Tjänsteutlåtande
Utfärdat 2023-01-20
Diarienummer 1727/22

Handläggare
Mathias Henriksson
Telefon: 031-365 00 00 (växel)
E-post: mathias.henriksson@arbvux.goteborg.se

Information från nämndens dataskyddsombud om årsrapport för dataskyddsarbetet 2022

Förslag till beslut

Nämnden för arbetsmarknad och vuxenutbildning antecknar mottagandet av informationen till protokollet.

Sammanfattning

Nämnden för arbetsmarknad och vuxenutbildning är enligt nämndens reglemente personuppgiftsansvarig för de behandlingar av personuppgifter som sker i verksamheten. Dataskyddsombudets roll är att ge råd och information till den personuppgiftsansvarige. I uppdraget ingår även att följa upp att den personuppgiftsansvarige följer dataskyddslagstiftningen.

I det här ärendet informerar nämndens dataskyddsombud om dataskyddsarbetet under 2022, inklusive de fördjupade kontroller som genomförts under året samt uppföljning av dessa. De rekommendationer som dataskyddsombudet lämnat kommer tas om hand i förvaltningens fortsatta utvecklingsarbete inom dataskyddsområdet.

Bedömning ur ekonomisk dimension

I Sverige är Integritetsskyddsmyndigheten (tidigare Datainspektionen) ansvarig tillsynsmyndighet för att gällande dataskyddslagstiftning följs. Integritetsskyddsmyndigheten har ytterst getts rätt att besluta om sanktionsavgifter när reglerna inte följs. Hur hög sanktionsavgiften blir beror dels på vilken bestämmelse överträdelsen gäller, dels på omständigheterna i det enskilda fallet. Integritetsskyddsmyndigheten ska bland annat att titta på hur allvarlig överträdelsen är, hur stor skada som skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Dataskyddslagstiftningen är till för att skydda grundläggande rättigheter och friheter, särskilt enskildas rätt till skydd av sina personuppgifter. Grunden till enskildas integritetsskydd har även stöd i Europakonventionen, EU:s stadga om de grundläggande rättigheterna och den svenska regeringsformen. Som kommunal myndighet har Arbetsmarknad och vuxenutbildning generellt rätt att hantera enskildas personuppgifter

om det är nödvändigt för att utföra vårt myndighetsuppdrag, förutsatt att dataskyddsförordningens grundläggande principer i övrigt följs.

Samverkan

Information vid förvaltningens samverkansgrupp (FSG) den 31 januari 2023.

Bilagor

1. Årsrapport för dataskyddsarbetet 2022, 2022-12-22

Ärendet

I det här ärendet informerar nämndens dataskyddsombud om dataskyddsarbetet under 2022, inklusive fördjupade kontroller som genomförts samt uppföljning av dessa.

Beskrivning av ärendet

Dataskyddsförordningen ställer krav på att bland annat alla myndigheter och andra offentliga organ ska ha ett dataskyddsombud. Dataskyddsombudets roll är att ge råd och information till den personuppgiftsansvarige. I uppdraget ingår även att följa upp att den personuppgiftsansvarige följer dataskyddslagstiftningen genom att till exempel utföra kontroller på området. Däremot driver eller utför dataskyddsombudet inte själva arbetet med dataskydd, utan detta arbete utförs av förvaltningens egna medarbetare. I Göteborgs Stad är dataskyddsombuden organisatoriskt placerade på förvaltningen för Intraservice.

Enligt dataskyddsförordningen är personuppgiftsansvarig den som bestämmer för vilka ändamål uppgifter ska behandlas och hur behandlingen ska gå till. Nämnden är enligt kommunfullmäktiges beslutade reglemente personuppgiftsansvarig för de behandlingar av personuppgifter som sker i dess verksamhet. Med rollen som personuppgiftsansvarig följer en lång rad administrativa och säkerhetsmässiga krav för att uppfylla lagstiftningen på området.

I bifogad årsrapport informerar dataskyddsombudet om arbetet under 2022, och presenterar resultatet av de fördjupade kontroller av förvaltningens dataskyddsarbete som genomförts under året samt uppföljningen av dessa.

Förvaltningens bedömning

Bilaga 1 till årsrapporten visar resultat av fasta kontrollpunkter 2022 jämfört med 2021, där det framgår att förvaltningens dataskyddsarbete utvecklats positivt på samtliga kontrollerade områden.

De rekommendationer som dataskyddsombudet lämnat i årsrapport kommer tas om hand i förvaltningens fortsatta utvecklingsarbete inom området. Gällande tidigare lämnade rekommendationer från oktober 2022 om elevhanteringssystemet Alvis pågår ett arbete tillsammans med aktuell IT-leverantör och i samverkan med stadens fyra socialförvaltningar.

