetare. Dataskyddsombudet förstår att det kan behövas en viss mognad innan man inför intern kontroll. Förvaltningen uppmanas därför att på lite längre sikt återkomma till frågan om intern kontroll av följsamhet gentemot GDPR.

Utifrån förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen ser över rutinerna för efterlevnad av GDPR i samband med fysiska och digitala sammankomster.

Förvaltningen har berättat muntligen att man har påbörjat ett projekt för att inventera informationstillgångar. Inventeringen görs avdelningsvis eftersom man anser att detta är mest ändamålsenligt. Dataskyddsombudet ser positivt på att man arbetar med frågan och att man har en strategi kring hur inventeringsarbetet ska gå till. Dataskyddsombudet uppmuntrar förvaltningen att jobba vidare med detta och att prioritera detta arbete.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av arbetet med utbildning kring dataskyddsfrågor ligger det kvar på samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver förvaltningens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Förvaltningen behöver därför även fortsättningsvis ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd. Den lokala dataskyddsorganisationen bör också ges rätt förutsättningar för att kunna genomföra informationsinsatser. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser behöver förvaltningen kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

Förvaltningen har muntligen berättat att man har idéer kring diverse utbildnings- och informationsinsatser. Som en del av detta arbete försöker man exempelvis bli tidigare involverad i olika inköps- och upphandlingsprocesser. Vidare har

förvaltningen uppgett att man försöker samordna utbildnings- och informationsinsatser med arkivarie och IT. Dataskyddsombudet ser det som positivt att förvaltningen samordnar och försöker få ett helhetsgrepp kring olika frågor där dataskyddsperspektivet kommer in som ett av flera perspektiv.

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:

Enligt förvaltningens skattning av förvaltningens integritetspolicy ligger den kvar på samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Integritetspolicyn är en del av det kontinuerliga dataskyddsarbetet. Informationen som presenteras på den externa hemsidan med rubriken *Så behandlar äldre samt vård- och omsorgsförvaltningen personuppgifter*[4] uppfyller delvis innehållskraven enligt artikel 13-14 i GDPR, men det finns förbättringar att göra. Förvaltningen rekommenderas därför att se över integritetspolicyn både utifrån innehåll, utifrån hur innehållet presenteras och utifrån vilken specifik information som ges i samband med olika behandlingar.

Möjligen kan det i informationstexten på hemsidan preciseras exempel på konkreta mottagare av uppgifter, samt läggas till information om automatiserat beslutsfattande (om det är aktuellt och relevant).

Vidare rekommenderar dataskyddsombudet förvaltningen att särskilt se över informationen om sociala medier och tredjelandsöverföringar så att den svarar mot kraven enligt artikel 13.1.f respektive 14.1.f. Frågan om användning av sociala medier bör även i grunden ses över. I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även Instagram och Youtube är exempel på sociala medier som överför personuppgifter till USA. Ingen av dessa plattformar har angett att de vidtagit några extra skyddsåtgärder och utifrån det saknar alla överföringar som görs inom dessa tjänster laglig grund. Dataskyddsenheten avråder därför

[4] Äldre samt vård- och omsorgsförvaltningen. Så behandlar äldre samt vård- och omsorgsförvaltningen personuppgifter. Tillgänglig: Så behandlar äldre samt vård- och omsorgsförvaltningen personuppgifter - Göteborgs Stad (goteborg.se). (Hämtad 2022-11-22).

förvaltningen från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

Förvaltningen behöver kontinuerligt säkerställa att integritetspolicyn hålls aktuell i de olika kanalerna som förvaltningen använder sig av och att rutinerna kopplat till integritetspolicyn följs.

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 GDPR. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av sitt arbete med e-post och dokumenthantering ligger det kvar på ungefär samma nivå som vid förra årets enkät. Eftersom förvaltningen har svarat väldigt lågt på sex av åtta frågor (förvaltningen har uppgett siffran ett eller två) är dataskyddsombudets sammantagna bedömning att detta är ett område som behöver prioriteras. Resultatet indikerar att det finns risker och att flera av dessa risker är brådskande, omfattande eller allvarliga.

