Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

GS Trafikantservice AB

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 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 behörighetsstyrning i personalplaneringssystemet Quinyx. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa synpunkter och därför lämnat ett antal rekommendationer om att vidta vissa åtgärder.

Sammanfattade rekommendationer:

- Dataskyddsombudet rekommenderar att bolaget konkretiserar instruktionen för Quinyx och tydligt anger hur och när behörigheter ska

tilldelas/ändras. Det bör i denna instruktion även framgå vilken roll som har behörighet att begära att roller/behörigheter tilldelas och ändras.
- Konkretisera och komplettera instruktionen med rutiner för uppföljning av tilldelade behörigheter.
- Komplettera instruktion med rutiner för hur och när det är aktuellt att ta fram loggar i systemet. Det bör också förtydligas vad som utgör misstanke om oegentlighet och när kontroll ska ske utifrån en sådan misstanke.
- Bolaget rekommenderas att definiera sina personuppgiftbehandlingar i Quinyx, bedöma om de uppfyller kraven för när en konsekvensbedömning ska göras samt i förevarande fall genomföra en konsekvensbedömning.

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 GS Trafikantservice AB:s 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:

Bolaget har inom denna kontrollpunkt genomgående angett höga värden i sin skattning vilket medför en placering inom risknivå fyra. Denna placering innebär att inga direkta risker kan identifieras.

Mot bakgrund av antalet anställda och därigenom omfattning av personuppgifter som behandlas av bolaget bör dataskyddsfrågor vara något som regelbundet kommer upp och något som det arbetas relativt aktivt med. Dataskyddsombudet har ett fåtal gånger kontaktats av bolaget det senaste året rörande dataskyddsfrågor. Att bolaget, utifrån rådande läge med aktivt beslut om försäljning, inte prioriterar arbetet med dataskydd är förståeligt. Så länge personuppgifter behandlas av bolaget behöver emellertid bestämmelserna i GDPR följas vilket ställer krav på att det finns en fungerande dataskyddsorganisation. Dataskyddsombudet rekommenderar att bolaget kartlägger, till exempel genom att titta på andra verksamheter i Göteborgs Stad, vilka delar som en välfungerande dataskyddsorganisation ska bestå av och vilka frågor som det inom en sådan behöver arbetas med. Dataskyddsombudet rekommenderar också att bolaget i större utsträckning involverar eller i vart fall informerar dataskyddsombudet om de dataskyddsfrågor som är aktuella för bolaget.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

I jämförelse med föregående års enkätsvar har det enligt bolaget skett en klar förbättring vad gäller arbetet med personuppgiftsincidenter. Dataskyddsombudet är inte helt insatt i vad dessas förbättringar rent konkret består av men dataskyddsombudet har inte heller anledning att ifrågasätta bedömningen. I sammanhanget kan det noteras, vilket kan verka motsägelsefullt, att ju fler incidenter som en verksamhet upptäcker och dokumenterar desto bättre fungerar det generella dataskyddsarbetet. I och med att till och med ett felskickat mejl kan utgöra en incident är det positivt när dessa incidenter upptäcks eftersom det är ett tecken på att medarbetare är medvetna och uppmärksamma vad gäller dataskyddsfrågor. Detta är något som bolaget framåt kan ha med sig vid utvärdering av hur dataskyddsarbetet inom bolaget fungerar.

Dataskyddsombudet rekommenderar i övrigt att bolaget fortsätter att arbeta aktivt med att förbättra och/eller bibehålla de goda förutsättningarna som finns för att identifiera och hantera personuppgiftsincidenter.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Dataskyddsombudets kommentarer:

Den sammantagna skattningen inom denna kontrollpunkt indikerar att detta utgör ett förbättringsområde för bolaget, eftersom risker som behöver åtgärdas kan identifieras.

Bolagets svar indikerar bl.a. att det finns personuppgiftsavtal tecknat i ca 50 % av fallen där detta krävs, att det i viss mån saknas rutiner för att utföra efterlevnadskontroller samt i viss mån saknas rutiner och kompetens för att bedöma kedjan av biträden och underbiträden. Dataskyddsombudet delar bolagets uppfattning om var man befinner sig i detta arbete. Bolaget rekommenderas att prioritera arbetet med att teckna personuppgiftsbiträdesavtal i de fall där detta saknas. Bolaget rekommenderas också att se över vilka rutiner som saknas och säkerställa att dessa tas fram.