Andreas Lökholm
Förvaltningsdirektör

Maria Löfgren
HR- och kanslichef

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Förvaltningen för arbetsmarknad och vuxenutbildning

2022-12-22

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 GDPR
[2] Artikel 38.3 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

Den fördjupade kontrollen har bestått av en kontroll av förvaltningens behörighetsstyrning i systemet Alvis. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten för kontrollen haft vissa anmärkningar och därför lämnat ett antal rekommendationer till verksamheten för att förbättra arbetet med behörighetsstyrningen och säkerställa följsamhet mot GDPR.

Sammanfattande rekommendationer från kontrollen:

- Ta fram rutin för tilldelning och ändring av behörigheter
- Ta fram rutin för regelbunden uppföljning av tilldelade behörigheter

- Ta fram rutin för regelbunden åtkomstkontroll/kontroll av loggar
- Upphöra med informationsutbytet genom direktåtkomst i Alvis för socialtjänsten i enlighet med tidigare rekommendationer lämnade 2022-10-07
- Utreda Arbetsförmedlingens direktåtkomst i Alvis med utgångspunkt från rekommendationer lämnade 2022-10-07

2.2.2 Uppföljning av tidigare genomförda kontroller

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

Fördjupad kontroll (2021): Personuppgiftsbiträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

- Förvaltningen bör utreda behov av att ta fram rutiner för hur man gör bedömningen av om leverantör/annan part är personuppgiftsbiträde eller om man är gemensamt personuppgiftsansvarig.
- Förvaltningen bör utreda behov av att ta fram rutin för avtalsuppföljning.
- Förvaltningen bör ta fram rutiner/checklista för vad personuppgiftsbiträdesavtal/datadelningsavtal ska innehålla.
- Förvaltningen bör ta fram rutin eller tydliggöra hur redan existerande stöddokument ska användas vid säkerställande/uppföljning av ett biträdes tekniska och organisatoriska säkerhetsåtgärder.

Uppföljningen visar att verksamheten har tagit fram en ny anvisning kring personuppgiftsansvar och personuppgiftsbiträdesavtal som följs upp årligen samt att förvaltningen genomfört utbildning på temat för inköpsenheten. Inköpsenhetens uppdragsformulär har också kompletterats med fråga om den externa parten kommer att behandla personuppgifter, för att kunna uppmärksamma och bedöma personuppgiftsansvar. Förvaltningen har även inlett en omvärldsbevakning för att följa upp biträdes säkerhetsåtgärder samt personuppgiftsbiträdesavtal. Eftersom förvaltningen har genomfört eller inlett åtgärder kopplat till samtliga rekommendationer kommer den fortsatta uppföljningen att ske inom ramen för de fasta kontrollpunkterna.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

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

Beskrivning av risknivåer

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

2.4 Förvaltningen för arbetsmarknad och vuxenutbildnings 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:

Förvaltningen har genomgående angett det näst högsta värdet inom denna kontrollpunkt. Det medför en placering inom riskområde med tre, men man gränsar

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

till fyra. Denna placering innebär att det finns risker men dessa bedöms inte som brådskande eller allvarliga.

Dataskyddsombudets uppfattning är att förvaltningen arbetar aktivt med frågor kring dataskydd och att det överlag finns goda förutsättningar för att kunna bedriva dataskyddsarbetet. Dataskyddsombudet rekommenderar att förvaltningen fortsätter att arbeta för att dataskydd ska vara en integrerad och naturlig del i alla delar av verksamheten. Det rekommenderas också att förvaltningen kontinuerligt utvärderar den interna organisationen och säkerställer att den har rätt förutsättningar för att bedriva ett effektivt dataskyddsarbete.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Förvaltningen har för denna kontrollpunkt skattat att påståendena stämmer bra eller stämmer helt med hur arbetet med personuppgiftsincidenter bedrivs i verksamheten. Dataskyddsombudet genomförde 2021 en fördjupad kontroll gällande hantering av personuppgiftsincidenter och lämnade rekommendationer till förvaltningen att arbeta vidare med. Förvaltningen har vidtagit flera åtgärder utifrån de förbättringsområden som identifierades i samband med kontrollen.

Enligt förvaltningen har det enbart inträffat ej anmälningspliktiga incidenter under det gångna året. Dataskyddsombudet har ingen anledning att misstänka att en annan bedömning avseende dessa borde har gjorts men vill påminna förvaltningen om att rådfråga dataskyddsombudet i gränsfall/fall då det finns osäkerhet.

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:

Förvaltningen anger varierande värden i skattningen av påståendena för kontrollpunkten. Verksamheten anger hög skattning för andelen personuppgiftsbiträdesavtal som är tecknade samt för rutiner att bedöma relationen

mellan personuppgiftsansvarig och personuppgiftsbiträde samt teckna biträdesavtal innan en tjänst tas i drift. Verksamheten bedömer också att det finns rutiner för att bedöma om andra överenskommelser/avtal behöver upprättas vid personuppgiftshantering. Av skattningen framgår att lägre värde har angetts gällande att ha rutiner för att genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden och för rutiner och kompetens att bedöma hela kedjan av biträden och underbiträden.