Dataskyddsombudet rekommenderar att förvaltningen prioriterar att få på plats en dokumenthanteringsplan samt rutiner för gallring och att förvaltningen vidtar åtgärder för att få innehållet i dessa dokument kända bland medarbetarna. Vidare rekommenderar dataskyddsombudet att förvaltningen ser över rutinerna för e-posthantering och innehållet i e-postsignatur. Förvaltningen behöver även se över verksamhetens arbete med informationsklassificering av personuppgiftsbehandlingar och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet.

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:

Enligt förvaltningens skattning av sitt arbete med konsekvensbedömningar ligger det kvar på ungefär samma nivå som vid förra årets enkät. Eftersom förvaltningen har svarat väldigt lågt på nio av tretton frågor (förvaltningen har uppgett siffran ett eller två) är dataskyddsombudets sammantagna bedömning att detta är ett område

som behöver prioriteras. Resultatet indikerar att det finns risker och att flera av dessa risker är brådskande, omfattande eller allvarliga.

Förvaltningen har uppgett att man har en stor ”skuld” vad gäller antalet genomförda konsekvensbedömningar. Man har för avsikt att genomföra konsekvensbedömningar med utgångspunkt i olika processer (t.ex. utifrån processen att rekrytera personal) istället för att exempelvis ta avstamp i olika system. Genom detta arbetssätt hoppas man att arbetet med att ”beta av” skulden ska bli görbart. Dataskyddsombudet ser det som positivt att förvaltningen har en plan och strategi för hur arbetet med konsekvensbedömningar ska drivas framåt.

Förvaltningen rekommenderas att utreda och ta ställning till när det kan anses vara lämpligt att inhämta de registrerades synpunkter. Vägledning finns bl.a. att hämta hos Integritetsskyddsmyndigheten samt EDPB:s vägledning för konsekvensbedömning.

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:

Enligt förvaltningens skattning av sitt dataskyddsarbete i IT-projekt och upphandling ligger det kvar på ungefär samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer delvis i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet har förstått att det finns en del projekt kring välfärdsteknik och bistår gärna i arbetet med att se över dessa projekt utifrån de registrerades fri- och rättigheter.

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 GDPR. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av sitt dataskyddsarbete vad gäller IT-system och digitala verktyg ligger det kvar på ungefär samma nivå som vid förra årets enkät. Eftersom förvaltningen har svarat väldigt lågt på nio av tretton frågor (förvaltningen har uppgett siffran ett eller två) är dataskyddsombudets sammantagna bedömning att detta är ett område som behöver prioriteras. Resultatet indikerar att det finns risker och att flera av dessa risker är brådskande, omfattande eller allvarliga.

Som tidigare nämnts har förvaltningen ett pågående arbete kring inventering av informationstillgångar och detta är bra. Dataskyddsombudet vill åter igen påminna om rekommendationen att prioritera detta arbete.

Dataskyddsombudet ser även att det finns behov av att utreda vissa frågor kopplat till behörighetsstyrning, vilket var föremål för den fördjupade kontrollen under våren 2022 (för mer detaljer se den fördjupade kontrollen i Bilaga 2).

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:

Enligt förvaltningens skattning av hanteringen av de registrerades rättigheter ligger den kvar på ungefär samma nivå som vid förra årets enkät. Dataskyddsombudet instämmer i denna bedömning. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet ser det som positivt att välfärdsförvaltningarna arbetar med att ta fram gemensamma rutiner och svarsmallar rörande frågor kopplat till de registrerades rättigheter. Dataskyddsombudet uppmuntrar förvaltningarna att tillvarata dataskyddsombudets lämnade synpunkter. Nästa steg blir att vidta åtgärder för att medarbetare ska få kunskap om rutinerna.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som

bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

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

- Kontrollpunkt 2 och 6 (Personuppgiftsincidenter och utbildning).
  Se över rutiner för hantering av personuppgiftsincidenter och höj medvetenhet bland medarbetare.

- Kontrollpunkt 5 och 11 (Övergripande strategi för dataskydd och IT-system och digitala verktyg).
  Genomför inventering av informationstillgångar.