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:

Bolagets svar i denna del indikerar att det inom detta område finns risker som omedelbart behöver åtgärdas. Dataskyddsombudet instämmer i den bedömning som görs genom skattningen inom detta område. Bolaget rekommenderas att prioritera arbetet med att ta fram ett komplett och uppdaterat personuppgiftsregister.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolaget har på denna punkt angett varierande värden i sin skattning vilket sammanlagt medför en placering inom riskområde två. Viss förbättring har enligt bolaget skett i förhållande till föregående år, främst vad gäller punkten om att genom dokumenterade rutiner säkerställa att styrande dokument hålls uppdaterade. I övrigt kan dataskyddsombudet konstatera, i likhet med bolaget, att det finns utrymme för förbättring.

Mot bakgrund av bolagets egen skattning rekommenderar dataskyddsombudet att det säkerställs att det finns en informationssäkerhetspolicy, att informationstillgångar värderas och att interna kontroller införs för att säkerställa följsamhet med GDPR. Bolaget rekommenderas också att ta fram rutiner för hur kraven enligt GDPR ska efterlevas vid fysiska och digitala sammankomster/möten.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolaget svar på enkäten i denna punkt indikerar att medarbetarna regelbundet utbildas inom dataskydd och att den allmänna kunskapsnivån ger goda förutsättningar för att bedriva dataskyddsarbetet. Dataskyddsombudet har inte fått några indikationer som medför en annan bedömning. Dataskyddsombudet vill dock

lyfta att höga skattningar på denna punkt t.ex. innebär att i princip alla anställda korrekt ska kunna identifiera en personuppgiftsincident, att relevanta roller ska veta hur och när en konsekvensbedömning ska göras och att ansvariga ska ha kunskap om tillvägagångssätt när registrerade utövar sina rättigheter i förhållande till bolaget. Detta knyter också an till kontrollpunkten biträdesavtal och andra överenskommelser och frågan om att ha kompetens att bedöma hela kedjan av biträden och underbiträden, vilket också måste finnas för att den allmänna kunskapsnivån ska anses tillräcklig.

Såvida detta inte stämmer in på bolaget bör arbetet ses över även inom denna kontrollpunkt.

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:

Svaren på enkäten i denna del indikerar inga direkta risker och att knappt några förbättringar finns att göra avseende den information som ges till registrerade om bolagets personuppgiftsbehandlingar. Årets svar indikerar också en klar förbättring i förhållande till föregående år.

Efter en snabb genomläsning av bolagets integritetspolicy kan dataskyddsombudet konstatera att den inte uppfyller de grundläggande kraven i GDPR och att den behöver ses över. Policyn är gemensam för tre bolag och det framgår inte vilka personuppgiftsbehandlingar som faktiskt sker hos respektive bolag. Policyn innehåller inte heller konkreta uppgifter om ändamål eller vilka rättsliga grunder som bolaget lutar sig mot, utan nämner endast i mycket generella ordalag vilka uppgifter som kan förekomma och varför insamlingen är nödvändig.

Till skillnad från bolaget bedömer dataskyddsombudet att det finns risker inom denna kontrollpunkt som behöver hanteras. Dataskyddsombudet rekommenderar att bolaget genomför en grundlig omarbetning av policyn för att säkerställa att informationsplikten enligt GDPR uppfylls.

2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för mejl 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:

Bolaget har i sina svar på denna punkt angett varierande värden i sin skattning vilket medför en placering inom riskområde två. Detta innebär att det är ett område med risker som bolaget behöver hantera. Trots riskerna indikerar bolagets svar en klar förbättring vad gäller att ha en aktuell och fastställd dokumenthanteringsplan samt rutiner för gallring. Detta är ett viktig framsteg för bolaget och det finns nu bättre förutsättningar för en korrekt e-post- och dokumenthantering. Bolaget behöver fortfarande informationsklassa sin information och ta fram anvisningar för vilken information som får lagras var samt vilka uppgifter som får hanteras i e-post. Dataskyddsombudet rekommenderar att bolaget ser över detta och tar fram de anvisningar som saknas för att ge medarbetare bättre förutsättningar att göra rätt.