Som framgår av uppföljningen verkar förvaltningen vara i färd med att undersöka hur personuppgiftsbiträdesavtal och personuppgiftsbiträdens säkerhetsåtgärder kan följas upp, vilket är positivt. Dataskyddsombudet rekommenderar att förvaltningen under det kommande året går från utredning till genomförande avseende uppföljning och efterlevnadskontroller. Eftersom flera rutiner och arbetssätt är relativt nya rekommenderas det att förvaltningen utvärderar sitt arbete för att säkerställa att det är effektivt och ändamålsenligt.

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:

Skattningen på denna punkt indikerar att arbetet med personuppgiftsregistret fungerar väl och att inga direkta eller brådskande risker finns identifierade. Förvaltningen uppskattar att ca 100 % av alla förvaltningens behandlingar finns registrerade i förteckningen, vilket är en förbättring i förhållande till föregående års svar.

Dataskyddsombudet gör ingen annan bedömning avseende detta arbete än vad som framgår av förvaltningens skattning. För att förvaltningen ska bibehålla sin placering inom den aktuella risknivån är det viktigt att förvaltningen fortsätter att arbeta aktivt med sitt personuppgiftsregister och säkerställer att det hålls aktuellt och uppdaterat.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Förvaltningens svar i denna del utgörs av varierande värden där det bl.a. indikeras att förvaltningen har dokumenterade rutiner som säkerställer att styrande dokument hålls uppdaterade, att man i relativt stor utsträckning arbetar riskbaserat och att ca 75 % av informationstillgångar har värderats i enlighet med stadens styrande dokument. Det anges dock vara något sämre ställt med att ha rutiner för att säkerställa dataskyddet vid fysiska och digitala sammankomster/möten och vad gäller interna följsamhetskontroller.

Trots att förvaltningen är kvar inom samma risknivå som föregående år har det enligt självskattningen skett en förbättring inom denna kontrollpunkt. Dataskyddsombudet har inte genomfört någon generell översyn av förvaltningens dataskyddsstrategi under året. Det har dock inte framkommit något som föranleder dataskyddsombudet att göra en annan bedömning än vad förvaltningen gör via sin skattning.

För att minska riskerna än mer inom detta område rekommenderar dataskyddsombudet att förvaltningen ser över hur det arbetas med dataskydd vid fysiska och digitala sammankomster samt tar fram rutiner där detta saknas. Förvaltningen rekommenderas också att se över hur interna kontroller kan genomföras för att följa upp hur förvaltningen efterföljer GDPR. Detta är en viktig del av arbetet eftersom det annars är svårt att veta om framtagna rutiner och arbetssätt får eftersträvansvärd effekt.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Vid jämförelse med föregående års skattning har det inom denna kontrollpunkt skett en förbättring. Förbättringen avser att möjliggöra för medarbetare att delta i externa utbildningar samt vad gäller att ha rutiner för att följa upp och bibehålla kunskapsnivå hos medarbetare. Skattningen indikerar också att verksamheten i viss mån fortfarande behöver kartlägga vilken nivå av dataskyddskunskaper som olika befattningars arbete kräver och genomföra utbildningsinsatser därefter.

Förvaltningen har under året genomfört interna utbildningsinsatser och medarbetare från förvaltningen har också deltagit vid dataskyddsenhetens utbildningar inom dataskydd vilket indikerar intresse och engagemang. Förvaltningen rekommenderas att fortlöpande utbilda medarbetare för att öka och/eller bibehålla deras kunskapsnivå. Dataskyddsombudet rekommenderar också, i likhet med föregående år, att förvaltningen genomför en kartläggning av olika befattningars behov av kunskapsnivå och undersöker var olika utbildningsinsatser kan behöva fokuseras.

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:

Förvaltningens skattning i denna del indikerar att det här inte finns några direkta risker och att det finns ett systematiskt dataskyddsarbete vad gäller informationsplikten. Vid jämförelse med föregående års skattning har en viss försämring angetts avseende om de registrerade enkelt kan nå informationen från samtliga kanaler. Dataskyddsombudet rekommenderar att förvaltningen ser över hur detta kan åtgärdas.

Dataskyddsombudet har inte genomfört någon granskning av den information som tillhandahålls registrerade under det gånga året men har inte heller fått indikationer som medför en avvikande bedömning. För att bibehålla det generellt sett höga betyget på denna punkt behöver förvaltningen säkerställa att rutinen att uppdatera och justera integritetspolicyn fortsätter att följas.