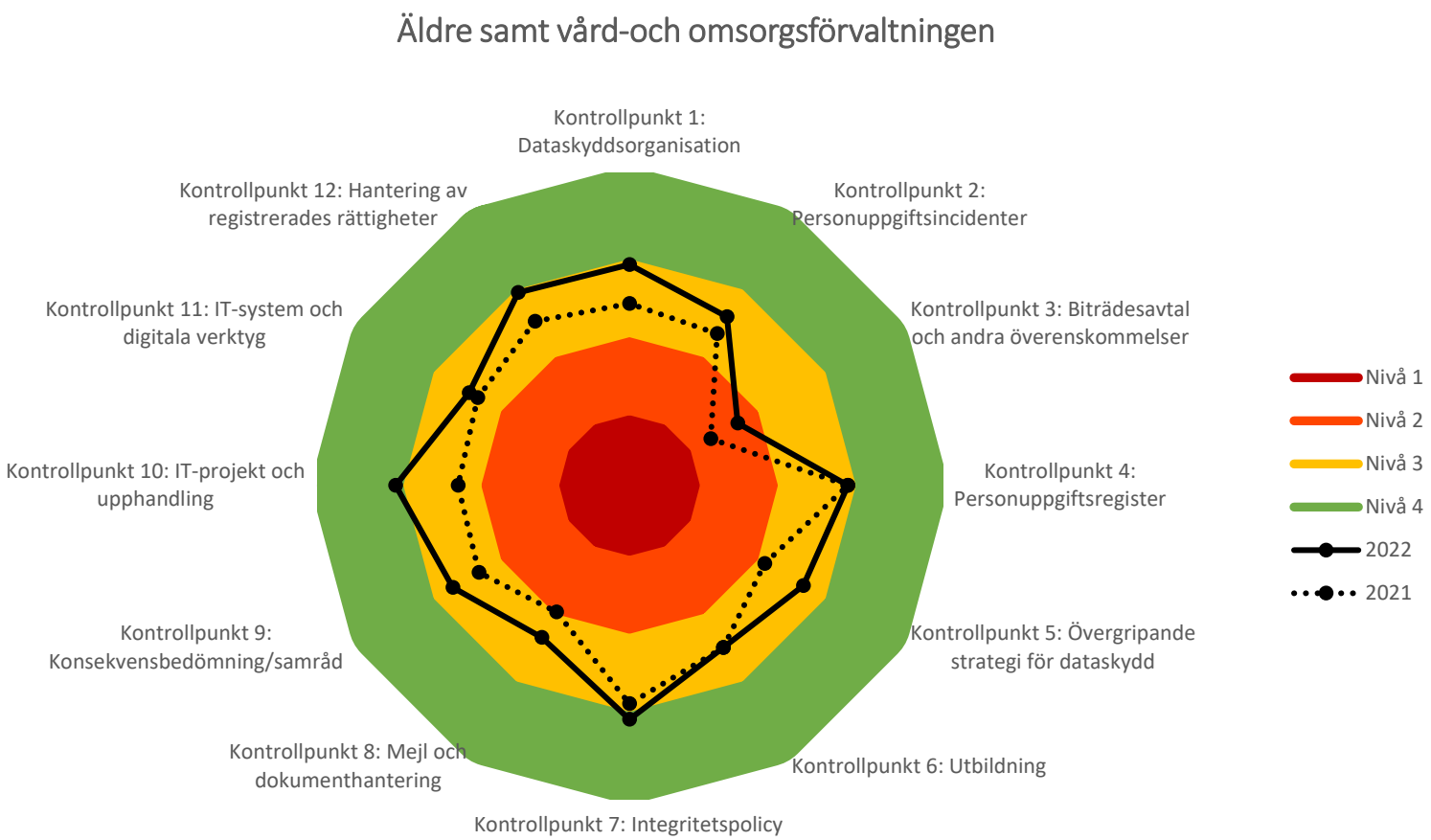
- Kontrollpunkt 8 (E-post och dokumenthantering).
  Ta fram en dokumenthanteringsplan och genomför informationsklassning av personuppgiftsbehandlingar.

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, Äldre samt vård- och omsorgsförvaltningen.

Bakgrund

Under 2022 har dataskyddsombudet genomfört en fördjupad kontroll av verksamhetens arbete med behörighetsstyrning och hur detta används för att begränsa vilka personuppgifter som medarbetare får ta del av. Kontrollen har omfattat verksamhetens rutiner för tilldelning av behörigheter i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller. Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. Kontrollen vad gäller äldre samt vård- och omsorgsförvaltningen har avgränsats till att endast omfatta tilldelning och kontroll av behörigheter i systemet Treserva för chefer och medarbetare vid avdelning Myndighet Hisingen och Sydväst.

