Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Socialförvaltningen Hisingen

2022-12-23

Innehåll

1 Dataskydd i kommunal verksamhet

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

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

1.1 Göteborgs Stads dataskyddsombud

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

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

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

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

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

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

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

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

2.2 Fördjupad kontroll

2.2.1 Kontroll av behörighetsstyrning 2022

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

I avstämning med verksamheten har tjänstepersoner angett att de har informerat vid förvaltningens interna informationssäkerhetsråd om vikten av att informera alla medarbetare om vilka regler som gäller för slagningar i Treserva. Det har under

hösten förekommit personuppgiftsincidenter, när medarbetare har gjort otillåtna slagningar i IT-system. Förvaltningen anger att de kommer att informera nämnden om förekomsten av incidenter i sin delårsrapport.

Dataskyddsombudets kommentarer:

Med anledning av den information som förvaltningen har lämnat rekommenderar dataskyddsombudet förvaltningen att utreda om den nuvarande behörighetstilldelningen till avdelningens ärenden i Treserva, medför en hög risk för personuppgiftsincidenter. Detta såväl utifrån de behörigheter som innebär att medarbetare kan se men inte öppna ärenden, som behörigheter att arbeta i ärenden. Förvaltningen rekommenderas att ta fram och dokumentera rutiner för att med viss regelbundenhet kontrollera att aktiva behörigheter är korrekta utifrån varje medarbetares anställning och arbetsuppgifter. Förvaltningen rekommenderas att följa upp inträffade incidenter och ta ställning till om nuvarande behörighetstilldelning till avdelningens ärenden i Treserva medför en hög risk för obehörig åtkomst till personuppgifter. Förvaltningen rekommenderas att säkerställa att berörda medarbetare informeras om gällande rutiner för uppföljning och kontroll av loggar.

Mer om kontrollen finns att läsa i bilaga till årsrapporten.

2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har valt att följa upp verksamhetens arbete med dataskyddsorganisation, eftersom dataskyddsombudets rekommendation från våren 2021 endast delvis har omhändertagits. Verksamheten har besvarat en kort enkät med frågor om vilka åtgärder som har vidtagits med anledning av dataskyddsombudets lämnade rekommendationer om att säkerställa att de personer som involveras i dataskyddsarbetet har tillräckligt med tid för arbetet för arbetet med dataskyddsorganisation. Samt om att ta fram en tydligare metod för att identifiera och bedöma risker utifrån de krav som ställs i dataskyddsförordningen och brottsdatalagen, med fokus på de registrerades rättigheter men också vad identifierade risker skulle kunna medföra för konsekvenser för organisationen

Verksamheten har uppgett att förvaltningens informationssäkerhetsråd i juni 2022 fattat beslut om en ny dataskyddsorganisation. Syftet med den nya organisationen uppges vara att ta fram fler resurser som kan arbeta med dataskyddsarbetet och för att säkerställa att resurserna har tillräckligt med tid för att kunna arbeta med dataskydd. Av verksamhetens svar framgår vilka arbetsuppgifter som tilldelats den utvecklingsledare inom informationssäkerhet och dataskydd som anställdes under hösten 2022. Vidare anges att två nya befattningar har tilldelats plats i informationssäkerhetsrådet. Därtill har det fortsatta arbetet med personuppgiftsincidenter bland annat inneburit att förvaltningens process för handläggning av incidenter implementerats i organisationen genom APT-material. Förvaltningen har även tagit fram ett styrande dokument för sin dataskyddsorganisation. I detta finns bland annat beskrivet ansvaret för att inleda konsekvensbedömningar samt vilka roller som har vilket ansvar dessa har i det

arbetet. Förvaltningen uppger i sina svar att de registrerades rättigheter stärks, genom att kravet på och arbetet med konsekvensbedömningar av nya och pågående personuppgiftsbehandlingar på detta sätt har tydliggjorts.

Dataskyddsombudets kommentarer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om inget särskilt föranleder att det behöver följas upp separat.

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 Hisingens 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:

På fem av de sex frågorna under denna kontrollpunkt har verksamheten angett att påståendena *stämmer bra* eller *stämmer helt*. På påståendet om att dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten har verksamheten svarat *stämmer inte bra*. Sammantaget indikerar verksamhetens skattning att det inte finns direkta risker identifierade. Samtidigt är risken som relaterar till huruvida dataskydd är en integrerad del i det dagliga arbetet en risk som bör åtgärdas, framför allt med hänsyn till dess påverkan på andra kontrollpunkter.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete avsevärt förbättrats sedan föregående år. Enligt skattningen har verksamheten en i flera delar fungerande intern dataskyddsorganisation. Ett fortsatt utvecklingsarbete behövs dock för att göra dataskydd till en naturlig och integrerad del i det dagliga arbetet i alla delar i verksamheten. Av den redovisning som förvaltningen skickat in med anledning av dataskyddsombudets uppföljning av 2021 års fördjupade kontroll framgår bland annat att förvaltningen genomfört organisationsförändringar och utbildningsinsatser. I avstämning med verksamheten har tjänstepersoner angett att en av de åtgärder som genomförts är att involvera förvaltningens verksamhetsutvecklare i arbetet med att säkerställa följsamhet till GDPR. Förvaltningen planerar att efter årsskiftet genomföra implementering av det arbete som planerats under året. Vidare har information till chefer gått ut och förvaltningen bedömer att de omhändertagit dataskyddsombudet rekommendationer under året.

