Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Socialförvaltningen Sydväst

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 avdelningen Vuxen och försörjningsstöd.

Dataskyddsombudet har i rapporten lämnat följande sammanfattande rekommendationer:

- Förvaltningen rekommenderas att säkerställa att det finns en ändamålsenlig behörighetstilldelning samt en tydlig och enhetlig process för tilldelning av behörigheter.
- Förvaltningen rekommenderas att bestämma vilka funktioner som ska ha befogenhet att besluta om behörighetstilldelning.
- Förvaltningen rekommenderas att följa upp hur genomförandet av behörighetskontroller har fungerat samt utvärdera om kontrollerna behöver ske oftare än en gång per år.
- Förvaltningen rekommenderas att följa upp hur genomförandet av stickprovskontroller har fungerat samt att utvärdera om det är ett lagom antal kontroller som genomförs.
- 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.	

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

Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Socialförvaltningen Sydvästs 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 påståenden 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 uppger vidare att dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten och att verksamheten har regelbunden kontakt med dataskyddsombudet. Dataskyddsombudet upplever att det finns en väl fungerande intern organisation och att det finns en 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 personuppgiftsincidenter under senaste året som inneburit en rapporteringsskyldighet har rapporterat 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 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. 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 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 inte finns tillräckliga rutiner för bedömningen om en ny leverantör är personuppgiftsansvarig eller biträde för behandlingen samt för tecknandet av biträdesavtal. Det finns dock tecknade personuppgiftsbiträdesavtal för uppskattningsvis 100 % av verksamhetens anlitade personuppgiftsbiträden. Dataskyddsombudet rekommenderar verksamheten att säkerställa att det finns rutiner för att identifiera och reglera förhållandet med personuppgiftsbiträden och eventuella underbiträden. Verksamheten bör även kontrollera att personuppgiftsbiträdesavtal har tecknats i de fall det krävs.

Verksamheten uppger att det inte finns tillräckliga rutiner för att kontinuerligt genomföra efterlevnadskontroller och för att bedöma andra typer av överenskommelse/avtal som kan behöva upprättas avseende gemensam eller annan delad hantering av personuppgifter. Tillräckliga rutiner saknas även 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 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. Vidare anges att de dokumenterade behandlingarna innehåller all obligatorisk information som krävs enligt artikel 30 i GDPR. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda arbetet och säkerställa att samtliga behandlingar dokumenteras i personuppgiftsregistret.

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 och rutiner för att säkerställa att styrande dokument som reglerar verksamhetens personuppgiftsbehandlingar hålls uppdaterade. Verksamheten har identifierat och värderat uppskattningsvis 75% av dess informationstillgångar i enlighet med stadens styrande dokument inom informationssäkerhet. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda 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. Det behöver även säkerställas att regelbundna interna kontroller genomförs för att garantera följsamheten gentemot GDPR.

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

Verksamhetens svar på enkäten i denna del indikerar att medarbetarna regelbundet ges möjlighet att delta i utbildningar inom dataskydd. Det finns hos medarbetarna

inom verksamheten en god allmän kunskapsnivå som i sin tur skapar goda förutsättningar i dataskyddsarbetet. Däremot saknas det någon form av kartläggning av mer behovsanpassad utbildning för olika befattningar samt 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:

Resultatet av verksamhetens skattning av utformningen och tillhandahållandet av integritetspolicyn genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter. Av bestämmelserna i GDPR framgår vilka krav som ställs på informationen. Verksamheten anger under denna punkt att integritetspolicyn uppfyller kraven på information. Informationen är tydlig och lättillgänglig samt uppdateras vid behov. Även medarbetare informeras om hur deras personuppgifter behandlas. Dataskyddsombudet noterar dock att verksamheten behöver säkerställa att de registrerade på ett enkelt sätt kan nå verksamhetens integritetspolicy från verksamhetens samtliga digitala kanaler. Dessutom vill dataskyddsombudet påminna om att det alltid är viktigt att säkerställa att policyn uppfyller kraven på information samt 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:

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 säkerställa att den informationsklassificering som verksamheten gjort av sina personuppgiftsbehandlingar är aktuell.

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. 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 samt metod för att inhämta och dokumentera

dataskyddsombudets synpunkter när konsekvensbedömning inte bedöms behövas genomföras. Därutöver finns rutiner för att genomföra och dokumentera konsekvensbedömningar innan behandlingen påbörjas och även för att uppdatera befintliga konsekvensbedömningar vid förändringar. Verksamheten har under det gångna året involverat dataskyddsombudet i de tröskelanalyser och konsekvensbedömningar som verksamheten genomfört.