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:

Bolaget skattar sitt arbete på denna punkt med genomgående låga värden och placerar sig därför inom riskområde två. Det innebär att det finns omfattande risker som behöver åtgärdas. Skattningen är i flera delar samma som bolaget angav i föregående års enkät. Bolaget har alltså inte arbetat aktivt med att åtgärda de risker som identifierades förra året. Dataskyddsombudets rekommendationer är därför de samma som gavs i 2021 års årsrapport: dataskyddsombudet rekommenderar att det genomförs en kartläggning av de behandlingar med hög risk som genomförs där det saknas konsekvensbedömningar. Därefter bör en handlingsplan tas fram för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Bolaget har på denna punkt genomgående angivit låga värden i sin skattning. I jämförelse med föregående år har en försämring på denna punkt skett eftersom de flesta påståenden i år har besvarats med 0 dvs. ”vet inte/kan inte besvara frågan”. Att ha överblick och kontroll över vad som sker i bolaget är en grundläggande del av dataskyddsarbetet och brist på detta utgör en stor risk för personuppgiftsansvarig.

Vid en övergripande genomgång av resultatet med bolaget framkom att inga nya upphandlingar eller IT-projekt sker i dagsläget. Det är, på grund av bolagets ovissa framtid, inte heller något som kommer att ske på sikt. Utifrån läget framstår bolagets svar i denna del som rimliga. Dataskyddsombudet vill dock lyfta att för det fall upphandlingar eller införande av nya system m.m. planeras behöver dataskyddsperspektivet säkerställas.

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:

I förhållande till föregående års enkätsvar har det för denna kontrollpunkt skett en försämring. Sammantaget medför skattningen att bolaget placerar sig inom riskområde två vilket innebär att det finns risker som omgående behöver åtgärdas.

Dataskyddsombudet saknar överblick över hur användningen av IT-system och digitala verktyg ser ut i bolaget men har inte heller någon anledning att göra en annan bedömning än den som görs av bolaget. Två av punktens påståenden besvaras dock med ”vet inte/kan inte besvara frågan” vilket drar ner punktens övergripande skattning.

I likhet med föregående kontrollpunkt beror svaren enligt bolaget på att inga nya tjänster och verktyg införs utifrån rådande läge. Så länge bolaget behandlar personuppgifter behöver dock GDPR följas och skyddet för personuppgifterna säkerställas. Det innebär att det behöver finnas kontroll och översikt över de tjänster och digitala verktyg som används och användningen behöver ske på ett säkert sätt. Dataskyddsombudet rekommenderar att bolaget ser över sin användning av IT-system och digitala tjänster och säkerställer att medarbetare vet hur dessa får användas för att säkerställa en korrekt och säker behandling av personuppgifter.

Som nämnts tidigare i rapporten har dataskyddsombudet även genomfört en fördjupad kontroll inom ramen för denna kontrollpunkt avseende

behörighetsstyrningen i Quinyx. De specifika kommentarerna och rekommendationerna kopplat till detta framgår i sin helhet 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:

Bolaget har på denna kontrollpunkt skattat sitt arbete med varierande, men främst medelhöga, värden vilket innebär en placering inom risknivå tre. Det innebär att det finns risker men att dessa inte är akuta eller omfattande.

Dataskyddsombudet har ingen inblick i hur vanligt förekommande det är att registrerade kontaktar bolaget för att utöva sina rättigheter men har heller inga indikationer som innebär en avvikande bedömning än den som visas genom skattningen.

Utifrån skattningen behöver bolaget främst ta fram en process för att hitta/få tillgång till efterfrågad information vid en begäran om registerutdrag. Dataskyddsombudet rekommenderar att bolaget går igenom på vilka ytor och i vilka tjänster/system som personuppgifter behandlas och tar fram en process som gör det möjligt att genomsöka dessa vid en begäran om registerutdrag.

