Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Förvaltningen för funktionsstöd

2022-12-30

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 dataskyddsförordningen. Kontrollen har avgränsats till att endast omfatta tilldelning och kontroll av behörigheter för chefer och medarbetare vid enheterna tillhörande Myndighet Hisingen/Centrum under avdelningen Myndighet och socialpsykiatri.

Dataskyddsombudet har i rapporten lämnat följande sammanfattande rekommendationer:

- Förvaltningen rekommenderas säkerställa att uppföljning av tilldelade behörigheter i Treserva genomförs i enlighet med beslutade rutiner.
- Förvaltningen rekommenderas att minimera risken för felaktiga behörigheter vid personalförändringar och att detta sker i direkt anslutning till att en medarbetare exempelvis byter tjänst.
- Förvaltningen rekommenderas att fortsätta arbetet med att ta fram rutiner för åtkomstkontroll/loggуppföljning. Berörda medarbetare måste sedan informeras om gällande rutiner.
- Förvaltningen rekommenderas att ge personuppgiftsbiträdet dokumenterade instruktioner.
- Förvaltningen rekommenderas att se över behovet av konsekvensbedömning för behandlingarna i systemet, eftersom det då kan identifieras risker med för vida behörigheter.

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.	

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

2.4 Förvaltningen för funktionsstöds 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:

Verksamheten har skattat höga värden på flera av påståendena under denna kontrollpunkt. Sammantaget genererar svaren ett högt resultat som innebär att inga direkta risker av betydelse har identifierats och indikerar att verksamheten har organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt och systematiskt dataskyddsarbete.

Verksamheten anger att det stämmer bra att det finns en intern organisation för dataskyddsarbetet, där roller och ansvar är tydligt definierade. De anser vidare att det stämmer bra att det finns särskilda befattningar med utpekat ansvar, att det finns möjlighet att rapportera om dataskyddsarbetet till högsta förvaltningsnivå och att de har regelbunden kontakt med dataskyddsombudet. Däremot behöver dataskydd bli mer en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten, vilket det inte är idag. Det anges även att den interna dataskyddsorganisationen inte har tillräckliga resurser för att kunna bedriva ett systematisk dataskyddsarbete.

Dataskyddsombudet anser att verksamheten har goda förutsättningar att kunna bedriva ett effektivt och välfungerande dataskyddsarbete. Det finns en kompetent och engagerad intern dataskyddsorganisation som lyfter många och viktiga dataskyddsfrågor med dataskyddsombudet. Det är därför viktigt att verksamheten fortsätter stödja och prioritera det interna dataskyddsarbetet och att möjligheter ges för att förbättra arbetet ytterligare, bland annat genom att säkerställa tillräckliga resurser för att bedriva arbetet. Verksamheten behöver även arbeta för att dataskydd blir en naturlig och integrerad del i verksamhetens dagliga arbete.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Verksamheten har skattat sig högt på denna kontrollpunkt. Sammantaget genererar svaren ett högt resultat som innebär att inga direkta risker av betydelse har identifierats och indikerar att det bedrivs ett bra arbete med att identifiera och hantera inträffade personuppgiftsincidenter.

Verksamheten anger att de har rutiner på plats för att hantera personuppgiftsincidenter och att dessa regelbundet ses över och utvärderas. Vidare uppger verksamheten att de systematiskt följer upp inträffade personuppgiftsincidenter som en naturlig del i dataskyddsarbetet. Medarbetare informeras om vad personuppgiftsincidenter är och rutinerna för hanteringen av dessa. Dataskyddsombudets uppfattning är att det bedrivs ett bra arbete med att identifiera och hantera inträffade personuppgiftsincidenter. Verksamheten kontaktar vid behov dataskyddsombudet när personuppgiftsincidenter har inträffat, för att stämma av den fortsatta handläggningen.

