Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Socialförvaltningen Nordost

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 försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten lämnat följande sammanfattande rekommendationer:

- Förvaltningen rekommenderas säkerställa att det finns en ändamålsenlig behörighetstilldelning till försörjningsstödsenheternas ärenden.
- Förvaltningen rekommenderas överväga behovet av att införa åtkomstkontroll/logguppföljning i form av regelbundna slumpmässiga stickprovskontroller.
- 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 Socialförvaltningen Nordosts 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 påståenden under denna kontrollpunkt. Sammantaget genererar svaren ett mycket 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 uppger att dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten samt att verksamheten har regelbunden kontakt med dataskyddsombudet. Dataskyddsombudet upplever att det finns en väl fungerande intern organisation och att det finns en stor medvetenhet om hanteringen av personuppgifter inom verksamheten. Verksamheten lyfter många och viktiga dataskyddsfrågor med dataskyddsombudet. Dataskyddsombudet instämmer därför med den skattning som verksamheten gjort avseende dessa frågor. Det är däremot viktigt att verksamheten fortsätter stödja och prioritera det interna dataskyddsarbetet och att möjligheter ges för att förbättra arbetet ytterligare.

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. Samtliga inträffade incidenter under senaste året som inneburit en rapporteringsskyldighet har rapporterats inom angivna tidsfristen om 72 timmar till tillsynsmyndigheten. Vidare uppger verksamheten att de systematiskt följer upp inträffade personuppgiftsincidenter som en naturlig del i dataskyddsarbetet. Medarbetare informeras om vad personuppgiftsincidenter är samt vad det finns för rutiner 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 incidenter har inträffat för att stämma av den fortsatta handläggningen. Verksamheten återrapporterar dessutom regelbundet till dataskyddsombudet om samtliga personuppgiftsincidenter som inträffat. Dataskyddsombudet vill ändå skicka med att det är viktigt att kontinuerligt se över och säkerställa att det finns väl fungerade rutiner för hanteringen av personuppgiftsincidenter.

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 som bedöms vara omfattande och/eller kräver omgående åtgärder.

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 inte finns tillräckliga rutiner för bedömningen om en ny leverantör är personuppgiftsansvarig eller biträde för behandlingen samt för tecknandet av biträdesavtal. Det finns tecknade personuppgiftsbiträdesavtal för uppskattningsvis 25 % av verksamhetens anlitade personuppgiftsbiträden. Dataskyddsombudet rekommenderar därför verksamheten att säkerställa att det finns rutiner för att identifiera och reglera förhållandet med personuppgiftsbiträden och eventuella underbiträden. Dessutom bör verksamheten fortsätta kartläggningen av personuppgiftsbiträden och upprätta personuppgiftsbiträdesavtal i de fall det saknas.

Verksamheten uppger vidare 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 dokumentering av hela kedjan av underbiträden behövs exempelvis för att få en bättre överblick av behandlingen 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 i princip samtliga behandlingar är dokumenterade i personuppgiftsregistret men de bedömer att endast hälften av dessa innehåller all obligatorisk information som krävs enligt artikel 30 i GDPR. Dataskyddsombudet rekommenderar därför verksamheten att fortsätta arbetet med att tillföra den information som krävs.

Ett aktuellt och uppdaterat personuppgiftsregister kan vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete. Dataskyddsombudet rekommenderar därför verksamheten att säkerställa att det finns rutiner för att uppdatera registret när en behandling tillkommit eller förändras. Verksamheten bör 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 och regelbundna interna kontroller genomförs för att säkerställa följsamheten gentemot GDPR. Det finns rutiner för att säkerställa att styrande dokument som reglerar verksamhetens personuppgiftsbehandlingar hålls uppdaterade. Verksamheten har emellertid endast identifierat och värderat upp till 50% av informationstillgångarna i enlighet med stadens styrande dokument och dataskyddsombudet rekommenderar att verksamheten vidtar de åtgärder som behövs inom detta område.