Verksamheten anger att de för uppskattningsvis 25 % av verksamhetens personuppgiftsbehandlingar genomfört konsekvensbedömning utifrån hög risk eller för att det krävs enligt Integritetsskyddsmyndighetens lista. 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 dataskyddsrutiner för IT-projekt och upphandling genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

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. De arbetar dessutom systematiskt och kontinuerligt med att bedöma risker för personuppgiftsbehandlingar i såväl nya som befintliga system och tjänster. Det finns rutiner för att involvera dataskyddsombudet från start vid införandet av tjänster där personuppgifter hanteras och det är dataskyddsombudets uppfattning att detta oftast görs.

Av enkätsvaren framgår att verksamheten inte i tillräcklig utsträckning kan säkerställa en anpassning till inbyggt dataskydd och dataskydd som standard vid upphandlingar. Verksamheten har dock berättat att den interna dataskyddsorganisationen i de flesta fall involveras när förvaltningen gör egna upphandlingar men att det inte sker när Intraservice ansvarar för upphandlingen. Dataskyddsombudet rekommenderar därför verksamheten att verka för 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.

Verksamheten anger i enkäten att de har överblick över sina IT-system och digitala verktyg samt att det finns rutiner för tilldelning av behörigheter och åtkomst till dessa. Medarbetarnas behörigheter och möjlighet att komma åt uppgifter i systemen och verktygen följs regelbundet upp. Eftersom IT-system och digitala verktyg är några av de främsta arbetsredskapen inom en verksamhet är det av stor vikt att det kartläggs och dokumenteras information om samtliga de system och verktyg som används. Dataskyddsombudet rekommenderar även verksamheten 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.

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

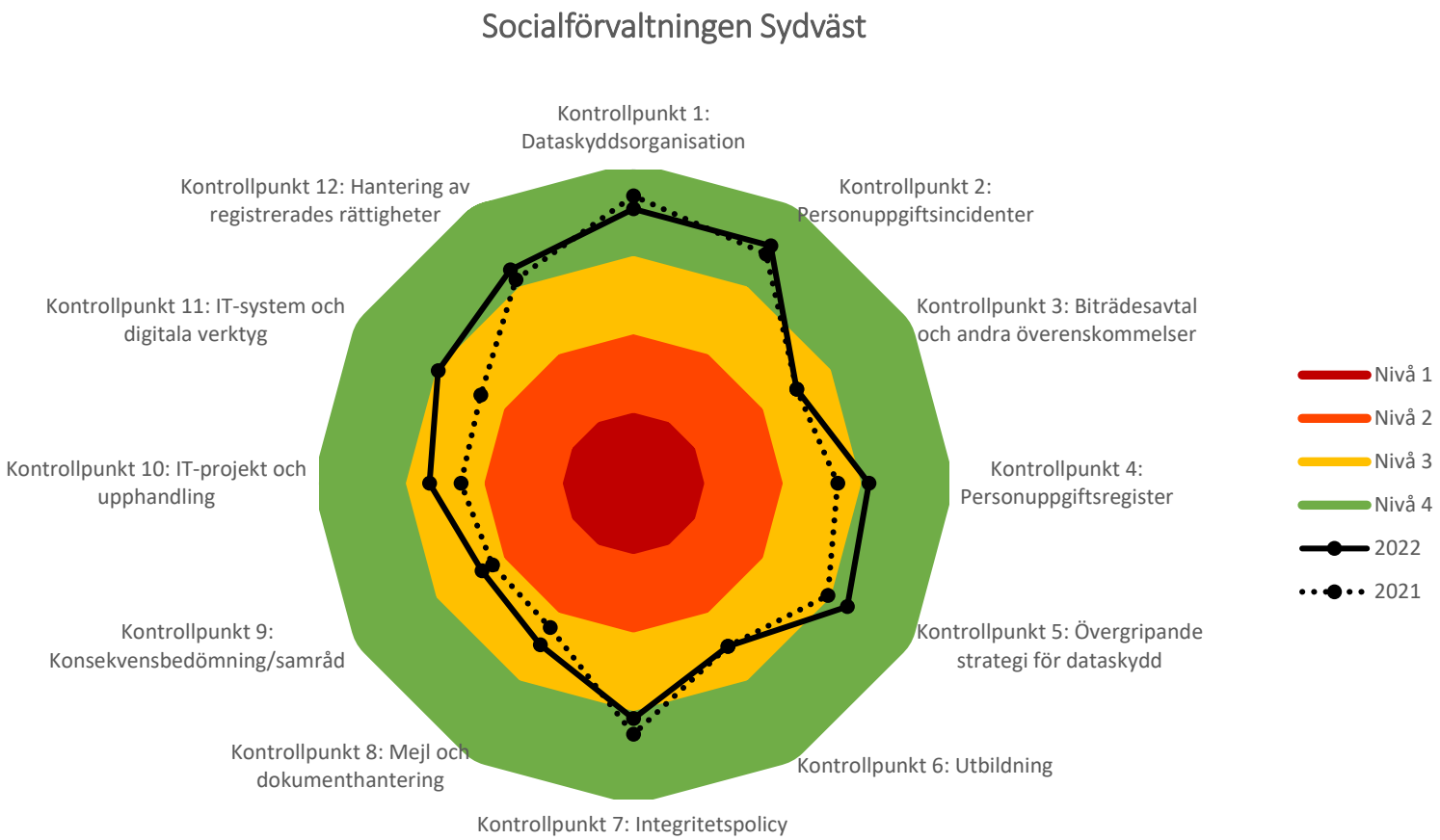
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg samtliga personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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 Sydväst)