Verksamheten anger att de inte har tillräckliga rutiner för när och hur information till registrerade ska tillhandahållas, samt vilken information som ska lämnas. Dataskyddsombudet rekommenderar därför verksamheten att ta fram rutiner för bedömningen av hög risk och information till registrerade. Dataskyddsorganisationen bör dessutom ges möjlighet att kontinuerligt se över och förbättra verksamhetens rutiner för hanteringen av personuppgiftsincidenter för att bland annat säkerställa att samtliga anmälningar till Integritetsskyddsmyndigheten sker i rätt tid.

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:

Resultatet av verksamhetens skattning av dataskyddsarbetet med biträdesavtal och andra överenskommelser genererar sammantaget ett resultat som indikerar att det

finns risker identifierade, men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Att reda ut rollerna inom dataskydd är en av de svårare men också en av de absolut viktigaste utmaningarna i dataskyddsarbetet. En personuppgiftsansvarig behöver säkerställa att samtliga personuppgiftsbiträden har identifierats och att nödvändiga avtal har tecknats.

Verksamheten anger att det finns rutiner för bedömningen om en ny leverantör är ansvarig eller biträde och för tecknandet av biträdesavtal. Det finns tecknade personuppgiftsbiträdesavtal för uppskattningsvis 75 % av verksamhetens anlitade personuppgiftsbiträden. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda arbete som bedrivits med att kartlägga personuppgiftsbiträden och upprätta personuppgiftsbiträdesavtal i de fall det saknas.

Verksamheten uppger emellertid att det inte finns tillräckliga rutiner för att kontinuerligt genomföra efterlevnadskontroller och för att bedöma hela kedjan av underbiträden vid anlitandet av nya personuppgiftsbiträden. Dataskyddsombudet rekommenderar verksamheten att arbeta vidare med dessa frågor och ta fram nödvändiga rutiner. En rutin för dokumenteringen av hela kedjan av underbiträden behövs exempelvis för att få en bättre överblick och på så vis kunna se om det finns risker för tredjelandsöverföring eller liknande.

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:

Resultatet av verksamhetens skattning av efterlevnaden av skyldigheten att ha ett personuppgiftsregister genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten uppskattar att upp till 75 % av behandlingarna är dokumenterade i personuppgiftsregister. De bedömer att ungefär 75 % av dessa innehåller all obligatorisk information som krävs enligt artikel 30 i GDPR. Verksamheten har berättat att det kommer att ske ett övergripande arbete under 2023 med att kartlägga alla processer och behandlingar inom förvaltningen. Dataskyddsombudet rekommenderar därför verksamheten att som ett led i detta arbete uppdatera registret med samtliga behandlingar och tillföra den information som krävs enligt GDPR i de fall uppgifter saknas.

Verksamheten anger att det inte finns tillräckliga rutiner avseende regelbundna uppdateringar av registret. Dataskyddsombudet rekommenderar därför verksamheten att säkerställa att det finns ansvariga för att uppdatera registret och att det uppdateras när en behandling tillkommit eller förändras. Ett aktuellt och uppdaterat personuppgiftsregister kan vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete. Verksamheten behöver därför även fundera över på vilket sätt personuppgiftsregistret kan användas som del i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av den övergripande strategin för arbetet med dataskydd genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Verksamheten anger under denna punkt att det finns en övergripande strategi för arbetet med dataskydd och att arbetet sker systematiskt med att integrera dataskyddsfrågorna i informationssäkerhetsarbetet. Det finns därutöver ett riskbaserat arbetssätt i dataskyddsfrågor, regelbundna interna kontroller genomförs för att säkerställa följsamheten gentemot GDPR och det finns rutiner för att säkerställa att styrande dokument som reglerar verksamhetens personuppgiftsbehandlingar hålls uppdaterade. Verksamheten har identifierat och värderat uppskattningsvis 50 % av dess informationstillgångar i enlighet med stadens styrande dokument inom informationssäkerhet. Dataskyddsombudet rekommenderar verksamheten att fortsätta arbetet för att säkerställa att samtliga informationstillgångar värderas.

Verksamheten har sammanfattningsvis de flesta övergripande strategier på plats men bör kontinuerligt fortsätta att förbättra det strategiska arbetet med dataskydd.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Resultatet av verksamhetens skattning av utbildning inom dataskyddsområdet genererar sammantaget ett resultat som indikerar att det finns risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.