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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av utbildning inom dataskyddsområdet genererar sammantaget ett mycket högt resultat som innebär att inga direkta risker av betydelse har identifierats.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Förvaltningen behöver därför även fortsättningsvis ge medarbetarna möjlighet att delta i utbildnings- och informationsinsatser för att säkerställa en god kunskapsnivå om 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 mycket högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter. Av bestämmelserna i GDPR framgår vilka krav som ställs på informationen. Verksamheten har under denna punkt angett att verksamheten uppfyller informationsplikten genom integritetspolicyn och informationen är tydliga och lättillgänglig. Policyn uppdateras vid behov och de registrerade kan på ett enkelt sätt kan nå verksamhetens integritetspolicy från verksamhetens samtliga digitala kanaler. Även verksamhetens medarbetare informeras om hur deras personuppgifter behandlas. Dataskyddsombudet vill dock 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, ändamål och 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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av rutiner för e-post och dokumenthantering genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Idag saknar verksamheten en dokumenthanteringsplan med gallringsbeslut. Det är av vikt att verksamheten säkerställer att en sådan kommer på plats för att

personuppgiftsbehandlingar ska kunna ske i enlighet med bestämmelserna 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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av dataskyddsarbetet med konsekvensbedömningar genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

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 och även för att uppdatera befintliga konsekvensbedömningar vid förändringar. Det behöver dock tas fram ett arbetssätt för att inhämta de registrerades synpunkter på en behandling i vissa fall. Verksamheten har under det gångna året involverat dataskyddsombudet i de tröskelanalyser och konsekvensbedömningar som verksamheten genomfört.

Verksamheten uppger att de för uppskattningsvis 75 % av verksamhetens personuppgiftsbehandlingar genomfört konsekvensbedömning utifrån hög risk eller för att det krävs enligt Integritetsskyddsmyndighetens lista. Det finns därutöver en planering som omfattar ungefär 75 % av de behandlingar för vilka en konsekvensbedömning behöver göras. Dataskyddsombudet rekommenderar därför verksamheten att kartlägga samtliga de personuppgiftsbehandlingar som kan innebära en hög risk för de registrerades fri- och rättigheter och ta fram en handlingsplan 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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av dataskyddsrutiner för IT-projekt och upphandling genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Verksamheten uppger att de har organisatoriska förutsättningar och rutiner för att arbeta med dataskyddsfrågor inom IT-projekt och upphandling. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda arbetet inom detta område samt att fortsätta involvera dataskyddsombudet på samma sätt som den interna dataskyddsorganisationen gjort under det gångna året.

Dataskyddsombudet vill även skicka med att det är viktigt att kontinuerligt se över och säkerställa att det finns väl fungerade rutiner för upphandlingen av nya system/tjänster. Vid upphandlingar behöver det tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. Det är nämligen av stor vikt att ta hänsyn till integritetsskyddet redan vid upphandlingen av exempelvis ett IT-system för att säkerställa att funktioner byggs in som stödjer detta. Det ska 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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av dataskyddsrutiner för IT-system och digitala verktyg genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Verksamheten bedriver ett väl fungerande arbete för att säkerställa att IT-system och digitala verktyg är förenliga med GDPR. Eftersom IT-system och digitala verktyg är några av de främsta arbetsredskapen inom en verksamhet är det viktigt att detta arbete fortsätter och att verksamheten ger den interna dataskyddsorganisationen möjlighet att förbättra rutiner och processer ytterligare.

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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av rutiner för att hantera de registrerades rättigheter genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Resultatet visar att verksamheten har goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet vill dock påminna om att det är viktigt att verksamheten också fortsättningsvis arbetar systematiskt med att se över och förbättra verksamhetens rutiner och processer för att säkerställa efterlevnaden av de registrerades rättigheter. I detta ingår även att framöver se till så att medarbetarna inom verksamheten har en god medvetenhet om de rättigheter som de registrerade har och när dessa begränsas.

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 3: Biträdesavtal och andra överenskommelser
  Säkerställ att det finns rutiner för att identifiera och reglera förhållandet med personuppgiftsbiträden och eventuella underbiträden. Fortsätt kartläggningen av personuppgiftsbiträden och upprätta personuppgiftsbiträdesavtal i de fall det saknas.

- Kontrollpunkt 4: Personuppgiftsregister
  Säkerställ att personuppgiftsregistret innehåller all obligatorisk information om behandlingarna som krävs enligt artikel 30 i GDPR.