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:

I jämförelse med föregående års skattning är det största lyftet avseende e-post och dokumenthantering att förvaltningen nu har en aktuell och fastställd dokumenthanteringsplan. Eftersom det utgör en grundförutsättning för ett systematiskt och korrekt dokumenthanteringsarbete och följaktligen dataskyddsarbete är detta en mycket positiv utveckling. Förvaltningen behöver, enligt sin egen skattning, emellertid fortfarande säkerställa fungerande rutiner för att handlingar gallras, vilket är en viktig del i att följa principerna om uppgifts- och lagringsminimering enligt GDPR.

Förvaltningen behöver också arbeta med sin informationsklassning samt ta fram rutiner för hur olika klasser får hanteras och var de får sparas/lagras. Det behöver även ske en förbättring vad gäller hantering av personuppgifter i e-post.

Förvaltningen rekommenderas att ta fram rutiner för gallring samt rutiner för vilken information som får sparas/hanteras var – inklusive hur hanteringen i e-post får ske.

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:

Inom denna kontrollpunkt har det i förhållande till föregående års skattning skett en förbättring. Det har dock inte skett en förbättring vad avser faktiskt genomförda konsekvensbedömningar, vilket får anses vara den viktigaste delen. Att förvaltningen arbetar med rutiner, metoder och arbetssätt för att korrekt hantera konsekvensbedömningar spelar liten roll om inte förvaltningen också genomför de konsekvensbedömningar som krävs.

I likhet med föregående års enkätsvar har förvaltningen genomfört konsekvensbedömningar för ca 25 % av de behandlingar som förvaltningen utför som har höga risker. Det anges inte heller att det i någon större utsträckning finns en planering för genomförandet av de konsekvensbedömningar där detta krävs.

Trots förvaltningens placering inom risknivå tre ser dataskyddsombudet att det här finns risker som omgående behöver åtgärdas. Dessa utgörs både av risker för de registrerade eftersom behandlingar där deras personuppgifter ingår inte har bedömts och risker för förvaltningen som vid en eventuell tillsyn kan få sanktionsavgifter. Dataskyddsombudet rekommenderar att förvaltningen framåt prioriterar arbetet med att genomföra konsekvensbedömningar.

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:

Förvaltningen har på denna punkt skattat sitt arbete med främst medelhöga värden vilket indikerar att det finns risker men att dessa inte är akuta eller brådskande. Utifrån skattningen verkar förvaltningen ha identifierat att det främst är vid införande av nya digitaliseringslösningar som det behöver ske en förbättring vad gäller säkerställande av dataskydd. Dataskyddsombudet har under det gångna året

blivit tillfrågad angående upphandlingen av nytt elevhanteringssystem, då gällande formulering av krav.

Dataskyddsombudets upplevelse är att förvaltningen inom detta område (samt även generellt) är mycket självgående i dataskyddsfrågor, vilket är övervägande positivt. Det är dock viktigt att dataskyddsombudet ändå hålls informerad i frågor som rör dataskydd för att kunna ha överblick och insyn i verksamheten. Även om förvaltningen inte upplever att det behöver efterfrågas synpunkter och råd är det viktigt att dataskyddsombudet hålls uppdaterad för att kunna lyfta eventuella risker och för att korrekt kunna återge hur dataskyddsarbetet de facto fortlöper. Dataskyddsombudet rekommenderar att förvaltningen utreder hur arbetet i denna del skulle kunna förbättras.

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:

Förvaltningens skattning inom denna punkt indikerar att det finns risker och att det finns förbättringar som behöver ske. Skattningen medför en placering i risknivå tre men man gränsar till nivå två. Skattningen är också identisk med föregående år vilket indikerar att detta inte är ett område som förvaltningen har arbetat med under det gångna året.

Dataskyddsombudets rekommendationer är därför, i likhet med föregående år, att förvaltningen tar fram rutiner som säkerställer att tilldelning av behörigheter och åtkomst är begränsat till det som är nödvändigt. Förvaltningen rekommenderas också ta fram rutiner som säkerställer att behörigheter och åtkomster följs upp regelbundet. För att säkerställa att de IT-system och digitala verktyg som införs lever upp till kraven i förordningen rekommenderas förvaltningen också att ta fram en anskaffningsprocess. Förvaltningen bör även ta fram målgruppsanpassad information om hur personuppgifter behandlas i de digitala verktyg och IT-system som används. Det bör också finnas dokumenterat vilka IT-system och digitala verktyg som används inom förvaltningen.