Dataskyddsombudet delar förvaltningens uppfattning att dokumenterade arbetssätt och rutiner för dataskyddsarbetet är en viktig del. Samtidigt framgår av förvaltningens beskrivning att ett omfattande arbete med implementering av nya

arbetssätt kvarstår. Därför anser dataskyddsombudet att det fortfarande föreligger vissa risker inom kontrollpunkten. Dataskyddsombudet delar alltså inte tillfullo förvaltningens skattning. Det är viktigt att förvaltningens medarbetare vet hur de ska hantera personuppgifter och vart de kan vända sig med frågor. Det är också viktigt att verksamheten har tydliga rutiner för att säkerställa att dataskyddsombudet involveras i dataskyddsarbetet, avsett var i verksamheten dataskyddsfrågor förekommer.

Dataskyddsorganisationen var föremål för en fördjupad kontroll under våren 2021, vilken har följts upp under hösten 2022. Förvaltningens svar framgår under avsnitt 2.2.2.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Verksamheten har på samtliga de åtta påståendena om personuppgiftsincidenter angett att påståendena *stämmer bra* eller *stämmer* helt. Verksamheten har angett att cirka 100 procent av incidenterna från det senaste året har rapporterats till tillsynsmyndigheten i tid. Sammantaget indikerar skattningen att det inte finns några direkta risker av betydelse identifierade och att verksamheten har ett systematiskt dataskyddsarbete inom detta område.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med personuppgiftsincidenter förbättrats sedan tidigare år. I avstämning med verksamheten har tjänstepersoner angett att de arbetat med att förenkla och tydliggöra anmälan av personuppgiftsincidenter genom att ta fram blanketter och i så stor utsträckning som möjligt använda befintliga verksamhetssystem. Det APT-material som tagits fram har gått ut till chefer, på enhetschefsnivå.

Dataskyddsombudet ser positivt på förvaltningens arbete med att informera om och förenkla anmälningsförfarandet för personuppgiftsincidenter. Mot bakgrund av verksamhetens skattning under föregående kontrollpunkt (dataskyddsorganisationen) vill dataskyddsombudet dock påtala följande. Eftersom verksamheten angett att dataskydd inte är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten föreligger sannolikt risker också i relation till arbetet med personuppgiftsincidenter. Trots att verksamheten svarat att de till stor del informerar medarbetare om vad personuppgiftsincidenter är och dokumenterar inträffade incidenter, ser dataskyddsombudet risker med att incidenter inte identifieras och därmed heller inte dokumenteras och anmäls till tillsynsmyndigheten.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Dataskyddsombudets kommentarer:

Verksamheten har på fem av sex frågor svarat att påståendet *stämmer bra.* Den sjätte frågan avser med hur stor andel personuppgiftsbiträden som verksamheten har tecknat personuppgiftsbiträdesavtal. På denna fråga har verksamheten angett samma svar som föregående år, cirka 50 procent. Sammantaget indikerar skattningen att det finns risker identifierade som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. I avstämning med verksamheten har tjänstepersoner angett att kartläggning och diarieföring av biträdesavtal och andra överenskommelser pågår. För gemensamma system är Intraservice i flera delar ansvariga för att teckna avtal med personuppgiftsbiträden och i dessa relationer har verksamheten begränsad insyn.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med biträdesavtal avsevärt förbättrats sedan föregående år. Dataskyddsombudet har under året inte varit involverad i verksamhetens arbete med biträdesavtal och andra överenskommelser, varför dataskyddsombudet heller inte har någon insyn i arbetet. Mot bakgrund av verksamhetens resultat föregående år då skattningen indikerade att det inom denna kontrollpunkt fanns omfattande risker som kräver omgående åtgärder, ser dataskyddsombudet mycket positivt på den utveckling som uppges ha skett inom verksamheten. Samtidigt är det fortsatta arbetet med att säkerställa att biträdesavtal och andra nödvändiga överenskommelser tecknas ett arbete som bör prioriteras. Dataskyddsombudet vill även påminna om det arbete som förvaltningen i egenskap av personuppgiftsansvarig alltid förväntas göra, oavsett om en annan förvaltning i staden har ansvar för att drift av ett system eller tillhandahålla en tjänst. I de delar som förvaltningen inte får den information som efterfrågas, från biträden eller underbiträden, rekommenderas förvaltningen att i vart fall dokumentera vilken information som har efterfrågats och varför den inte har kommit förvaltningen till del.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även

verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Verksamheten har på fyra av fem frågor under denna punkt skattat att arbetet i stort är väl fungerande. På frågan om hur stor andel av verksamhetens personuppgiftsbehandlingar som finns dokumenterade i personuppgiftsregistret har verksamheten svarat cirka 75 procent, vilket är en förbättring sedan föregående år då verksamheten angett cirka 50 procent. Andelen av dessa som innehåller all den information som krävs enligt art. 30 GDPR har verksamheten också i år angett cirka 75 procent. Kvarstående risker avser avsaknad av fungerande rutiner för att kontinuerligt uppdatera registret. Sammantaget indikerar verksamhetens skattning att det finns risker som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med personuppgiftsregister avsevärt förbättrats sedan tidigare år. Det finns dock enligt skattningen ett fortsatt behov av att arbeta med att upprätta rutiner för att tillförsäkra att registret regelbundet uppdateras och att det finns särskilt utpekade ansvariga för uppgiften. Dataskyddsombudet noterar också att den förteckning över personuppgiftsbehandlingar som finns i systemstödet Draft-it under året har uppdaterats med endast en behandling. Av vad som går att utläsa i Draft-it saknas information enligt art. 30 i samtliga behandlingar. Oavsett om verksamheten använder Draft-it eller inte, behöver verksamheten säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret och att all nödvändig information läggs in i registret.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Verksamheten har på sex av sju frågor under denna punkt svarat att påståendet *stämmer bra* eller *stämmer helt*. På den av dessa frågor som avser hur stor del av verksamhetens informationstillgångar som har identifierats och värderats utifrån stadens informationsklassning har verksamheten angett cirka 75 procent. Detta kan jämföras med förra årets svar, då verksamheten angett cirka 25 procent. Kvarvarande risker har identifierats utifrån att verksamheten ännu inte genomför regelbundna interna kontroller för att säkerställa efterlevnad av GDPR. Sammantaget indikerar skattningen att det inte finns några direkta risker av betydelse identifierade och att verksamheten har ett systematiskt dataskyddsarbete.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med övergripande strategi för dataskydd avsevärt förbättrats sedan föregående år. Utifrån den kännedom om verksamhetens övergripande strategi för dataskydd som dataskyddsombudet har fått genom de månatliga avstämningar som hållits under våren 2022 framstår verksamhetens skattning som allt för positiv. I avstämning med verksamheten har tjänstepersoner angett att riktlinjer för dataskyddsarbetet har tagits fram (jmf kontrollpunkt 1) och att verksamheten numera har en plan för det fortsatta arbetet med att identifiera och värdera informationstillgångar. Vidare har verksamhetsutvecklare involverats även i detta arbete (jmf kontrollpunkt 1 och 2). Tjänstepersonerna har vidare uppgett att det arbete som avser systemstödet Treserva samt den användning av Microsofts tjänster som förekommer ännu inte har genomförts. Vad gäller Treserva inväntar förvaltningen en planering för att genomföra arbetet i samverkan med övriga socialtjänstförvaltningar. Vad gäller Microsoft tjänsters inväntar förvaltningen det arbete som Intraservice annonserat att de ska genomföra för att klargöra dels hur tjänsterna är uppbyggda och vilka personuppgiftsbehandlingar som förekommer, dels vilka eventuella risker som finns för den behandling av personuppgifter som förekommer i tjänsterna.

Trots detta arbete bedömer dataskyddsombudet att det inom kontrollpunkten inte är tillräckligt att riktlinjer har tagits fram och kartläggning påbörjats för att risker ska anses omhändertagna. Därtill kvarstår, utifrån vad dataskyddsombudet förstår, ett omfattande arbete med att kartlägga informationstillgångarna i Treserva och Microsoft, vilket torde utgöra en betydande andel av verksamhetens informationstillgångar. Sammantaget delar dataskyddsombudet inte till fullo verksamhetens skattning av arbetet inom kontrollpunkten.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Verksamheten har på tre av fem frågor svarat att påståendena *stämmer bra*. Kvarstående risker finns relaterat till brist på rutiner för kartläggning och uppföljning av medarbetares kunskapsnivå inom dataskydd. Sammantaget indikerar skattningen att det finns risker identifierade som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. I avstämning med verksamheten har tjänstepersoner angett att informationsinsatser har genomförts bland annat genom att artiklar har publicerats på intranätet och att utskick har gjort till chefer om vikten av att säkerställa att deras medarbetare tar till sig den publicerade informationen. Ett material för APT-utbildning om hantering av personuppgiftsincidenter har också tagits fram av förvaltningens tjänstepersoner.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med utbildning avsevärt förbättrats sedan tidigare år. Eftersom verksamhetens

skattning föregående år indikerade omfattande risker som kräver omgående åtgärder, ser dataskyddsombudet mycket positivt på att verksamheten arbetat med att utveckla arbetet inom kontrollpunkten. Samtidigt finns anledning att anta att verksamhetens skattning föregående år inte till fullo motsvarade de faktiska förhållandena, varför dataskyddsombudet ser att skillnaden i skattning likväl kan bero på att årets skattning ger en mer rättvisande bild av verksamhetens arbete.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser måste verksamheten kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

2.4.7 Kontrollpunkt 7: Integritetspolicy

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

Dataskyddsombudets kommentarer:

Verksamheten har på fem av fem påstående svarat *stämmer helt* eller *stämmer bra*. Sammantaget indikerar skattningen att inga direkta risker av betydelse är identifierade och att verksamheten har ett systematiskt dataskyddsarbete.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med integritetspolicy avsevärt förbättrats sedan föregående år. Utifrån dataskyddsombudets kännedom om de uppdateringar som gjorts av integritetspolicyn ser dataskyddsombudet att verksamheten arbetat framgångsrikt med kontrollpunkten.

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:

För tre av åtta påståenden har verksamheten angett *stämmer helt* eller *stämmer bra.* Kvarstående risker har koppling till avsaknad av aktuell och fastställd dokumenthanteringsplan och rutiner för att informera om och kontrollera

dokumenthantering och gallring av handlingar som innehåller personuppgifter. Enligt verksamhetens skattning har cirka 75 procent av verksamhetens personuppgiftsbehandlingar informationsklassificerats och för samma andel uppges klassificeringen vara aktuell. Detta kan jämföras med föregående år då verksamheten angav att cirka 25 procent av personuppgiftsbehandlingarna klassificerats och att i stort sett inte någon av behandlingarna kontrollerats utifrån korrekthet under året 2021.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete avsevärt förbättrats sedan föregående år. Årets skattning indikerar sammantaget att det finns risker identifierade som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. Dataskyddsombudet bedömer ändå att det är viktigt att förvaltningen säkerställer att det finns en dokumenthanteringsplan som omfattar alla verksamhetens processer och att det finns rutiner för att kontrollera att gallring av handlingar som innehåller personuppgifter sker på rätt sätt. Det är också viktigt att se till så att alla medarbetare har kunskap om förvaltningens dokumenthantering och gallringsbestämmelser. Detta arbete bör enligt dataskyddsombudet prioriteras eftersom det inte bara är en fråga om dataskydd, utan även handlar om efterlevnad av arkivlag, regler om sekretess med mera.