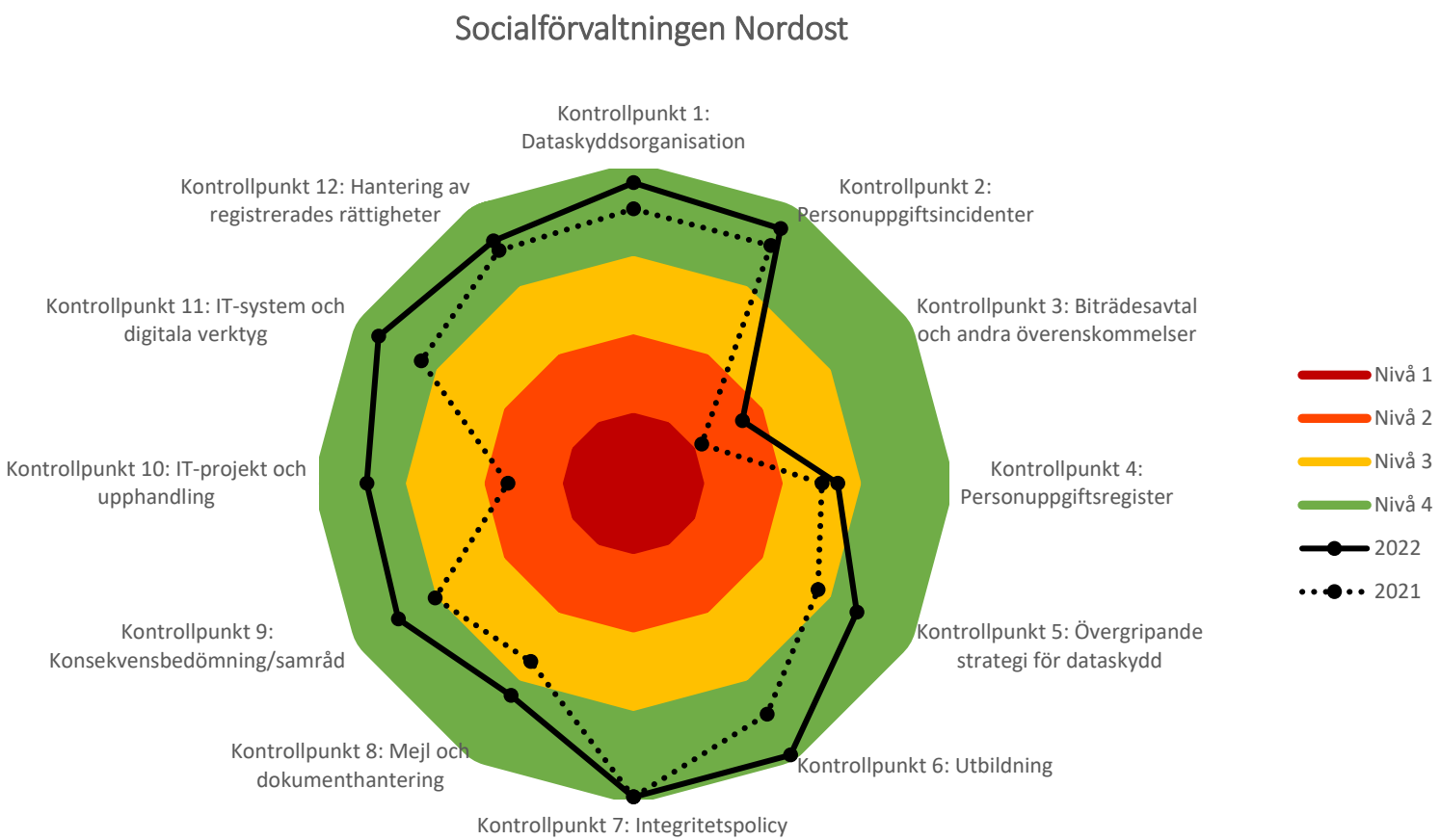
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg samtliga personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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 (Socialförvaltningen Nordost)

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 försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd.

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

Vid försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd finns enhetschef, 1:e socialsekreterare, 1:e socialsekreterare Mottaget, handläggare, handläggare Mottaget och studenter med verksamhetsförlagd utbildning. Antalet medarbetare vid de aktuella enheterna med behörighet till enhetens ärenden i Treserva varierar mellan 17–33 personer.

Även medarbetare som organisatoriskt tillhör andra enheter än försörjningsstödsenheterna tilldelas behörigheter utifrån befattning för att kunna genomföra arbetsuppgifter. Det rör sig om bland annat administratör/chefsstöd som hanterar klientfakturor, arkivarier, nämndsekreterare och receptionist.