Som nämnt tidigare i rapporten har dataskyddsombudet även genomfört en fördjupad kontroll inom ramen för denna kontrollpunkt avseende behörighetsstyrningen i Alvis. De specifika kommentarerna och rekommendationerna kopplat till detta framgår av bilaga 2.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Förvaltningen har på denna punkt angett medelhöga och medellåga värden i sin skattning. En förbättring verkar utifrån skattningen främst vara behövlig vad gäller den allmänna medvetenheten om registrerades rättigheter inom verksamheten, att ha rutiner för att kunna hantera invändningar och återtagande av samtycken från registrerade. Även om det kanske i dagsläget är ovanligt att registrerade vill utöva sina rättigheter i förhållande till förvaltningen är detta något det behöver finnas förutsättningar för att kunna hantera. Dataskyddsombudet rekommenderar därför att förvaltningen utreder hur medvetenheten kring dessa frågor kan ökas inom verksamheten samt säkerställer att man är tillräckligt förberedd för att kunna hantera inkommande frågor.

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/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 9: Konsekvensbedömningar/samråd
- Kontrollpunkt 11: IT-system och digitala verktyg

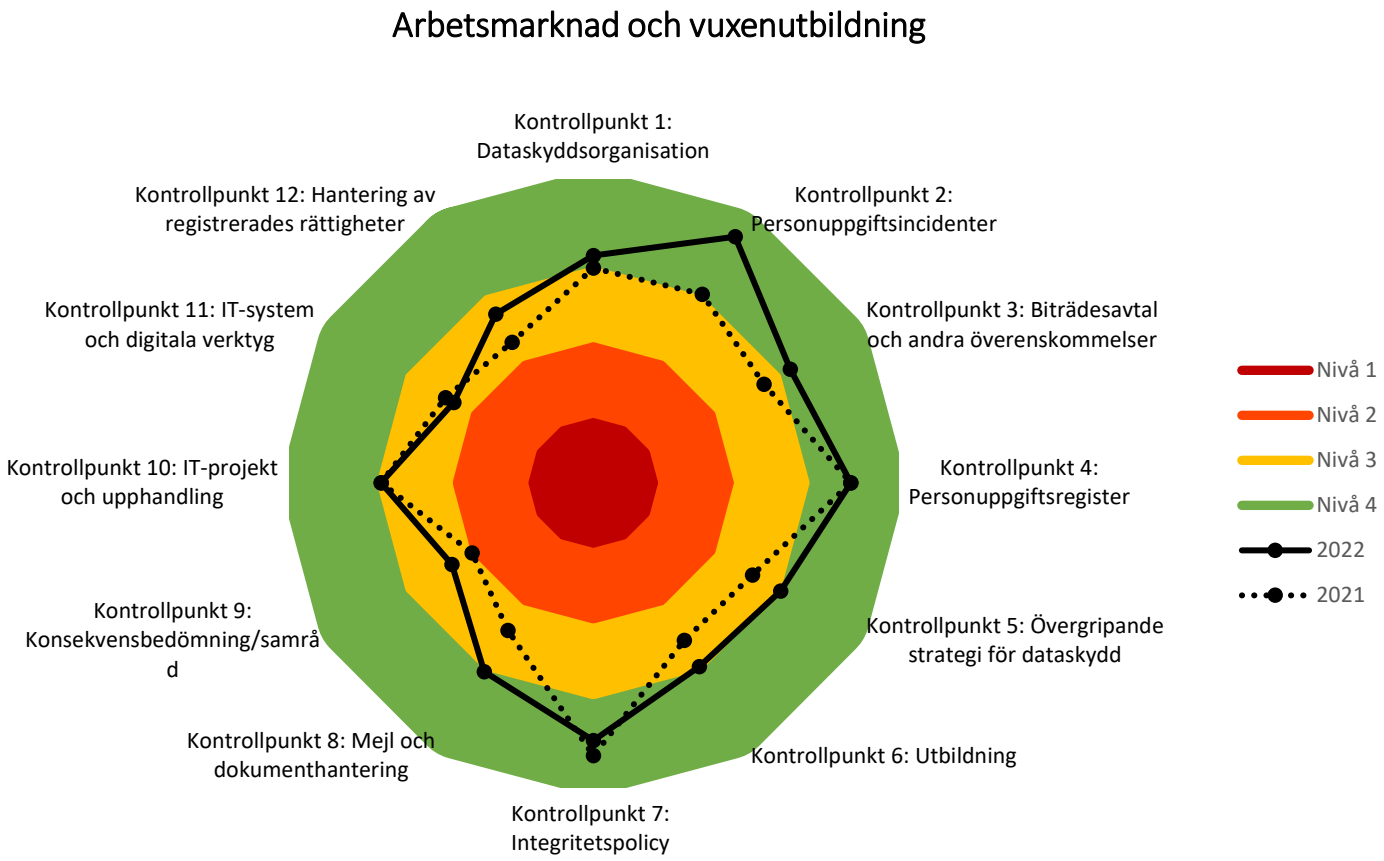
3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021

Bilaga 2: Fördjupad kontroll 2022, behörighetsstyrning

Bilaga 1

Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

Kontrollpunkt 11: Behörighetsstyrning

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 i systemet Alvis för chefer och medarbetare inom förvaltningen för arbetsmarknad och vuxenutbildning samt för externa användare.