Verksamhetens svar på enkäten i denna del indikerar att medarbetarna regelbundet ges möjlighet att delta i utbildningar inom dataskydd. Trots detta saknas det en god allmän kunskapsnivå hos medarbetarna inom verksamheten som i sin tur kan skapa goda förutsättningar i dataskyddsarbetet. Det saknas även rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetare. Dataskyddsombudet rekommenderar verksamheten att kartlägga utbildningsnivån inom förvaltningen och undersöka vilka utbildningsinsatser man behöver fokusera på, samt till vilka målgrupper utbildningarna ska ges. Verksamheten rekommenderas också att ta fram och besluta om en långsiktig utbildningsplan och rutiner som gäller för alla medarbetare som behöver kunskaper i dataskydd.

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 skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av utformningen och tillhandahållandet av integritetspolicyn genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. Verksamheten anger under denna punkt att integritetspolicyn uppfyller kraven på information. Informationen är tydlig och lättillgänglig samt uppdateras vid behov. De registrerade kan på ett enkelt sätt nå verksamhetens integritetspolicy från verksamhetens samtliga digitala kanaler. Dataskyddsombudet noterar dock att verksamheten behöver säkerställa att det finns dokumenterade rutiner för att informera medarbetare om hur deras personuppgifter behandlas. Därutöver vill dataskyddsombudet påminna om att det alltid är viktigt att kontinuerligt säkerställa att policyn uppfyller kraven på information och att informationen är lättillgänglig oavsett i vilken del av verksamheten som den registrerades personuppgifter behandlas. Det behöver vara tydligt vilka enskilda behandlingar som hanteras inom verksamheten, rättslig grund för respektive behandling, samt tillämpliga lagrings- och gallringsfrister.

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:

Resultatet av verksamhetens skattning av rutiner för e-post och dokumenthantering genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Idag saknar verksamheten en dokumenthanteringsplan med gallringsbeslut. Det är av stor vikt att verksamheten säkerställer att en sådan kommer på plats för att personuppgiftsbehandlingar ska kunna ske i enlighet med bland annat principen om lagringsminimering i GDPR. En dokumenthanteringsplan behöver omfatta alla verksamhetsdelar och det ska finnas rutiner för när handlingar med personuppgifter gallras. Enligt besked till dataskyddsombudet ska en dokumenthanteringsplan antas under 2023.

Dataskyddsombudet rekommenderar dessutom verksamheten att informationsklassificera samtliga sina personuppgiftsbehandlingar och säkerställa att de klassningar som gjorts är aktuella.

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:

Resultatet av verksamhetens skattning av dataskyddsarbetet med konsekvensbedömningar genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Arbetet med konsekvensbedömningar behöver inledas i ett tidigt skede vid nya eller förändrade behandlingar och vid införanden behöver man ta höjd för att arbetet kräver tid, resurser och korrekt kompetens. Detta arbete är till stor del avhängigt den generella medvetenheten om dataskydd inom förvaltningen som helhet och dataskyddsorganisationen i stort.

Detta eftersom det behöver vara tydligt vart inom verksamheten som bedömningar av behov av konsekvensbedömningar ska göras, vilka som fattar beslut om genomförandet och sedermera också beslutar om de risker som konsekvensbedömningen belyser.

Avseende konsekvensbedömningar anger verksamheten att det finns rutiner/arbetssätt för att identifiera personuppgiftsbehandlingar med hög risk för de registrerades fri- och rättigheter och metod för att inhämta och dokumentera dataskyddsombudets synpunkter när konsekvensbedömning inte bedöms behövas genomföras. Verksamheten har därutöver rutiner för att genomföra och dokumentera konsekvensbedömningar innan behandlingen påbörjas samt för att involvera dataskyddsombudet i detta arbete. Dataskyddsombudet har under det gångna året involverats i de tröskelanalyser och konsekvensbedömningar som verksamheten genomfört. Verksamheten behöver dock se till så att det finns rutiner även för att uppdatera befintliga konsekvensbedömningar vid förändringar. Därutöver behöver de säkerställa att det finns rutiner för hur beslut om att acceptera risker i en konsekvensbedömning ska fattas och dokumenteras samt att det finns rutiner för att följa upp beslutade åtgärder.