Förvaltningen uppger att det är mellan 599–615 medarbetare som har behörighet till respektive försörjningsstödsenhets ärenden men de flesta av dessa personer har endast

[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

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

läsbehörighet. Uppgiften om behöriga personer avser både medarbetare på övriga försörjningsstödsenheter och medarbetare på andra enheter. Antalet behöriga på Intraservice är 12 personer.

I maj 2022 hade försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd totalt 3 610 öppna/pågående ärenden. Antalet sökbara avslutade ärenden på avdelningen för perioden 2021-01-01 till 2022-05-31 uppgick till 3 998.

I försörjningsstödsärendena i Treserva finns personuppgifter tillhörande klienter men även uppgifter om förvaltningens anställda. De uppgifter som finns om klienter är bland annat namn, personnummer, adress, övriga kontaktuppgifter, familjeförhållanden (inklusive uppgifter om barn) och anhöriguppgifter. Därutöver finns information om klientens ekonomiska förhållanden tillsammans med ekonomiska uppgifter från andra myndigheter som CSN, Skatteverket, Försäkringskassan och Pensionsmyndigheten. De uppgifter om förvaltningens anställda som finns i Treserva är namn, personnummer, befattning, Stadenkonto (inloggning) och tjänstetelefonnummer.

Behörighetsstruktur och roller i system

Förvaltningen redogör för att det i Treserva finns en särskild modul i systemet för hantering av behörigheter. Medarbetare som ska få behörighet till systemet tilldelas en roll, en profil och ett gruppfilter. De roller som finns för de aktuella enheterna är bland annat enhetschef, 1:e socialsekreterare, 1:e socialsekreterare Mottaget, handläggare, handläggare Mottaget och studenter med verksamhetsförlagd utbildning. Profilen anger vilka rättigheter medarbetaren har till olika funktioner i systemet. Gruppfiltret anger vilka organisatoriska enheter medarbetaren har behörighet till. Det finns ett inbyggt gruppfilter som innebär att det lokala verksamhetsstödet (LVS Treserva) enbart kan tilldela behörigheter till enheter i Treserva inom SF Nordost och för medarbetare i SF Nordost.

Om en medarbetare behöver behörighet till enheter inom en annan förvaltning för samma Stadenkonto, vid exempelvis delad tjänst, är det enbart Intraservice förvaltarenhet som har behörighet att tilldela en sådan behörighet. I annat fall krävs att medarbetare har ett Stadenkonto i respektive förvaltning och då hanteras behörigheten av LVS Treserva i respektive förvaltning.

Tilldelning av behörighet

Förvaltningen uppger att behörigheterna till Treserva tilldelas inom förvaltningen utifrån medarbetarens befattning och ansvar utifrån delegation. Vid tilldelning av behörighet kontrollerar LVS Treserva att beställning för berörd medarbetare är befogad utifrån uppdrag och organisatorisk tillhörighet. För varje medarbete finns en behörighetsblankett av vilken det framgår namn, personnummer, befattning, avdelning, enhet och medarbetarens behörigheter.

Det finns särskilda rutiner för att begränsa och reglera vilka som får ha behörigheter till skyddade ärenden. För de skyddade ärendena finns det både lokala och staden-övergripande rutiner. Vad gäller andra mer specifika behörigheter, så som exempelvis attestbehörighet och läsbehörighet sekretess, tilldelas dessa av Intraservice efter beställning undertecknad av förvaltningsdirektören.

Dataskyddsombudet tycker att det är bra att det finns tydliga rutiner för hur behörigheter till Treserva ska tilldelas och att detta sker utifrån befattning och delegerat ansvar. 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] Dataskyddsombudet anser att förvaltningen, med sin verksamhetskunskap, är bäst lämpad att göra denna bedömning. Utifrån bland annat uppgiften om att det är ett stort antal medarbetare som har tilldelats behörighet, främst läsbehörighet, till försörjningsstödsenheterna ärenden vill dock dataskyddsombudet rekommenderar förvaltningen att säkerställa att det finns en ändamålsenlig behörighetstilldelning. Vid en sådan bedömning är det även viktigt att beakta att ju vidare 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 en rutin.[3]

Beslut om behörighet

Förvaltningen anger att det finns en samordnad rutin för hanteringen av behörigheter till IT-system, varav ett av dem är Treserva. Det är enhetschef som fattar beslut om att tilldela behörigheter till medarbetare. Behörigheterna tilldelas därefter av LVS Treserva. Vissa behörigheter kan endast tilldelas av systemförvaltare på Intraservice efter beställning från förvaltningen.