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 på 11 av 14 frågor angett att påståendet *stämmer bra* eller *stämmer helt*. Kvarvarande risker finns vad gäller rutin eller metodstöd för att inhämta registrerades synpunkter när en konsekvensbedömning genomförs. Andelen av verksamhetens personuppgiftsbehandlingar som analyserats utifrån risk uppges vara cirka 50 procent. Andelen personuppgiftsbehandlingar som konsekvensbedömts uppges vara cirka 75 procent. Andelen av verksamhetens personuppgiftsbehandlingar där konsekvensbedömning planeras uppges vara cirka 50 procent. Detta är en betydande förbättring från föregående år, då verksamheten angav att andelen riskbedömda personuppgiftsbehandlingar var cirka 25 procent och andelen behandlingar som konsekvensbedömts cirka 25 procent. Sammantaget indikerar skattningen för 2022 års arbete att det finns risker identifierade som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga.

Dataskyddsombudet ser positivt på verksamhetens arbete med att utveckla sitt arbete med konsekvensbedömningar. Samtidigt finner dataskyddsombudet anledning att ifrågasätta förvaltningens skattning av andelen personuppgiftsbehandlingar som konsekvensbedömts. Detta utifrån att verksamhetens skattning skiljer sig avsevärt mellan innevarande och föregående år.

Också utifrån den information dataskyddsombudet har om hur långt förvaltningen har kommit i att identifiera och värdera informationstillgångar i Treserva och Microsofts tjänster (jmf kontrollpunkt 5). Att verksamheten under 2022 har gått från att endast 25 procent till 75 procent av verksamhetens personuppgiftsbehandlingar konsekvensbedömts förefaller osannolikt. Detta också mot bakgrund av antalet konsekvensbedömningar som dataskyddsombudet lämnat rekommendationer för till verksamheten under 2022.

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. Det är därför mycket viktigt att verksamheten ser till så att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingar samt att konsekvensbedömningar genomförs. Verksamheten måste se till så att dataskyddsombudet även involveras och får möjlighet att lämna synpunkter i de fall beslut fattas att inte genomföra en konsekvensbedömning, och inte enbart när konsekvensbedömning ska genomföras.

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 för tre av de fem påstående angett *stämmer bra*. Risker kvarstår enligt verksamhetens skattning vad gäller att kravställning i upphandling ännu inte omfattar inbyggt dataskydd och dataskydd som standard. Sammantaget indikerar skattningen att det finns risker identifierade som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. I avstämning med verksamheten har tjänstepersoner angett att de hoppas på en större samordning i arbetet med IT-projekt och upphandling efter den omorganisering som sker vid årsskiftet 2022/23 (projekt STADIG).

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med IT-projekt och upphandling avsevärt förbättrats sedan föregående år. För år 2021 besvarades samtliga frågor med *stämmer inte alls*. Eftersom verksamhetens skattning föregående år indikerade omfattande risker som kräver omgående åtgärder, ser dataskyddsombudet mycket positivt på att verksamheten arbetat med att utveckla arbetet inom kontrollpunkten. Samtidigt finns anledning att anta att verksamhetens skattning föregående år inte till fullo motsvarade de faktiska förhållandena, varför dataskyddsombudet ser att skillnaden i skattning likväl kan bero på att årets skattning ger en mer rättvisande bild av verksamhetens arbete.

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 besvarat samtliga åtta frågor med *stämmer bra* eller *stämmer helt*. Sammantaget indikerar skattningen att inga direkta risker av betydelse är identifierade och att verksamheten har ett systematiskt dataskyddsarbete.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete avsevärt förbättrats sedan föregående år. Utifrån den kännedom om verksamhetens arbete som dataskyddsombudet har fått genom de månatliga avstämningar som hållits under våren 2022 framstår verksamhetens skattning som allt för positiv. Det har inte framkommit att verksamheten har kartlagt och sammanställt information om samtliga IT-system, kommunikationskanaler och digitala verktyg som verksamheten använder. Inte heller att en översyn gjorts över om behörigheter i IT-system är anpassade utifrån vad medarbetare behöver ha tillgång till för sitt arbete. Under året har dataskyddsombudet genomfört en fördjupad kontroll av verksamhetens arbete med behörighetsstyrning i Treserva. Mer om kontrollen finns att läsa under avsnitt 2.2.1 samt i bilaga till årsrapporten. För rekommendationer inom kontrollpunkten hänvisas till bilaga 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 för fyra av sju påståenden angett *stämmer bra* eller *stämmer helt*. Risker kvarstår relaterat till att det ännu saknas en utbredd medvetenhet om registrerades rättigheter hos medarbetare i verksamheten. På de två frågor som rör detta ämne har verksamheten svarat *stämmer inte bra*. Vidare saknas i verksamheten dokumenterade rutiner för tillbakadragande av samtycke från en registrerad. Sammantaget indikerar skattningen att inga direkta risker av betydelse är identifierade. I avstämning med verksamheten har tjänstepersoner angett att det hos medarbetare inom förvaltningen finns bred kunskap om sekretess, vilket leder till att medarbetare har goda förutsättningar att också behandla personuppgifter och registrerades rättigheter på ett bra sätt. Vidare anger tjänstepersonerna att

förvaltningens egna jurister regelbundet ger utbildningar till medarbetare om sekretess.

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete med registrerades rättigheter avsevärt förbättrats sedan föregående år. Samtidigt kvarstår behov för verksamheten att öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas. Verksamheten behöver även säkerställa att det finns rutiner för att hantera situationen då ett samtycke från en registrerad dras tillbaka. Dataskyddsombudet rekommenderar därför förvaltningen att säkerställa att de utbildningar som medarbetare ges också omfattar GDPR-specifika kunskaper som medarbetare behöver för att kunna tillgodose registrerades rättigheter.