Granskningen har gjorts med utgångspunkt i artikel 32 i dataskyddsförordningen (GDPR) som handlar om lämpliga tekniska och organisatoriska säkerhetsåtgärder vid personuppgiftsbehandling. Vid bedömningen av lämplig säkerhetsnivå ska hänsyn tas till bland annat risken för obehörig åtkomst till personuppgifter. Behörighetsstyrning är ett verktyg som verksamheterna kan använda sig av för att förhindra obehörig åtkomst till personuppgifter i ett IT-system.

En medarbetares tillgång till system med personuppgifter bör vara anpassad och begränsad utifrån vad medarbetaren behöver för att kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten dokumentera sitt arbetssätt för tilldelning av behörigheter, uppföljning av behörigheter samt för hur logg-/åtkomstkontroller används.

Iakttagelser från kontrollen

I systemet finns personuppgifter tillhörande klienter och medarbetare. Antal öppna ärenden vid ÄVO Hisingen är 5 306 varav 4 725 unika personer och vid Sydväst 5 272 varav 6 699 unika personer. Antal avslutade ärenden som är sökbara är vid ÄVO Hisingen 11 453 varav 7 279 unika personer och vid Sydväst 10 108 varav 6 648 unika. Det går inte att söka på ärenden som är avslutade och inte har varit aktuella de senaste 5 åren.

Antal personer som har åtkomst till ärenden i Treserva vid enheten på Hisingen är 71. Vid andra organisatoriska enheter har 23 administratörer, 2 socialt ansvariga samordnare (SAS), 3 ekonomer, 6 boendesamordnare, 7 lokalt verksamhetsstöd (LVS), 15 centralt verksamhetsstöd (CVS) åtkomst. Vid enheterna vid förvaltningen Sydväst har 76 personer åtkomst. Vid andra organisatoriska enheter har 21 administratörer, 3 SAS, 6 boendesamordnare, 6 LSV, 15 CVS åtkomst.

Förvaltningen har uppgett att följande personuppgifter behandlas i systemet: namn, adress, telefonnummer, personnummer, kontaktuppgift till närstående. Vidare har förvaltningen uppgett att ansökan om bistånd, social utredning kopplat till ansökan om bistånd, beslut om beviljad/avslagen insats hanteras i systemet. Utifrån beskrivningen av

ärenden är dataskyddsombudets bedömning att behandlingen sannolikt omfattar så väl särskilt skyddsvärda som känsliga personuppgifter.

Behörighetsstruktur och roller i system

Förvaltningen har uppgett att det finns tre behörighetsnivåer. Den högsta behörigheten tilldelas vissa funktioner inom LVS och ekonomistyrning och det finns specialbehörigheter för vissa ansvarsuppdrag som t.ex. hantering av personer med skyddad identitet. De två övriga behörighetsnivåerna utgörs av LVS som har behörighet att administrera användarbehörigheter samt användare. Samtliga behörigheter är kopplade till ett gruppfilter inom det stadsområde myndigheten tillhör, i detta fall Sydväst och Hisingen. För biståndshandläggare finns en roll. För enhetschefer finns en roll som enhetschef, en roll för att se avvikelser och en roll för att attestera ekonomistyrning.

Tilldelning av behörighet utifrån bedömning

Förvaltningen har uppgett att utgångspunkten är att användaren ska ges den behörighet som behövs för att den ska kunna utföra sitt arbete. Vissa rollen kräver genomgången utbildning och detta gäller exempelvis LVS-rollen.

Intraservice är den som administrerar tilldelningen av den högsta behörigheten. Lokalt verksamhetsstöd lägger till behörigheter kopplat till rollen som enhetschef, rollen för att se avvikelser, rollen för att attestera ekonomi samt rollen som biståndshandläggare.