Uppföljning av behörighet

Förvaltningen har rutiner för att hantera behörigheter till nya medarbetare samt ändring och avslut av behörigheter för befintliga medarbetare. Vid ändringar i medarbetarens tjänst sker borttag och tillägg av behörigheter utifrån vilka förändrade behov medarbetaren har i tjänsten. Förvaltningen uppger att LVS Treserva gör löpande kontroller under året av vissa behörigheter. Det sker exempelvis om medarbetare återgår i tjänst efter en längre ledighet. I dessa fall kontrolleras att behörigheter är aktuella och motsvarar uppdraget.

Förvaltningen genomför även en särskild intern kontroll på IT-behörigheter två gånger per år. LVS Treserva ansvarar för kontrollen i Treserva och de granskar då, med hjälp av enhetscheferna, att medarbetare har rätt behörighetsnivå utifrån uppdraget. Avstämning sker dessutom med chefen för förvaltarenheten på Intraservice för att kontrollera att det är rätt medarbetare vid Intraservice som har fått behörighet till Treserva.

Dataskyddsombudet ser det som positivt att förvaltningen genomför regelbundna behörighetskontroller. Att följa upp tilldelade behörigheter utgör en viktig del av arbetet med behörighetsstyrning, då det syftar till att upptäcka och motverka obehörig åtkomst.

Åtkomstkontroll/kontroll av loggar

Förvaltningen uppger att LVS Treserva kan beställa olika typer av logglistor från Intraservice. Inom ramen för egenkontroll beställer LVS Treserva logglistor från Intraservice över skyddade ärenden en gång per år. Det är enhetschefen som ansvarar för att kontrollera logglistan över de skyddade ärenden som finns inom enheten. Även

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

medarbetare vid Intraservice som har behörighet till Treserva kontrolleras genom egenkontroll för skyddade ärenden två gånger per år genom slumpmässigt urval.

LVS Treserva kan därutöver beställa logglista på uppdrag av enhetschef vid exempelvis misstanke om otillbörlig användning av systemet. Det är enhetschefen som kontrollerar logglistorna.

Dataskyddsombudet tycker att det är positivt att kontroll av åtkomstloggar sker inom förvaltningen. Förutom uppföljning av tilldelade behörigheter är logg- och åtkomstkontroller viktiga redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. Även åtkomstkontroller i form av regelbundna stickprovskontroller kan vara ett effektivt verktyg i detta arbete och dataskyddsombudet rekommenderar förvaltningen att överväga behovet av sådana kontroller.

Det är 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 åtkomstkontroller och gällande rutiner. Kontrollerna bör dessutom inte inskränka medarbetarnas integritet på ett oproportionerligt sätt.

Personuppgiftsbiträdet

Intraservice är förvaltningens personuppgiftsbiträde och kommunens beslutade riktlinjer för kommungemensamma tjänster ersätter ett personuppgiftsbiträdesavtal. Det finns inte några särskilda instruktioner framtagna till personuppgiftsbiträdet för Treserva.

Dataskyddsombudet vill uppmärksamma förvaltningen på att de som personuppgiftsansvarig behöver ge personuppgiftsbiträdet dokumenterade instruktioner.[4] 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.[5]

Konsekvensbedömning och risker

Förvaltningen beskriver att konsekvensbedömningar ännu inte har genomförts avseende de behandlingar som sker i systemet Treserva. Ambitionen är att välfärdsförvaltningarna ska arbeta tillsammans kring denna ”skuld”.

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.

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

Sammanfattade rekommendationer

- Förvaltningen rekommenderas säkerställa att det finns en ändamålsenlig behörighetstilldelning till försörjningsstödsenheternas ärenden.
- Förvaltningen rekommenderas överväga behovet av att införa åtkomstkontroll/loggуppföljning i form av regelbundna slumpmässiga stickprovskontroller.
- 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.

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 försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd.

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 försörjningsstödsenheterna under avdelningen Vuxna och försörjningsstöd.

- 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 ni frågor, kontakta ert 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 av försörjningsstödsenheterna tillhörande avdelningen Vuxna och försörjningsstöd?
- 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.