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 1 och 5: Dataskyddsorganisation och övergripande strategi för dataskydd
- Kontrollpunkt 6, 8 och 12: Utbildning, dokumenthantering och registrerades rättigheter

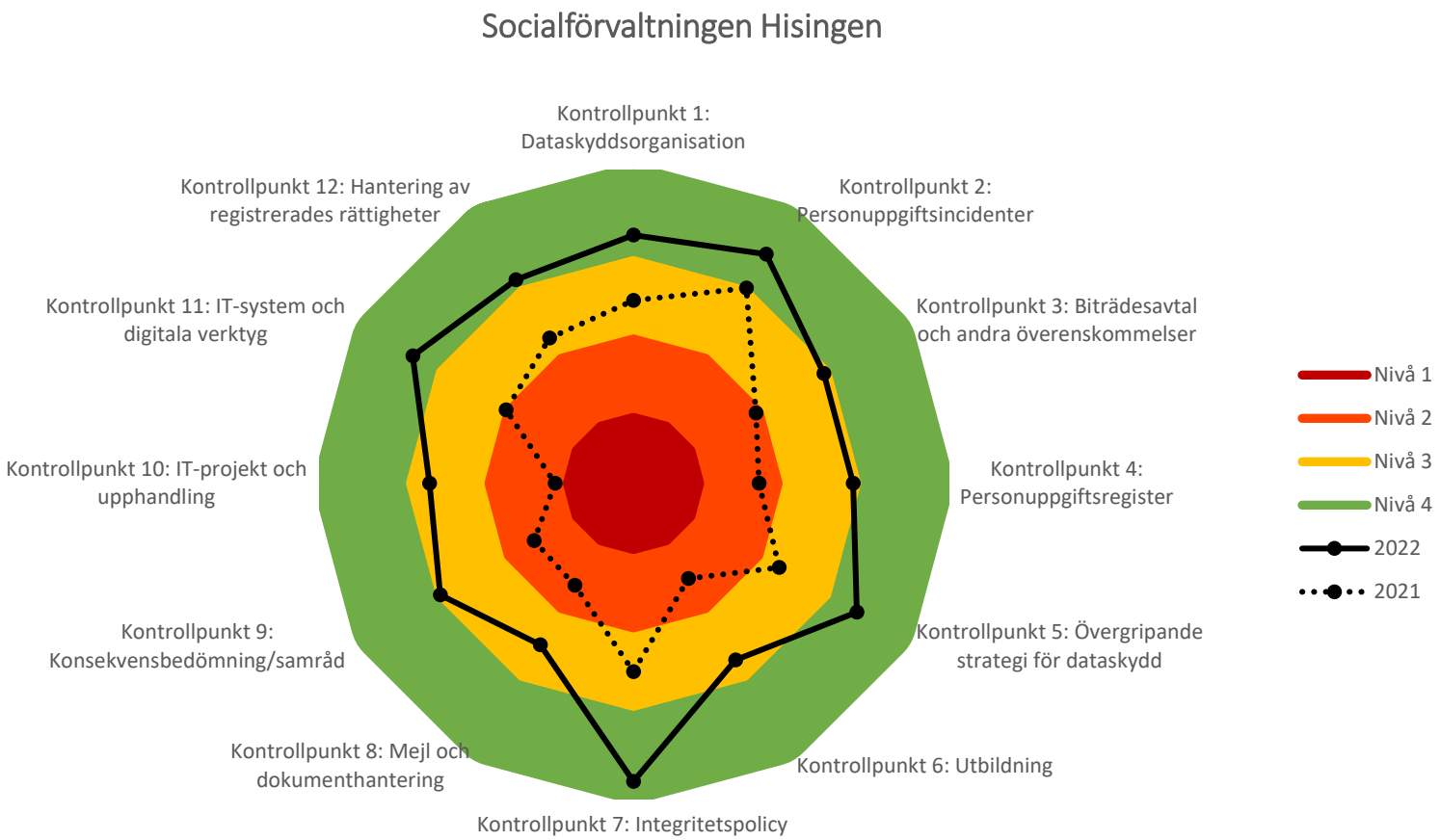
Av enkätsvaren framgår att man inom socialförvaltningen Hisingen i stort bedömer dataskyddsarbetet fungerar väl. Kontrollpunkterna 6, 8 och 10 har genererat de högsta riskvärdena i årets skattning. Trots detta resultat bedömer dataskyddsombudet att det finns anledning, utifrån att verksamheten ska arbeta riskbaserat, att framför allt prioritera arbetet med att implementera verksamhetens nya arbetssätt och rutiner för den interna dataskyddsorganisationen och det övergripande strategin för dataskyddsarbetet. Vidare har som framgått ovan, dataskyddsombudet i vissa delar en annan syn på hur långt förvaltningen har kommit i olika delar av dataskyddsarbetet. Det är dataskyddsombudets bedömning att ett arbete med att implementera den interna dataskyddsorganisationen och strategin för dataskydd sannolikt får effekt också på flera av de kontrollpunkter som dataskyddsombudet bedömer att förvaltningen behöver arbeta mer med för att minimera risker för de registrerade. Därtill ser dataskyddsombudet att det även framgent bör prioriteras att arbeta med utbildning, dokumenthanteringsplan, och de registrerades rättigheter, kontrollpunkterna 6, 8 och 12. Dataskyddsombudet bedömer att även ett sådant arbete sannolikt leder till att risker inom flera kontrollpunkter kommer att bli lägre.

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.