Verksamheten anger att de för uppskattningsvis 25 % av verksamhetens personuppgiftsbehandlingar har genomfört konsekvensbedömning utifrån hög risk eller för att det krävs enligt Integritetsskyddsmyndighetens checklista. Det saknas en planering som omfattar alla de behandlingar för vilka en konsekvensbedömning krävs. Detta är i sig en risk och dataskyddsombudet rekommenderar därför att verksamheten kartlägger de personuppgiftsbehandlingar som kan innebära en hög risk för registrerades fri- och rättigheter. Därefter bör en handlingsplan tas fram för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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:

Resultatet av verksamhetens skattning av dataskyddsarbetet med IT-projekt och upphandling genererar sammantaget ett resultat som indikerar att det finns risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.

Verksamheten uppger att de har rutiner på plats för att genomföra risk/behovsanalyser för att säkerställa att nya lösningar uppfyller de grundläggande kraven i GDPR och att det dessutom finns rutiner för att involvera dataskyddsombudet från start. Dataskyddsombudet instämmer i denna bedömning.

Däremot behöver verksamheten arbeta mer systematiskt och kontinuerligt med att bedöma risker för personuppgiftsbehandlingar i såväl nya som befintliga system och tjänster.

Av enkätsvaren framgår att den interna dataskyddsorganisationen saknar kunskap om huruvida det vid upphandlingar av nya system/tjänster säkerställs via kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. Enligt uppgift från verksamheten har dock den interna dataskyddsorganisationen i något större utsträckning än tidigare involverats när förvaltningen gör nya upphandlingar. Dataskyddsombudet rekommenderar därför verksamheten att prioritera ett ökat samarbete och involvering i dessa frågor. Det är nämligen viktigt redan vid upphandlingen, av exempelvis ett IT-system, att ta hänsyn till integritetsskyddet och bygga in funktioner som stödjer detta. Det är inte enbart vid nya upphandlingar som en anpassning till inbyggt dataskydd och dataskydd som standard behöver säkerställas, utan det måste även kontrolleras vid avrop och förnyad konkurrensutsättning att detta beaktats i ramavtalet.

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:

Resultatet av verksamhetens skattning av dataskyddsrutiner för IT-system och digitala verktyg genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet rekommenderar verksamheten att kontrollera så att IT-system och digitala verktyg används på rätt sätt och att det finns rutiner för att systematiskt följa upp användningen. Eftersom IT-system och digitala verktyg är några av de främsta arbetsredskapen inom en verksamhet är det dessutom alltid betydelsefullt att säkerställa så att det finns målgruppsanpassad information om hur personuppgifter behandlas i de digitala verktyg och IT-system som används, samt att denna information kontinuerligt uppdateras. I detta innefattas även att se till så att införandet och användandet av kostnadsfria tjänster så som gratis appar och sociala medier sker i överensstämmelse med reglerna i GDPR.

Verksamheten har uppgett att det finns rutiner för tilldelning av behörigheter och åtkomst till IT-system samt att dessa regelbundet följs upp. Dataskyddsombudets fördjupade kontroll för 2022 ligger inom ramen för denna kontrollpunkt och fokuserar på frågan om behörighetsstyrning och åtkomstkontroll. Resultatet av den fördjupade kontrollen presenteras i sin helhet i bilaga 2 till årsrapporten.

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:

Resultatet av verksamhetens skattning av rutiner för att hantera de registrerades rättigheter genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten har rutiner på plats avseende flertalet av de rättigheter som de registrerade kan åberopa. Dataskyddsombudet rekommenderar förvaltningen att säkerställa att de har alla rutiner på plats som behövs för att kunna garantera en korrekt och rättssäker hantering av de registrerades rättigheter. Svaren i enkäten indikerar att det inte finns en tillräckligt utbredd medvetenhet hos medarbetarna inom verksamheten om de rättigheter som de registrerade har eller när dessa begränsas. Dataskyddsombudet rekommenderar därför verksamheten att kartlägga kunskaperna angående registrerades rättigheter för att veta om verksamhetens medarbetare har behov av en riktad utbildning inom området.