Vad som är en ändamålsenlig behörighetstilldelning beror på flera faktorer, som hur arbetsuppgifterna ser ut, hur många personer det är som har samma arbetsuppgifter och hur socialtjänsten är organiserad.[1] Dataskyddsombudet tänker att förvaltningen, med sin verksamhetskunskap, är bäst lämpad att göra denna bedömning. Tänk på att ju bredare teknisk behörighet en anställd har i ett system desto viktigare blir det att förvaltningen klargör förhållningssätt för när det får anses tillåtet att ta del av information i systemet.[2] Det är viktigt att medarbetarna informeras om dessa förhållningssätt. Mot bakgrund av detta rekommenderas förvaltningen att se över och dokumentera sitt arbetssätt för tilldelning av behörigheter. Dokumentationen blir ett led i att uppfylla ansvarsskyldigheten enligt artikel 5.2 GDPR, eller med andra ord ett sätt för er att visa att ni följer reglerna kring personuppgiftsbehandling.

Beslut om behörighet

Förvaltningen har uppgett att som utgångspunkt beslutar den anställdes chef om behörighet för medarbetarna och i vissa fall beslutar en högre chef. Dataskyddsombudet har inget att anmärka 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 lokalt verksamhetsstöd följer upp behörigheter två gånger per år. Enhetschefer ansvarar för att kontrollera att de underlag som ligger till grund för

[1] Socialstyrelsen. 2019-2-6, Säker personuppgiftsbehandling i socialtjänsten. Rättsläge och utgångspunkter. s. 29. Tillgänglig: Säker personuppgiftsbehandling i socialtjänsten (socialstyrelsen.se). (Härefter Socialstyrelsen 2019-2-6).
[2] Socialstyrelsen. 2019-2-6, s. 29.

behörighetstilldelningen är korrekta. Förvaltningen har tagit fram en gemensam rutin för behörighetskontroll.

Dataskyddsombudet ser det som positivt att förvaltningen har tagit fram en rutin för halvårsvis uppföljning, men vill tillägga att det också kan vara lämpligt att ha ett arbetssätt som innebär att man följer upp behörigheter direkt i samband med att en person avslutar en anställning, får en ny roll inom organisationen eller har en längre frånvaro genom exempelvis tjänstledighet, föräldraledighet eller sjukskrivning. Dataskyddsombudet rekommenderar förvaltningen att se över sitt arbetssätt för uppföljning av tilldelade behörigheter.

Åtkomstkontroll/kontroll av loggar

Förvaltningen har uppgett att det finns ett utkast på rutin för loggranskning. Enligt detta utkast föreslås det att kontroller ska utföras en gång per kvartal.

Dataskyddsombudet ser det som positivt att förvaltningen arbetar med denna fråga. Logg- och åtkomstkontroller är ett praktiskt redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. 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.

Personuppgiftsbiträdet

Förvaltningen har uppgett att de inte har gett några specifika instruktioner till personuppgiftsbiträdet Intraservice gällande Treserva, men har istället hänvisat till den generella överenskommelsen gällande kommungemensamma system. Vidare har förvaltningen uppgett att man inte utför några kontroller gentemot Intraservice.

Dataskyddsombudet vill uppmärksamma förvaltningen på att ni som personuppgiftsansvarig behöver ge personuppgiftsbiträdet dokumenterade instruktioner (se artikel 28.3 a i GDPR). Förvaltningen rekommenderas därför att ge personuppgiftsbiträdet Intraservice dokumenterade instruktioner. Vidare eftersom Treserva innehåller sekretessbelagda uppgifter behöver förvaltningen se till så att Intraservice iakttar konfidentialitet och tystnadsplikt (se artikel 28.3 b i GDPR).

Andra åtgärder

Förvaltningen har uppgett att de har tagit fram en ny profil för behörighet för avvikelsehantering. Den nya profilen för avvikelsehantering uppges vara bättre än den gamla, men det kvarstår fortfarande risker. Dataskyddsombudet uppmuntrar förvaltningen att ta arbetet vidare för att motverka kvarstående risker.

Konsekvensbedömning och risker

Vad gäller tilldelning av behörighet till vikarier så har förvaltningen identifierat en risk, som man själva uttrycker det innebär att vikarier ofta får “för stora” behörigheter. Ytterligare en risk enligt förvaltningen är att samtliga användare kan söka fram namn, kontaktuppgifter, personnummer och inom vilket lagområdet personen handläggs för samtliga brukare som har pågående ärenden inom sitt stadsområde. Förvaltningen rekommenderas att se över utformningen av de behörigheter som tilldelas medarbetare i Treserva, med hänsyn till risker för klienters integritet.