Bilaga 2: Fördjupad kontroll

Behörighetsstyrning socialnämnden Hisingen

Bakgrund

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

Granskningen har gjorts med utgångspunkt i artikel 32 i dataskyddsförordningen (GDPR) som handlar om lämpliga tekniska och organisatoriska säkerhetsåtgärder vid personuppgiftsbehandling. Vid bedömningen av lämplig säkerhetsnivå ska hänsyn tas till bland annat risken för obehörig åtkomst till personuppgifter. Behörighetsstyrning 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

Förvaltningen har uppgett att de flesta kategorier av personuppgifter behandlas i Treserva av avdelning försörjningsstöd, bland dessa förekommer ofta såväl känsliga som extra skyddsvärda personuppgifter. I avdelningens ärenden i Treserva behandlas uppgifter om klienters namn, personnummer/samordningsnummer, adressuppgifter, telefonnummer, e-postadress, uppgift om barn, uppgift om sociala förhållanden, uppgift om ekonomiska förhållanden, uppgift om hälsa. Även uppgifter om sexualliv och sexuell läggning, etniskt ursprung, religiös eller filosofisk övertygelse, politisk åsikt förekommer.

Vad gäller omfattningen registrerade i avdelningens ärenden i Treserva har förvaltningen angett att de endast kan söka fram antalet ärenden och antalet så kallade *huvudpersoner* i ett ärende. Samma klient kan dock ha flera ärenden och i ett ärende kan fler registrerade än *huvudpersonen* förekomma. Därutöver är 380 av avdelningens ärenden skyddade och för dessa är det inte möjligt att se antalet unika huvudpersoner. Det totala antalet registrerade personer är därför inte möjligt att ange exakt. Förvaltningen har uppgett att antalet registrerade *huvudpersoner* i pågående ärenden under maj månad 2022 var cirka 2 812. Antalet registrerade *huvudpersoner* i avslutade ärenden på avdelningen var vid samma tidpunkt cirka 11 714.

Förvaltningen har uppgett att totalt 304 medarbetare har åtkomst till avdelningens ärenden i Treserva. Av dessa utgör 136 personer medarbetare inom avdelning *försörjningsstöd*, 73 personer är medarbetare inom avdelning *vuxen* och 68 personer är medarbetare inom avdelning *barn och unga myndighet*. Därutöver utgör 27 personer övriga medarbetare så som exempelvis arkivarier, arkivassistenter, lokalt verksamhetsstöd, verksamhetskontroller, och administratörer.

Med anledning av de uppgifter som förvaltningen lämnat om att medarbetare inom socialförvaltningen Hisingen kan få sökträffar på klienter som har ärenden i stadens andra fem förvaltningar som arbetar i Treserva, vill dataskyddsombudet påtala följande. För de fall även det motsatta förhållandet gäller, att medarbetare vid stadens andra fem socialförvaltningar kan se, men inte öppna, ärenden i Treserva som tillhör socialförvaltningen Hisingen så omfattas ännu fler medarbetare av tillgång till personuppgifter i förvaltningens ärenden än vad som angetts ovan. Detta i de fall när det förekommer personuppgifter, direkta eller indirekta, i den vy som går att se för medarbetare som kan då sökträffar och se, men inte öppna, förvaltningens ärenden.

Behörighetsstruktur och roller i systemet

Förvaltningen har beskrivit de olika roller som finns i Treserva och vilka behörigheter respektive roll har. Exempel på roller är bland annat *handläggare* och *enhetschef*. Behörigheter tilldelas utifrån vilken information de olika rollerna behöver ha tillgång till i Treserva för att kunna utföra sitt arbete. Förvaltningen beskriver att detta görs genom att de olika rollerna tilldelas behörighetsprofiler med så kallade gruppfilter, utifrån vilka arbetsuppgifter en viss roll har. Gruppfiltret innebär att en medarbetares behörighet är begränsad till socialförvaltningen Hisingens ärenden i Treserva. Behörighetsprofiler tilldelas utifrån vilken befattning en medarbetare har, exempelvis *socialsekreterare* eller *administratör*. Behörighetsprofilen innebär att en handläggare kan läsa och dokumentera i vissa ärendetyper, exempelvis *ekonomiskt bistånd*. Därtill tilldelas även behörighet till exempelvis Treservas kronologiska pärm eller skyddade ärenden för medarbetare som arbetar i vissa grupper eller har vissa arbetsuppgifter.

Förvaltningen har inte identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter i Treserva inom avdelning försörjningsstöd. Förvaltningen har också uppgett att behandlingarna i Treserva inte har konsekvensbedömts. Förvaltningen uppger att de hoppas att projektet Stadig kommer att påskynda arbetet med konsekvensbedömning av behandlingarna i Treserva eftersom ansvarsförhållandena för personuppgiftsbehandlingar ska ses över i projektet.

Angående svårigheter i systemet att begränsa behörigheter har förvaltningen uppgett bland annat följande. Medarbetare inom socialförvaltningen Hisingen kan få sökträffar på klienter som har ärenden i stadens andra fem förvaltningar som arbetar i Treserva. Förvaltningen uppger att detta är en organisatorisk svårighet och inte ett hinder som är inbyggt i systemet Treserva. Förvaltningen beskriver att en anledning till att medarbetare kan se (men inte öppna) ärenden som handläggs av andra förvaltningar är att detta minskar risken för att ärenden hamnar mellan stolarna. Vidare är det en del av en socialtjänstutredning att kontrollera om en person redan förekommer som klient i kommunen. Att genomföra denna kontroll skulle bli avsevärt svårare om det inte var möjligt för medarbetare att se sådan förekomst direkt i Treserva. Förvaltningen anger

vidare att förvaltningsjuristerna på socialförvaltningarna, äldre-, vård och omsorgsförvaltningen och förvaltningen för funktionsstöd har uttalat att de inte ser att det är nödvändigt att förändra denna hantering utifrån sekretesslagstiftningen. Detta, uppger förvaltningen, betyder inte nödvändigtvis att en personuppgiftsbehandling som därmed sker över myndighetsgränserna är tillräckligt begränsad utifrån krav i dataskyddsförordningen. Däremot kan resonemanget användas för att argumentera för att behandlingen är nödvändig för att fullfölja förvaltningens uppdrag.