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 avdelningen Vuxen 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

I maj 2022 hade avdelningen Vuxen och försörjningsstöd 1 917 öppna/pågående ärenden som gällde cirka 3 400 klienter. Förvaltningen beskriver att antalet ärenden förändras hela tiden då nya tillkommer och andra avslutas. Avslutade ärenden är sökbara så länge ärendet inte gallrats. Först när ärendet är gallrat försvinner det från Treserva och är då inte längre sökbart. Det går inte att göra ändringar i avslutade ärenden utan bara läsa innehållet. Tilldelade behörigheter gäller oavsett om ärendet är öppet eller avslutat.

Förvaltningen har ombetts besvara frågor avseende antalet medarbetare som har tilldelats behörighet till avdelningen Vuxen och försörjningsstöds ärenden men svar har inte inkommit i denna del.

I ett ärende behandlas klientens livssituation utifrån ansökan och eventuellt annat behov. De personuppgifter som kan förekomma om en klient är anställningsinformation, familjeinformation, finansiella uppgifter, kontaktinformation, myndighetsutfärdad

[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

identifikation, personlig identifikation, social välfärds- och arbetsdata, personliga egenskaper samt uppgifter om utbildning och arbete.

Behörighetsstruktur och roller i system

Förvaltningen anger att användarbehörigheten i Treserva består av fyra flikar; aktör, användare, organisation/roll och ärendetyp. Under ”aktör” registreras uppgifter om bland annat medarbetarens befattning, kontaktinformation och vissa personuppgifter. Under ”användare” registreras användar-id/användarnamn och vilka profiler som medarbetaren ska ha behörighet till. Under ”organisation/roll” registreras vilka organisatoriska enheter som medarbetaren ska ha behörighet till. Roller kan till exempel vara handläggare myndighet, 1:e socialsekreterare, enhetschef och administratör IFO. Under ”ärendetyp” registreras vilken ärendetyp inom respektive enhet som medarbetaren ska kunna arbeta med och vara beslutsfattare för. Ärendetyp är endast aktuellt att fylla i för medarbetare som är beslutsfattare.

Det finns många olika behörighetsnivåer i systemet. I Treserva kan en medarbetare ha åtkomst till vissa personuppgifter utan att ha åtkomst till hela ärendet. Exempelvis så kan en medarbetare med Treservas ”frågebehörighet” leta upp ett ärende via personnumret men kommer inte in i klientens journal. Av uppgifterna i Treserva framgår inte vilken enhet en medarbetare tillhör utan endast vilken enhet som medarbetaren har behörighet till. Förvaltningens medarbetare ser endast uppgifter som härrör till den egna förvaltningen.

Tilldelning av behörighet

Förvaltningen uppger att det lokala verksamhetsstödet (LVS) har utökad behörighet i Treserva och tilldelar behörighet i Treserva till medarbetare och chefer. När det gäller vissa behörigheter, så som exempelvis attestbehörigheter, läggs dess på av Intraservice.