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

Enligt underlag från förvaltningen finns det 1552 användare i Alvis, som avser personal inom förvaltning, på upphandlade skolor, socialtjänst och Arbetsförmedlingen. Det finns fyra personer som har hög behörighet och åtkomst till allt i systemet. Dessa fyra användare har arbetsuppgifter som kräver denna tillgång och är systemadministratörer, systemansvarig samt intern support.

Det finns ca 356 000 registrerade i Alvis, varav ca. 25–30 000 per termin är aktiva studerande.

Behörighetsstruktur och roller i system

I Alvis finns dels grundbehörigheter, dels tilläggsbehörigheter. Utifrån dessa har förvaltningen skapat särskilda behörigheter utifrån yrkesgruppers olika uppdrag och behov.

Av den lista som förvaltningen skickat in i samband med kontrollen framgår att 41 olika behörigheter finns i systemet. Dessa omfattar både grundbehörigheter, tilläggsbehörigheter samt de av förvaltningen skapade behörigheterna för olika yrkesgrupper.

Tilldelning av behörighet utifrån bedömning

Förvaltningen har uppgett att ansvarig chef meddelar Alvis support vid behov av behörighet till nya användare eller förändringar av behörighet för aktiva användare samt när behörigheter ska avaktiveras. Bedömning av användares behörighet görs utifrån yrkesroll och behov att utföra sina arbetsuppgifter.

För externa användare där upphandlade skolors personal, socialtjänstens samt Arbetsförmedlingens personal ingår är tillvägagångssättet olika.

Upphandlade skolor kan registrera personal direkt i Alvis, men det är Alvis support som tilldelar behörighet och aktiverar kontot. Skolorna kan själva inaktivera konton när personal slutar. Det finns specifika behörighetsgrupper utifrån olika yrkesroller på skolorna såsom rektor, lärare, administratör etc.

Socialtjänst och Arbetsförmedlingen meddelar Alvis support via ett beställningsformulär. För användare hos socialtjänsten och Arbetsförmedlingen finns endast en behörighetsnivå.

I Alvis går det även att bestämma tidsperiod för när konton ska vara aktiva samt att de ska låsas efter en viss period, 60 eller 90 dagar, vid inaktivitet.

Utifrån den beskrivning som förvaltningen har gett uppfattar dataskyddsombudet det som att behörigheterna kan anpassas utifrån olika roller och arbetsuppgifter som finns inom förvaltningen. Dataskyddsombudet anser det vara positivt att strukturen för behörighetstilldelning är uppbyggd kring grundbehörighet och tilläggsbehörighet, eftersom strukturen möjliggör mer individuellt anpassad tilldelning av behörigheter.

Av Göteborgs Stads riktlinjer för informationssäkerhet[1] framgår att det ska finnas dokumenterade regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst som är formellt beslutad. Utifrån de underlag förvaltningen skickat in i samband med kontrollen framgår att det i systemdokumentationen för Alvis kortfattat beskrivs hur behörighetstilldelning sker. Dataskyddsombudet konstaterar dock att beskrivningarna i dokumentet är generellt utformade och ytligt beskrivna vilket medför att relevant information i stora delar saknas. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram en rutin för tilldelning av behörigheter. Dokumentationen i en rutin blir ett led i att uppfylla ansvarsskyldigheten enligt artikel 5.2 dataskyddsförordningen, eller med andra ord ett sätt för förvaltningen att visa att reglerna för personuppgiftsbehandling följs.

Beslut om behörighet

När ansvarig chef har meddelat Alvis support om att en ny användare ska ges behörighet, är det systemansvarig som beslutar vilken behörighet den anställde ska ha i Alvis. Om enhetschef beställer behörighet för en av sina anställda tilldelas behörighet utifrån organisatorisk tillhörighet och roll. Exakt hur detta går till och vem som bestämmer över

[1] Göteborgs Stads riktlinje för informationssäkerhet, beslutad av kommunfullmäktige 2013-09-05, § 21, senast reviderad 2019-12-16, diarienummer 0540/14 (0110/19)

behörighetsnivån framgår inte av dokumentationen. Det framgår att ansvarig chef meddelar Alvis support om nya användare och ändringar i behörighetsnivå samt att systemansvarig beslutar om vem som ska ha vilken behörighet. Hur detta i praktiken går till och vem som bestämmer vad bör tydligare framgå av en rutin (se rekommendation ovan).