Förvaltningen har uppgett att det finns risker med att många medarbetare har behörighet att se försörjningsstödsärenden i Treserva. Exempelvis risk för röjande av personuppgifter eller sekretessbelagda uppgifter, om medarbetare läser mer information än de behöver för sitt arbete. För att framöver motverka det har förvaltningen tagit fram ett utkast till rutin för månadsvisa stickprovskontroller av händelseloggar i Treserva. Utöver detta har det, efter omorganisationen 2020/21, för allt fler ärenden bedömts att funktionen *lokalt skydd* i Treserva behövs. Denna funktion begränsar så att ett ärende endast är synligt för totalt tre medarbetare. Förvaltningen konstaterar därtill att det är svårt att motverka risker som ännu inte uppmärksammats. Därför utgör det en risk att det ännu inte finns riskanalyser eller konsekvensbedömningar för den behandling av personuppgifter som görs i Treserva.

Med anledning av vad som framkommit av förvaltningens svar om den tillgång till avdelningens ärenden som finns för förvaltningens egna medarbetare, så väl som den som eventuellt finns för samtliga medarbetare vid de förvaltningar i staden som använder Treserva, rekommenderar dataskyddsombudet förvaltningen att utreda hur denna behörighetstilldelning står sig i relation till dataskyddsförordningens krav om tillräckliga tekniska och organisatoriska åtgärder för att förhindra obehörig åtkomst till personuppgifter. Förvaltningen rekommenderas att utreda om den nuvarande behörighetstilldelningen till avdelningens ärenden i Treserva medför en hög risk för personuppgiftsincidenter, i form av obehörig åtkomst till personuppgifter.

Tilldelning av behörighet utifrån bedömning

Förvaltningen har uppgett att behörighetstilldelningen görs utifrån de rollerna som beskrivs ovan. Vilka behörigheter en viss roll får baseras på arbetsfördelning inom avdelningen och vilken information de olika rollerna behöver ha tillgång till för att handlägga ärenden/utföra sitt arbete.

Beslut om behörighet

Förvaltningen har uppgett att närmaste chef beslutar om sina medarbetares behörigheter. Chef eller personaladministratör gör beställning av behörighet till förvaltningens funktion lokalt verksamhetsstöd. Förvaltningsdirektör beslutar om den extra höga behörigheten till alla skyddade ärenden.

Uppföljning av behörighet

Förvaltningen uppger att de inte har identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter i Treserva inom avdelning försörjningsstöd.

Enligt vad förvaltningen uppger följs tilldelade behörigheter inte upp, utöver att ansvarig chef meddelar funktionen lokalt verksamhetsstöd (LVS) om en tilldelad behörighet behöver ändras eller tas bort, till exempel om en medarbetare byter befattning inom

förvaltningen eller avslutar sin tjänst. Ansvaret vilar på medarbetarens närmaste chef att meddela LVS.

Förvaltningen har vidare uppgett att det varje månad genomförs egenkontroll av att förvaltningens rutin för stickprov av attester och underlag för utbetalning av ekonomiskt bistånd följs. Därtill genomförs dagligen attestkontroller på ett antal ärenden i Treserva. En av de obligatoriska kontrollpunkterna vid attestkontroller är att kontrollera om beslut har fattats av behörig person med rätt delegation. Egenkontrollerna kan därmed leda till att den som genomför kontrollen uppmärksammar att de finns felaktigheter i behörigheterna till det ärende i Treserva som kontrolleras, uppger förvaltningen.

Dataskyddsombudet anser att det är bra att det finns utpekat ansvar för att säkerställa att en medarbetares behörighet tas bort i samband med att en medarbetares tjänst förändras. Samtidigt kan det finnas risker med ett sådant system, varför det kan finnas anledning att se över behovet av ytterligare uppföljning. Den uppföljning som förvaltningen beskriver att egenkontrollen innebär, ser dataskyddsombudet som otillräcklig för syftet att säkerställa att chefer följer rutinen om att meddela LVS när en medarbetares tjänst förändras. I stället ser dataskyddsombudet anledning att rekommendera förvaltningen att ta fram och dokumentera rutiner för att med viss regelbundenhet kontrollera att aktiva behörigheter är korrekta utifrån varje medarbetares anställning och arbetsuppgifter. Med hänsyn till att det är relativt vanligt att personer byter anställning inom de sex socialförvaltningarna anser dataskyddsombudet att det är extra viktigt att förvaltningen har tillräckliga rutiner för att säkerställa att medarbetare inte har obehörig åtkomst till personuppgifter genom att behörigheter som är inaktuella inte tas bort.

Åtkomstkontroll/kontroll av loggar

Det är, enligt förvaltningens bedömning, en risk att många medarbetare har behörighet att se försörjningsstödsärenden i Treserva och därmed har möjlighet att läsa sig till mer information än vad de egentligen behöver för sitt arbete. För att motverka detta kommer framöver stickprovskontroller att genomföras månadsvis i enlighet med en ny rutin. Förvaltningen har vidare uppgett att medarbetare utbildas i informationssäkerhet om det till exempel skett en incident eller om enhetschef/avdelningschef uppmärksammat ett behov av utbildning. Utöver detta har LVS-funktionen även sett en ökning av ärenden som behöver *lokalt skydd* i Treserva sedan omorganisationen till facknämnder 2020/21. Lokalt skydd innebär att LVS markerar ärendet så att det endast är synligt för högst tre handläggare. Ofta ges *lokalt skydd* för ärenden som tillhör klienter som inväntar att sekretessmarkering hos Skatteverket ska gå igenom. En ytterligare risk som förvaltningen anger är att det varken finns riskanalyser eller konsekvensbedömningar för personuppgiftsbehandlingarna i Treserva, eftersom det är svårt att motverka risker som ännu inte har uppmärksammats.