Förvaltningen redogör därutöver för att det har sett olika ut avseende vilken roll som får vilka behörigheter. Det finns inget formellt beslut fattat ännu om tilldelning av behörigheter. Vid tilldelning av behörigheter inom förvaltningen idag är dock utgångspunkten att medarbetaren endast ska ha den behörighet som krävs för att hen ska kunna utföra sitt jobb.

Förvaltningen lämnar följande exempel på hur det kan se ut idag:

Medarbetare/socialsekreterare:
Försörjningsstöd: *Generellt kan man säga att socialsekreterare har behörighet som beslutsfattare till varandras enheter inom försörjningsstöd samt läsbehörighet till övrigt bistånd (dvs. kan gå in och läsa i Vuxenenheternas ärenden).*
Vuxenenheten: *har behörighet som beslutsfattare till varandras enheter inom vuxen samt läsbehörighet till ekonomiskt bistånd.*
Unga vuxna: *jobbar både med försörjningsstöd och övrigt bistånd och har därför behörighet som beslutsfattare på sina egna enheter samt till Vuxenenheterna och även till enheter på avdelning Barn och unga då ärenden överflyttas den vägen. Vad gäller försörjningsstödsbehörighet endast som beslutsfattare på egen enhet.*
EC avdelning Vuxen/F-stöd: har behörighet som beslutsfattare till alla enheter inom avdelning vuxen/f-stöd samt attestbehörighet och ansvarig avvikelse.

1:e socialsekreterare:
Försörjningsstöd: *Läsbehörighet till skyddade personuppgifter. Attestbehörighet. Beslutsfattare till försörjningsstödsenheterna.*
Vuxenenheterna: *1:e på mottaget har läsbehörighet till skyddade personuppgifter. Beslutsfattare på vuxenenheterna (inkl. Unga vuxna), vissa behörigheter som beslutsfattare på försörjningsstöd men vissa har endast läsbehörighet.*
Unga vuxna: *Läsbehörighet till skyddade personuppgifter. Attestbehörighet. Beslutsfattare på samtliga vuxenenheter samt någon enhet på Barn och unga. Beslutsfattare på egen enhet för försörjningsstöd (Unga vuxna f-stöd).*

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. Förvaltningen rekommenderas att säkerställa att det finns en ändamålsenlig behörighetstilldelning samt en tydlig och enhetlig process för tilldelning av behörigheter. Det är lämpligt att dokumentera processen i en arbetsbeskrivning eller i ett rutindokument.

För att förvaltningen ska kunna bedöma riskerna för de registrerades integritet utifrån tilldelade behörigheter så behövs det även kunskap om i vilken omfattning åtkomst ges till de registrerades/klienternas personuppgifter. Eftersom det för dataskyddsombudet är oklart huruvida denna kunskap finns inom förvaltningen rekommenderas det att omfattningen av åtkomsten till de registrerades/klienternas personuppgifter ses över.

Det är även viktigt för förvaltningen att beakta att ju vidare teknisk behörighet en medarbetare har i ett system desto viktigare blir det att klargöra för dem när det får anses tillåtet att ta del av information i systemet, exempelvis genom arbetsinstruktioner eller en rutin.

Beslut om behörighet

Förvaltningen uppger att det inte finns något formellt beslut om vem som har befogenhet att fatta beslut om att tilldela behörigheter inom avdelningen Vuxen och försörjningsstöd och frågan har lyfts till avdelningsledningsgrupp.

Dataskyddsombudet rekommenderar förvaltningen att bestämma vilka funktioner som ska ha befogenhet att besluta om behörighetstilldelning. Vilka som får fatta besluten bör sedan lämpligen framgå av dokumentationen kring processen för tilldelning av behörigheter.

Uppföljning av behörighet

Förvaltningen har en rutin för egenkontroll av användarbehörigheter i Treserva. Syftet med rutinen är att se till att rätt personer har behörigheter till rätt saker och att bland annat ändrade användare följer med i systemet. Syftet är också att begränsa behörigheter för att säkerställa den registrerades integritet. Listor med behörigheter tas ut per enhet och dessa skickas till ansvarig enhetschef. Enhetschefen återkopplar till central LVS om förändringar skett i bemanningen, så som att någon medarbetare slutat eller tillkommit.

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

Resultatet av uppföljningen stäms av och uppdateras i Treserva av central LVS. Central LVS är tillsammans med enhetscheferna ansvariga för att genomföra genomgången av samtliga användare i förvaltningen en gång per år.