Uppföljning av behörighet

Behov ska styra behörighet, vilket bland annat innebär att om någon byter roll eller arbetsuppgifter, begär tjänstledigt eller är föräldraledig ska behovet av behörighet ses över och justeras. Om någon avslutar sin anställning är det särskilt viktigt att omedelbart inaktivera behörighet och stoppa tillgång till system och information. Därför behövs rutiner både för ändrat behov under anställning och vid anställnings slut.

Förvaltningen hänvisar till Göteborgs Stads regel för chefers informationssäkerhetsansvar, där det anges att det är chefen som inom sitt ansvarsområde ansvarar för att följa upp samt initiera upplägg, förändring och borttag av behörigheter.

Utbildningsleverantörer (upphandlade skolor), som bedöms vara personuppgiftsbiträden till nämnden, har ett eget ansvar att registrera samt inaktivera konton för personal som slutar.

För externa parter, som bedömts vara egna personuppgiftsansvariga, ska utsedda kontaktpersoner två gånger om året kontrollera att rätt personer har behörighet till Alvis. En gång om året följer Alvis Support och systemansvarig upp socialtjänstens behörigheter.

Förvaltningen har uppmärksammat risker kopplat till svårigheten att få kännedom om när en intern medarbetare byter tjänst/arbetsuppgifter och därmed bör få annan behörighet. Liknande svårigheter har identifierats kring ett fåtal användare som har flera anställningar på olika skolor/förvaltningar.

Dataskyddsombudet vill understryka vikten av att ha rutiner kring uppföljning av behörigheter såväl internt som externt. Vid uppmärksammade risker om att det är svårt att få kännedom om när användare byter tjänst/arbetsuppgifter är det viktigt att det tydligt framgår av rutiner hur chefer och andra som medverkar vid hantering av behörigheter ska agera samt att dessa rutiner är kommunicerade och kända för både externa parter och inom förvaltningen. De rutiner som finns kan behövas förtydligas och tillgängliggöras på ett enklare sätt. Vidare kan utbildning behövas för ansvariga personer som hanterar behörigheter. Uppföljningsrutiner behövs både för ändrat behov under anställning (kan innebära byte av tjänst eller längre planerad frånvaro) såväl som vid anställnings slut. Förvaltningen rekommenderas därför att ta fram och tillgängliggöra rutin för uppföljning av behörigheter.

Åtkomstkontroll/kontroll av loggar

Förvaltningen har uppgett att Alvis har olika loggningsfunktioner. Loggar avseende vilka registreringar en användare har gjort, vad som har sparats/ändrats och när kommer Alvis support själva åt. För mer detaljerade loggar som visar sökningar krävs support från personuppgiftsbiträdet Gotit.

Det sker inga regelbundna kontroller av loggar i Alvis, mer än vid förekommen anledning såsom vid utredning av personuppgiftsincidenter, om en elev blivit felregistrerad och liknande situationer.

Givet omfattningen användare och registrerade i systemet rekommenderar dataskyddsombudet att förvaltningen tar fram rutiner för systematisk och regelbunden genomgång av loggar. Det bör även framgå hur genomgång av loggar sker för de användare som har priviligierad åtkomst till systemet. Dataskyddsombudet vill understryka att nyttan med loggkontroller inte endast är att kontrollera riktighet/korrekthet av registrerade uppgifter, utan även att loggkontrollerna kan fylla en viktig funktion i uppföljningen av frågor som har med konfidentialitet att göra. Kontroll av loggar är också av särskild vikt i system som hanterar dels känslig information, dels har breda behörigheter. Det kan även vara av vikt att genomföra särskilda loggkontroller för utvalda grupper registrerade som är särskilt utsatta, såsom personer med skyddade personuppgifter eller där annan sekretess är tillämplig, för att kontrollera att inte fler användare än nödvändigt tar del av deras uppgifter.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

Förvaltningen har angett att det finns lagar och bestämmelser som påverkar behörighetstilldelningen. Dessa anges vara: skollagen, förordning om vuxenutbildning, förordning om den arbetsmarknadspolitiska verksamheten, socialtjänstlagen, offentlighets- och sekretesslagen, avtal med utbildningsanordnare, överenskommelser med andra kommuner/samverkan inom Göteborgsregionen (GR).

Det framgår dock inte på vilket sätt eller vilka lagrum i de olika lagarna som påverkar behörighetstilldelningen. Som nämnts ovan hanteras uppgifter om personer med skyddade personuppgifter i systemet, utöver detta kan även andra sekretessregler gälla för verksamheten, till exempel för den information som dokumenteras angående arbetsmarknadsinsatser i systemet. Dataskyddsombudet rekommenderar förvaltningen att utreda detta och dokumentera på vilket sätt det påverkar behörighetstilldelningen i en rutin för tilldelning och ändring av behörigheter.