I avstämning med verksamheten har tjänstepersoner angett att de har informerat vid förvaltningens interna informationssäkerhetsråd om vikten av att informera alla medarbetare om vilka regler som gäller för slagningar i Treserva. Det har under hösten förekommit personuppgiftsincidenter, när medarbetare har gjort otillåtna slagningar i IT-system. Förvaltningen anger att de kommer att informera nämnden om förekomsten av denna typ av incidenter i sin delårsrapport.

Förvaltningen har angett att åtkomstkontroller/loggkontroller kan göras genom att funktionen LVS begär ut händelseloggar över slumpmässigt utvalda ärenden i Treserva från nämnden för Intraservice. För närvarande utförs dock inte några loggkontroller. Socialförvaltningen Hisingen har tagit fram ett utkast till rutin för loggkontroll, som kommer att börja användas när rutinen är fastställd. Av det utkast till ny rutin som dataskyddsombudet har tagit del av framgår att syftet med kontroll av händelseloggar i Treserva är att kontrollera att personal inte tar del av information i Treserva som personalen inte behöver för att kunna utföra sitt uppdrag. Vidare framgår av rutinen att en beställning av händelseloggar ska göras varje månad, genom ett särskilt beställningsformulär på Serviceportalen. Intraservice levererar den beställda händelseloggen till funktionen LVS i en excelfil som skickas via e-post.

Dataskyddsombudet ser positivt på att förvaltningen har tagit fram ett utkast till rutin för kontroll av händelseloggar i Treserva. Logg och åtkomstkontroller är viktiga redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. Kontrollerna behöver dock utföras på ett så icke-integritetskränkande sätt som möjligt för den anställde som kontrolleras. Den anställde ska också få information om vilka kontroller som görs av dennes arbete i Treserva. Dataskyddsombudet vill även påtala för förvaltningen att en framtida konsekvensbedömning av den personuppgiftsbehandling som omfattas av loggkontroller också bör omfatta de delar av behandlingen som sker i serviceportalen och via e-post, utifrån den beskrivning som framgår av förvaltningens utkast till ny rutin. Förvaltningen rekommenderas också att följa upp inträffade incidenter och ta ställning till om nuvarande behörighetstilldelning till avdelningens ärenden i Treserva medför en hög risk för obehörig åtkomst till personuppgifter.

Personuppgiftsbiträdet

Förvaltningen har uppgett att Intraservice löpande utför uppdateringar i systemet och agerar tekniskt stöd för socialförvaltningen när problem och/eller incidenter uppstår. I nuläget kontrollerar inte förvaltningen personuppgiftsbiträdets behörigheter i systemet, men anger att det förmodligen sker egenkontroller inom Intraservice organisation.

Förvaltningen har uppgett att instruktioner till personuppgiftsbiträdet inte har tagits fram. Anledningen till det uppges vara att det ännu inte har genomförts konsekvensbedömning och riskanalys av personuppgiftsbehandlingarna i Treserva. Dessutom, anger förvaltningen, finns det behov av att se över ansvarsförhållanden och hur dessa ska regleras, i och med att projektet Stadig genomförs. Det är först när detta är gjort som förvaltningen bedömer att riskbilden kan bli tydlig och som personuppgiftsansvarig kommer att veta vilka konkreta åtgärder som personuppgiftsbiträdet behöver vidta för att minska riskerna.

Dataskyddsombudet delar förvaltningens bedömning om att en konsekvensbedömning för de här aktuella behandlingarna är ett viktigt verktyg för att kartlägga risker. Dataskyddsombudet delar även förvaltningens bedömning att det finns ett behov av att utreda och reglera ansvarsförhållanden i och med projektet Stadig. Behovet av att kartlägga och utreda ansvar och risker har koppling till både förvaltningens möjligheter att ta det ansvar för sina personuppgiftsbehandlingar som följer av GDPR och särskild registerlagstiftning, samt möjligheter att vidta relevanta riskminimerande åtgärder för de aktuella behandlingarna.

Sammanfattade rekommendationer

- Förvaltningen rekommenderas att utreda om den nuvarande behörighetstilldelningen till avdelningens ärenden i Treserva, medför en hög risk för personuppgiftsincidenter. Detta såväl utifrån de behörigheter som innebär att medarbetare kan se men inte öppna ärenden, som behörigheter att arbeta i ärenden.
- Förvaltningen rekommenderas att ta fram och dokumentera rutiner för att med viss regelbundenhet kontrollera att aktiva behörigheter är korrekta utifrån varje medarbetares anställning och arbetsuppgifter.
- Förvaltningen rekommenderas att följa upp inträffade incidenter och ta ställning till om nuvarande behörighetstilldelning till avdelningens ärenden i Treserva medför en hög risk för obehörig åtkomst till personuppgifter.
- Förvaltningen rekommenderas att säkerställa att berörda medarbetare informeras om gällande rutiner för uppföljning och kontroll av loggar.

Bilagor – fördjupad kontroll behörighetsstyrning

Information om fördjupad kontroll 2022

Fördjupad kontroll 2022 (del 1)

Fördjupad kontroll 2022 (del 2)

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning

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

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

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

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

Tillvägagångssätt

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

Kontrollen begränsas till att endast avse tilldelning av behörigheter och åtkomst till Treserva för chefer och medarbetare vid avdelning 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/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 1)

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

Kontrollen begränsas till att endast avse tilldelning av behörigheter och åtkomst till Treserva för chefer och medarbetare vid avdelning 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/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 10 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 2)

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

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

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

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.