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 4: Personuppgiftsregister
  Säkerställ att samtliga behandlingar dokumenteras i personuppgiftsregistret och att uppgifterna innehåller all obligatorisk information om behandlingarna som krävs enligt artikel 30 i GDPR.

- Kontrollpunkt 6: Utbildning
  Kartlägg utbildningsbehovet inom dataskydd och ta fram en långsiktig utbildningsplan.

- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg samtliga personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt

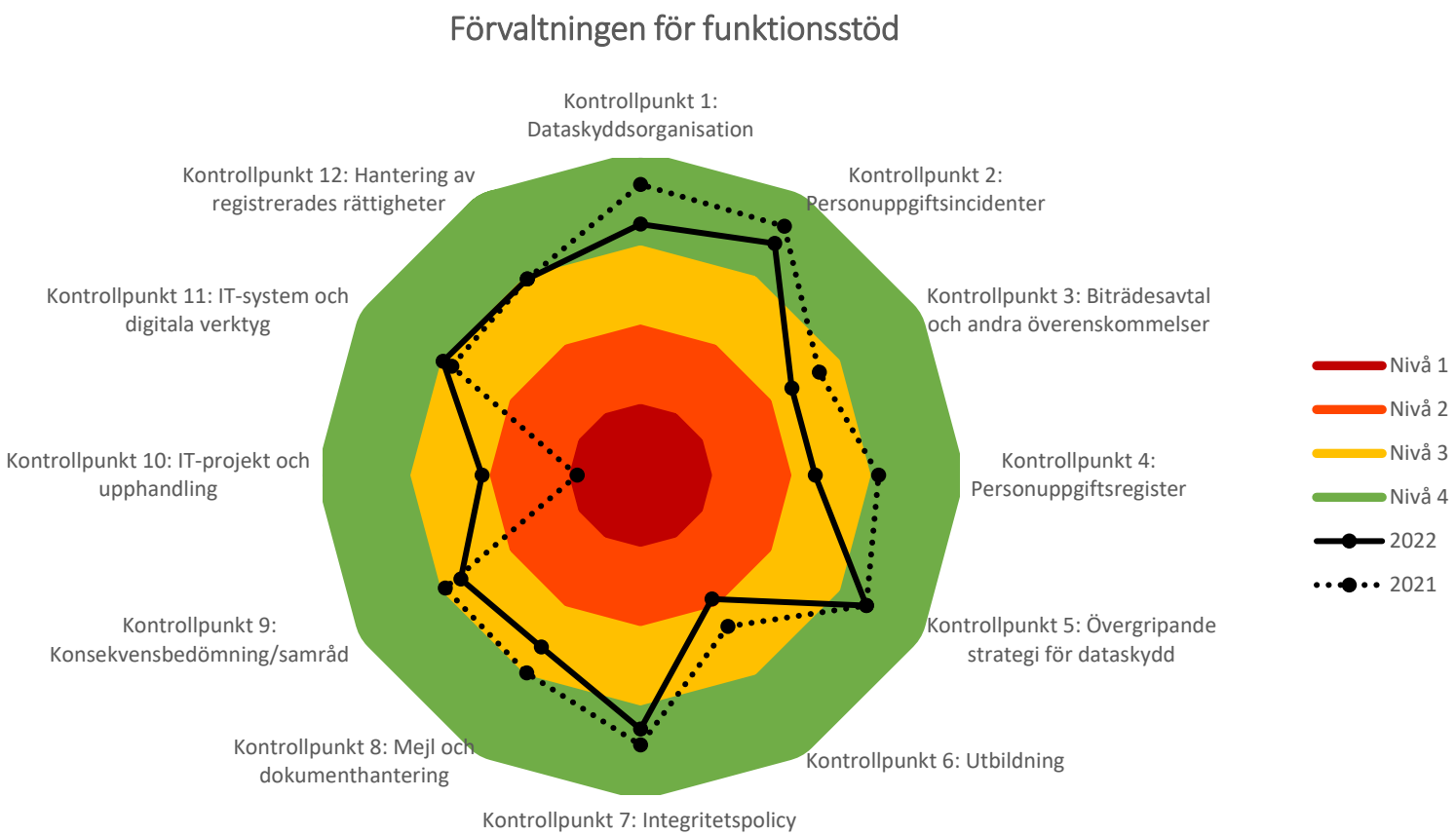
säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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 2022