Dataskyddsombudet är medveten om att det eventuellt kan finnas praktiska och tekniska utmaningar i att genomföra en ändamålsenlig behörighetsstyrning i Treserva. Dataskyddsombudet rekommenderar förvaltningen att göra vad man kan för att minska de risker som finns.

Förvaltningen har i skrivandets stund inte genomfört en konsekvensbedömning av behandlingarna i systemet. Dataskyddsombudet rekommenderar därför förvaltningen att göra en bedömning av om aktuella personuppgiftsbehandlingar behöver konsekvensbedömmas.

Sammanfattade rekommendationer

- Se över och dokumentera ert arbetssätt för tilldelning av behörigheter.
- Se över arbetssätt ert för uppföljning av tilldelade behörigheter.
- Fortsätt arbetet med att ta fram en rutin för loggranskning och gör dessa rutiner kända bland medarbetarna.
- Ge personuppgiftsbiträdet Intraservice dokumenterade instruktioner.
- Ta arbetet vidare med ny profil för avvikelsehantering och motverka kvarstående risker.
- Se över utformningen av de behörigheter som tilldelas medarbetare i Treserva, med hänsyn till risker för klienters integritet.
- Gör en bedömning av om aktuella personuppgiftsbehandlingar behöver konsekvensbedömmas.

Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022. Kontrollpunkt 11: Behörighetsstyrning (del 1)
3. Fördjupad kontroll 2022. Kontrollpunkt 11: Behörighetsstyrning (del 2)

Information om fördjupad kontroll 2022

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 IT-systemet Treserva. I del två kommer uppföljande frågor att ställas.

Kontrollen begränsas till att endast avse tilldelning av behörigheter och åtkomst till Treserva för chefer och medarbetare vid enheterna ingående i Myndighet Hisingen-Sydväst under avdelning Myndighet.

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

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.

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 Treserva.

Kontrollen begränsas till att endast avse tilldelning av behörigheter och åtkomst till Treserva för chefer och medarbetare vid enheterna ingående i Myndighet Hisingen-Sydväst under avdelning Myndighet.

- Beskriv systemets behörighetsstruktur och olika roller i systemet.
- Vilka roller får vilka behörigheter och vad baseras den bedömningen på?
- Vem beslutar om vilka som ska ha vilken behörighet?
- Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?
- Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.
- När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?
- Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?
- Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka?
- Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?
- 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.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 2)

Del 2: Utifrån vad som framkommit i del 1 av den fördjupade kontrollen ombeds ni besvara frågorna nedan.

- Vad är det för personuppgifter som behandlas i Treserva hos enheterna ingående i Myndighet Hisingen-Sydväst under avdelning Myndighet?
- Hur många registrerades personuppgifter hanteras i Treserva med anledning av ärenden som enheterna ingående i Myndighet Hisingen-Sydväst under avdelning Myndighet handlägger? Ange antalet registrerade som har öppna ärenden under maj månad 2022 samt antalet registrerade i enhetens avslutade ärenden som är sökbara i Treserva. Om det inte är möjligt att ta fram dessa uppgifter ange det i så fall (och varför).
- Ange antalet personer som har åtkomst till enheternas ärenden i Treserva. Specificera svaret så att det framgår hur många som arbetar inom enheterna ingående i Myndighet Hisingen-Sydväst under avdelning Myndighet och hur många som tillhör andra organisatoriska enheter/avdelningar inom förvaltningen eller hos personuppgiftsbiträdet.
- Föreligger det inbyggda svårigheter i aktuellt systemstöd att begränsa behörigheterna på så vis att personer enbart kan se sådana uppgifter som härrör till den egna förvaltningen? Varför/varför inte?
- Hur kontrolleras personuppgiftsbiträdets, i detta fall Intraservices, behörigheter i systemet?
- Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
- Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
- Har ni identifierat specifika risker kopplat till nuvarande hantering av behörigheter? Varför/varför inte? Beakta såväl risker inifrån organisationen som utanför (ex, intrång) för de registrerades rättigheter.

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 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.