Avseende behörigheter tilldelade till medarbetare på Intraservice kan förvaltningen inte själv kontrollera dessa utan uppgifter måste begäras ut från Intraservice.

Dataskyddsombudet ser det som positivt att förvaltningen infört en rutin avseende regelbunden behörighetskontroll. Att följa upp tilldelade behörigheter utgör en viktig del av arbetet med behörighetsstyrning, då det syftar till att upptäcka och motverka obehörig åtkomst. Eftersom rutinen infördes under 2022 rekommenderar dataskyddsombudet förvaltningen att följa upp hur genomförandet av behörighetskontroller har fungerat samt att utvärdera om kontrollerna behöver ske oftare än en gång per år. En risk om behörigheterna kontrolleras och uppdateras alltför sällan är att en medarbetare kan ha kvar en behörighet i systemet trots att hen inte längre ska ha den tilldelade behörigheten, exempelvis om hen får en ny roll inom organisationen.

Åtkomstkontroll/kontroll av loggar

Förvaltningen har en rutin för stickprovskontroll av händelselogg i Treserva. Syftet med att genomföra stickprovskontrollerna är att granska att medarbetare endast är inne i ärenden som är relevanta för att kunna utföra sitt arbete och att minska risken för att medarbetare tar del av mer information än nödvändigt. I förlängningen sker detta för att följa lagstiftningen och att säkerställa den registrerades integritet. Central LVS beställer en gång per kvartal händelselogg för tre dagar avseende tre slumpmässigt utvalda ärendenummer för avdelningen Vuxen och försörjningsstöd. Urvalet görs via Treserva och ska vara helt slumpmässigt. Händelseloggar begärs ut från Intraservice och granskas därefter av enhetschef. Loggarna granskas med utgångpunkt i vem/vilka som är berörda handläggare och eventuell utförare. Vid misstanke om oegentligheter tar enhetschef ställning till åtgärder.

Det finns även tekniska förutsättningar i Treserva att granska en specifik användare/handläggare. Om en handläggare väljs ut till granskning på grund av misstanke om oegentligheter ska enhetschef först ha samtal med berörd medarbetare och informera om att granskningen kommer att genomföras.

Dataskyddsombudet tycker att det är mycket positivt att förvaltningen infört en rutin avseende stickprovskontroll av händelselogg. Förutom uppföljning av tilldelade behörigheter är logg- och åtkomstkontroller viktiga redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. Eftersom även denna rutin infördes under 2022 rekommenderar dataskyddsombudet förvaltningen att följa upp hur genomförandet av stickprovskontrollerna har fungerat, samt att utvärdera om det är ett lagom antal kontrollerna som genomförs. Dataskyddsombudet vill även påminna om att det är viktigt att informera berörda medarbetare om rutinen för stickprovskontroller och att säkerställa att kontrollerna inte inskränker medarbetarnas integritet på ett oproportionerligt sätt.

Personuppgiftsbiträdet

Förvaltningen anger att relationen med Intraservice endast är reglerad i Regler för kommungemensamma interna tjänster. Förvaltningen har inte lämnat några instruktioner eller liknande anvisningar till Intraservice.

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 har inte genomfört någon konsekvensbedömning av behandlingarna i Treserva utan detta är del av den ”konsekvensbedömningsskuld” som kvarstår.

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.

Sammanfattade rekommendationer

- Förvaltningen rekommenderas att säkerställa att det finns en ändamålsenlig behörighetstilldelning samt en tydlig och enhetlig process för tilldelning av behörigheter.
- Förvaltningen rekommenderas att bestämma vilka funktioner som ska ha befogenhet att besluta om behörighetstilldelning.
- Förvaltningen rekommenderas att följa upp hur genomförandet av behörighetskontroller har fungerat samt utvärdera om kontrollerna behöver ske oftare än en gång per år.
- Förvaltningen rekommenderas att följa upp hur genomförandet av stickprovskontroller har fungerat samt att utvärdera om det är ett lagom antal kontroller som genomförs.
- 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)

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

- 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 avdelningen Vuxen 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 avdelningen Vuxen 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 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 av avdelningen Vuxen och försörjningsstöd?
- Hur många registrerades personuppgifter hanteras i Treserva med anledning av ärenden som avdelningen handlägger? Ange antalet registrerade som har öppna ärenden hos avdelningen under maj månad 2022 samt antalet registrerade i avdelningens 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 avdelningens ärenden i Treserva. Specificera svaret så att det framgår hur många som arbetar på avdelningen 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.