Kontrollpunkt 11: Behörighetsstyrning (Förvaltningen för funktionsstöd)

Bakgrund

Under 2022 har dataskyddsombudet genomfört en fördjupad kontroll av verksamhetens arbete med behörighetsstyrning i IT-systemet Treserva 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 har avgränsats till att endast omfatta tilldelning och kontroll av behörigheter för chefer och medarbetare vid enheterna tillhörande Myndighet Hisingen/Centrum under avdelningen Myndighet och socialpsykiatri.

Granskningen har gjorts med utgångspunkt i artikel 32 i dataskyddsförordningen (GDPR)[1] 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 kan vara ett verktyg för verksamheterna att använda för att förhindra obehörig åtkomst till personuppgifter i ett IT-system.

Utifrån risker för registrerade vid behandlingen av dennes personuppgifter bör en medarbetares tillgång till system med personuppgifter 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. Bland annat behandlas klienternas namn, personnummer och uppgifter om anhöriga.

I maj 2022 hade enheterna tillhörande Myndighet Hisingen/Centrum totalt 5 231 öppna/pågående ärenden. Antalet sökbara avslutade ärenden i Treserva uppgick till 8 806. Antalet personer med behörighet till enheternas ärenden i Treserva varierar mellan 63 – 118 personer/enhet. Vid enheterna arbetar enhetschefer, 1:e socialsekreterare och handläggare.

Behörighetsstruktur och roller i system

Förvaltningen uppger att behörigheterna i Treserva för chefer och medarbetare vid enheterna tillhörande Myndighet Hisingen/Centrum är baserade på vilken befattning medarbetaren har och vilka arbetsuppgifter som ska utföras. Behörigheter ges utifrån en

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

behörighetsprofil som är baserad på medarbetarens arbetsuppgifter och enligt det som Intraservice har lagt inom dessa behörigheter. Förvaltningen har rutinen *Behörighetsprofiler för Treserva FFS* och i denna regleras de behörighetsprofiler som kan tilldelas inom förvaltningen av lokalt verksamhetsstöd inom respektive stadsområde och verksamhet. Den behörighetsprofil som tilldelas medarbetaren styr vad hen får göra i Treserva. En behörighetsprofil kombineras oftast med ett gruppfilter som innehåller de organisatoriska enheter som medarbetaren ska vara behörig till. Gruppfiltret styr alltså var i Treserva som medarbetaren kan arbeta.

Behörighetsprofilerna inom förvaltningens myndighetsutövning är följande:

- FH Handläggare myndighet (gruppfilter)
- FH Enhetschef myndighet (gruppfilter)
- FH Läsbehörighet (gruppfilter)
- FH Debitering och kontrakt (gruppfilter)
- FH Frågebehörighet (gruppfilter)

Tilldelning av behörighet

Förvaltningen beskriver att det sker en begränsad behörighetstilldelning generellt i Treserva. Behörigheter tilldelas utifrån medarbetarnas behov att kunna utföra sitt arbete. Exempelvis är det så att en enhetschef behöver kunna hantera avvikelser och får en behörighet tilldelad för denna uppgift men en handläggare tilldelas inte den behörigheten. Omfattningen av behörigheten påverkas även av vilken/vilka enheter som medarbetaren ska ha tillgång till. Det läggs inte på fler behörigheter än vad som behövs för arbetet. Det sker endast en begränsad tilldelning av behörigheter för sekretesskyddade ärenden.