Andra åtgärder

Förvaltningen anger att de vidtagit följande åtgärder för att förhindra obehörig åtkomst till personuppgifter i systemet:

- Personal autentiserar sig med tvåfaktorsinloggning. Sökande och studerande autentiserar sig med antingen användarnamn och lösenord eller med BankId.
- Användarkonton låses automatiskt efter 100 dagars inaktivitet och konton som inte använts på sex månader inaktiveras.

Förvaltningen anger att någon konsekvensbedömning inte har genomförts för de behandlingar som görs i Alvis. Förvaltningen är mitt uppe i arbetet med upphandling av nytt verksamhetssystem varför det inte bedöms vara aktuellt att skriva någon konsekvensbedömning kopplat till Alvis. Dataskyddsombudet vill här framhålla att konsekvensbedömning ska göras inför att en behandling påbörjas eller ändras på ett väsentligt sätt. Av den anledningen är det ett bra tillfälle att kartlägga de behandlingar som berörs av eventuellt byte av system för att identifiera för vilka av dessa behandlingar

det behöver göras konsekvensbedömning/ar. Ett av syftena med att göra en konsekvensbedömning är att identifiera risker och förebygga dessa innan de uppkommer. Genom att identifiera riskerna i ett tidigt stadie kan förvaltningen också på ett mer effektivt sätt omhänderta dessa i samband med att nytt system upphandlas.

Förvaltningen har uppgett att en riskanalys har genomförts inom ramen för arbetet med informationsklassning där totalt 45 risker identifierades. Vissa av riskerna kan direkt eller indirekt kopplas till hanteringen av behörigheter och det stora antal individer som har tillgång till Alvis. Förvaltningen tar även upp att det finns risker kring behörigheter hos externa parter (socialtjänsten och Arbetsförmedlingen) samt att förvaltningen haft löpande kontakt med nämndens dataskyddsombud i frågan. Dataskyddsombudet har den 7 oktober 2022[2] lämnat rekommendationer angående socialtjänstens direktåtkomst i systemet. Dataskyddsombudet rekommenderar att förvaltningen upphör med informationsutbytet genom direktåtkomst i enlighet med lämnade rekommendationer. Vidare rekommenderar dataskyddsombudet att förvaltningen utreder och vidtar åtgärder med utgångspunkt från rekommendationerna även för Arbetsförmedlingens direktåtkomst i systemet eftersom samma förhållande torde gälla här som för socialtjänstens personal.

Sammanfattade rekommendationer

- Ta fram rutin för tilldelning och ändring av behörigheter
- Ta fram rutin för regelbunden uppföljning av tilldelade behörigheter
- Ta fram rutin för regelbunden åtkomstkontroll/kontroll av loggar
- Upphöra med informationsutbytet genom direktåtkomst i Alvis för socialtjänsten i enlighet med tidigare rekommendationer lämnade 2022-10-07
- Utreda Arbetsförmedlingens direktåtkomst i Alvis med utgångspunkt från rekommendationer lämnade 2022-10-07

Bilagor

Information om fördjupad kontroll 2022
Fördjupad kontroll 2022, kontrollpunkt 11: Behörighetsstyrning (del 1 och 2)

[2] Rättsliga förutsättningar och rekommendation avseende informationsutbyte genom direktåtkomst från arbetsmarknad och vuxenutbildning till försörjningsstödsenheterna inom socialtjänsten, lämnat av dataskyddsombud 2022-10-07

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 Alvis. I del två kommer uppföljande frågor att ställas.

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 Alvis.

- 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)

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

- Vilka typer av personuppgifter behandlas i Alvis? (t.ex. personnummer, betyg, sociala förhållanden osv.)
- Ca. hur många registrerades personuppgifter hanteras i systemet? (Om siffrorna i bilaga 5 är uppdaterade kan ni hänvisa till den)
- Hur många personer har behörigheter (personuppgiftsbiträde, administratörer)? (Om siffrorna i bilaga 5 är uppdaterade kan ni hänvisa till den)
- Föreligger det inbyggda svårigheter i Alvis att begränsa behörigheterna på så vis att personer enbart kan se sådana uppgifter som tillhör till den egna förvaltningen? Varför/varför inte?
- Vilket förhållande har förvaltningen till andra aktörer som har tillgång till Alvis (skola/leverantör och socialtjänst/AF)? Utgör de t.ex. personuppgiftsbiträden eller är de självständiga personuppgiftsansvariga.
- Hur kontrolleras personuppgiftsbiträdens behörigheter i systemet? (t.ex. leverantören)
- Finns det instruktioner till personuppgiftsbiträdet/biträdena? Om ja, översänd dessa. Om nej, varför inte?
- Det anges i svar på del 1 att det inte sker några regelbundna systematiska kontroller av loggar, utan endast vid förekommande anledning. Ange vad som kan utgöra ”förekommande anledning”.
- 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 (t.ex. antagonistiska angrepp)

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 9 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.