Förvaltningen redogör vidare för att i Treserva är det inte svårt att begränsa behörigheter till en specifik enhet och att medarbetarna har då enbart behörighet till de uppgifter som härrör till den egna enheten inom förvaltningen. Det uppges att enhetschefer kan vilja att handläggarna ska ha tillgång till fler enheter än vad som är nödvändigt. Detta kan ibland kan vara problematiskt för handläggaren som då får tillgång till information som inte är nödvändig för dennes arbete.

Dataskyddsombudet anser att förvaltningen beskriver en tydlig och ändamålsenlig tilldelning av behörigheter som utgår från särskilda behörighetsprofiler baserade på medarbetarens arbetsuppgifter och gruppfilter utifrån organisatorisk tillhörighet. 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.[2] Det är positivt att förvaltningen uppfattar att det kan vara problematiskt om för vida behörigheter ges till medarbetare. Det är dessutom viktigt att förvaltningen beaktar att ju bredare teknisk behörighet en medarbetare har i ett system desto viktigare blir det att förvaltningen klargör för medarbetarna när det får anses tillåtet att ta del av information i systemet, exempelvis genom arbetsinstruktioner eller rutindokument.

[2] Socialstyrelsen. 2019-2-6, Säker personuppgiftsbehandling i socialtjänsten. Rättsläge och utgångspunkter. s. 29.

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

Beslut om behörighet

Förvaltningen uppger att beslut om behörigheter fattas av en medarbetares närmsta chef eller en högre chef. Behörigheterna tilldelas därefter av lokalt verksamhetsstöd. Vissa behörigheter kan endast tilldelas av systemförvaltare på Intraservice efter beställning från förvaltningen.

Uppföljning av behörighet

Förvaltningen anger att det har beslutats att behörighetskontroller ska genomföras två gånger per år. Verksamhetsutvecklare för Treserva ska ansvara för kontrollerna. Någon kontroll har dock inte genomförts då organisationen inte fungerar så väl ännu.

Det uppges att det därutöver är viktigt att uppmärksamma när en handläggare byter enhet. Om handläggaren har sekretessmarkerade behörigheter måste dessa avslutas i samband med ett byte av enhet, för att förhindra fortsatt tillgång till den sekretessmarkerade personen. Det är chefers ansvar att meddela om en behörighet ska avslutas om någon slutar sin anställning, men det sker inte alltid.

Dataskyddsombudet ser det som positivt att förvaltningen beslutat att genomföra regelbundna behörighetskontroller. Förvaltningen rekommenderas att påbörja arbetet med att genomföra kontrollerna i enlighet med beslutade rutiner så snart som de organisatoriska problemen är lösta. Att följa upp tilldelade behörigheter utgör en viktig del av arbetet med behörighetsstyrning, då det syftar till att upptäcka och motverka obehörig åtkomst. Dataskyddsombudet rekommenderar även förvaltningen att se över sitt arbetssätt vid personalförändringar som innebär att medarbetaren inte längre ska ha en tilldelad behörighet i systemet. Detta för att säkerställa att behörigheten följs upp direkt i samband med att en medarbetare avslutar sin anställning, får en ny roll inom organisationen, eller har en längre frånvaro genom exempelvis tjänstledighet, föräldraledighet eller sjukskrivning.

Åtkomstkontroll/kontroll av loggar

Åtkomstkontroll sker genom specifika beställningar av loggranskningar. Förvaltningens rutin är inte klar ännu men tanken är att åtkomstkontroll ska genomföras två gånger per år. Det är verksamhetsutvecklare för Treserva som ska ansvara för kontrollerna.

Dataskyddsombudet tycker att det är mycket positivt att förvaltningen arbetar med denna fråga. Förutom uppföljning av tilldelade behörigheter är logg- och åtkomstkontroller viktiga redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. Det är därför av vikt att det finns ett tydligt arbetssätt och rutiner för kontroll av loggar och åtkomst. Genom att dokumentera hur arbetet ska bedrivas kan förvaltningen visa hur de arbetar för att efterleva kraven i GDPR. Dataskyddsombudet vill även påminna om att det är viktigt att informera berörda medarbetare om åtkomstkontrollerna och att kontrollerna bör inte inskränka medarbetarnas integritet på ett oproportionerligt sätt.

Personuppgiftsbiträdet

Förvaltningen beskriver att det finns ett personuppgiftsbiträdesavtal mellan Göteborgs Stad och leverantören av Treserva, CGI. I detta avtal finns instruktioner om hur personuppgifter ska behandlas. Förvaltningen har inte lämnat några instruktioner till Intraservice men förväntar sig att de har koll på behörigheterna.

Dataskyddsombudet vill uppmärksamma förvaltningen på att de som personuppgiftsansvarig behöver ge personuppgiftsbiträdet dokumenterade instruktioner.[3] 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.[4]

Konsekvensbedömning och risker

Förvaltningen anger att det inte finns någon genomförd konsekvensbedömning avseende de behandlingar som sker i Treserva. Bedömningar på processer kopplade till behandlingar i Treserva gjordes 2019 men dessa har varken uppdaterats eller säkerställts om de fortfarande gäller. Dataskyddsombudet rekommenderar förvaltningen att identifiera de behandlingar som sker i systemet och ta ställning till om de behöver konsekvensbedömas utifrån hög risk för de registrerades fri- och rättigheter. I samband med en konsekvensbedömning kan det identifieras risker med för vida behörigheter.

Avseende risker i övrigt uppger förvaltningen att det har uppmärksammats att när en insats om en klient avslutas kan man i Treserva välja att meddela om detta. Dessa interna mejl går då ut till alla som har tillgång till den aktuella enheten som utfört insatsen, oavsett om medarbetaren har kvar klienten eller inte. I samband med utbildningsinsatser informeras medarbetare att inte välja att meddela vid avslut av insats för att förhindra detta. Enligt information från Intraservice går funktionen inte att ta bort. Dataskyddsombudet är medveten om att det eventuellt kan finnas praktiska och tekniska utmaningar i att genomföra en ändamålsenlig behörighetsstyrning i Treserva. Det är dock bra att förvaltningen gör vad man kan för att minska de risker som finns.

Sammanfattade rekommendationer

- Förvaltningen rekommenderas säkerställa att uppföljning av tilldelade behörigheter i Treserva genomförs i enlighet med beslutade rutiner.
- Förvaltningen rekommenderas att arbeta för att minimera risken för felaktiga behörigheter vid personalförändringar och att det sker i direkt anslutning till att en medarbetare exempelvis byter tjänst.
- Förvaltningen rekommenderas att fortsätta arbetet med att ta fram rutiner för åtkomstkontroll/loggуppföljning. Berörda medarbetare måste sedan informeras om gällande rutiner.
- Förvaltningen rekommenderas att ge personuppgiftsbiträdet dokumenterade instruktioner.
- Förvaltningen rekommenderas att se över behovet av konsekvensbedömning för behandlingarna i systemet, eftersom det då kan identifieras risker med för vida behörigheter.

[3] Se artikel 28.3 a i GDPR
[4] Se artikel 28.3 b i GDPR

Bilagor

- Information om fördjupad kontroll 2022
- Fördjupad kontroll 2022, Kontrollpunkt 11: Behörighetsstyrning (del 1)
- 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 medarbetare och chefer vid enheterna tillhörande Myndighet Hisingen/Centrum under avdelningen Myndighet och socialpsykiatri.

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 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 medarbetare och chefer vid enheterna tillhörande Myndighet Hisingen/Centrum under avdelningen Myndighet och socialpsykiatri.

- 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 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 tillhörande Myndighet Hisingen/Centrum under avdelningen Myndighet och socialpsykiatri?
- Hur många registrerades personuppgifter hanteras i Treserva med anledning av ärenden som dessa enheter handlägger? Ange antalet registrerade som har öppna ärenden hos respektive enhet under maj månad 2022 samt antalet registrerade i respektive enhets 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 på respektive enhet med åtkomst till personuppgifterna samt hur många som tillhör andra organisatoriska enheter/avdelningar inom förvaltningen eller hos personuppgiftsbiträdet med åtkomst till personuppgifterna.
- 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 Intraservice/personuppgiftsbiträdets 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.