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 bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Personuppgiftsregister
- Kontrollpunkt 8: E-post och dokumenthantering

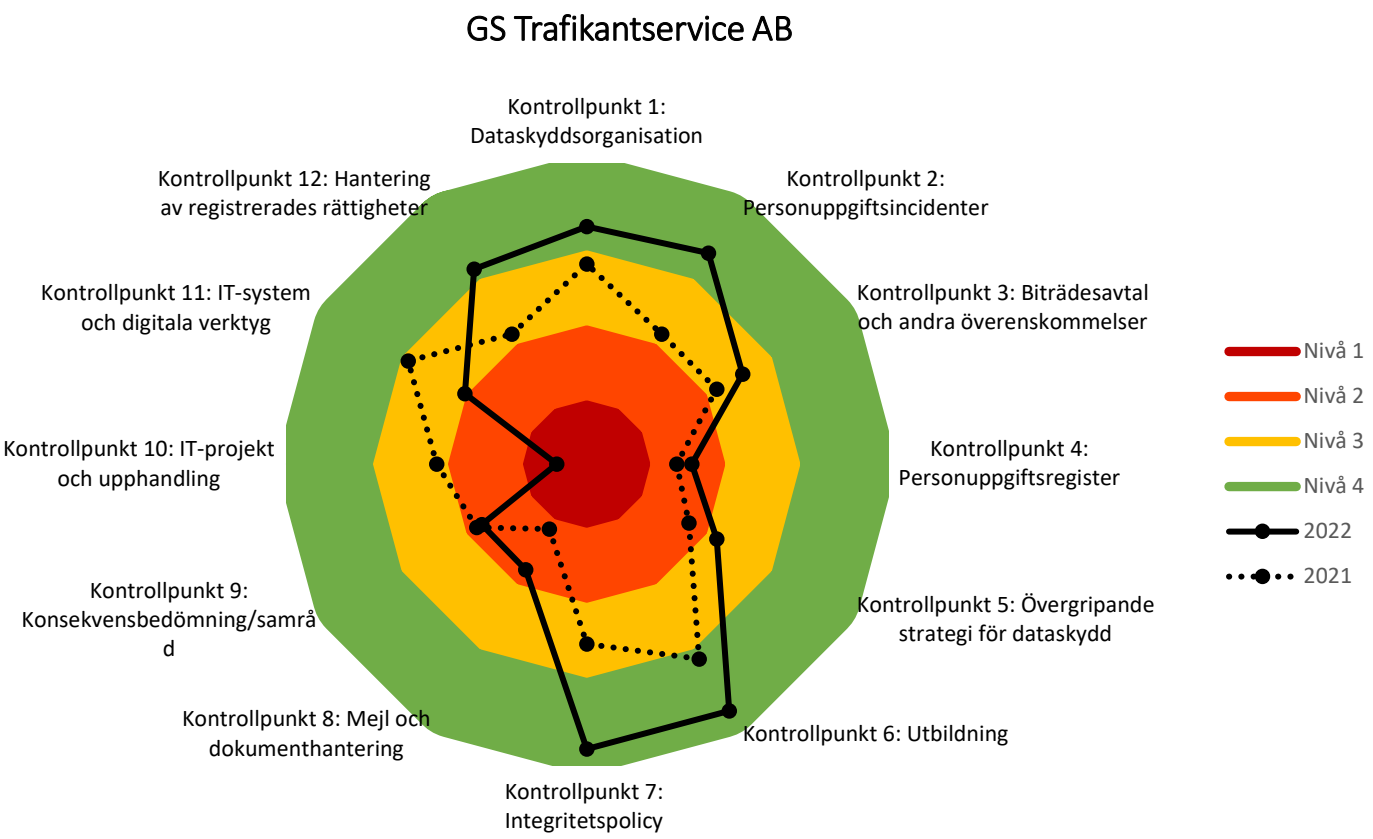
3 Bilagor

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. Granskningen har gjorts med utgångspunkt i artikel 32 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.

Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. I kontrollen ingick verksamhetens rutiner för tilldelning av behörigheter och åtkomster i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller.

Iakttagelser från kontrollen

En medarbetare i en verksamhet ska enbart ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten ha rutiner för tilldelning av behörighet, uppföljning av behörigheter samt hur användningen av logg-/åtkomstkontroller sker.

Kontrollen hos GS Trafikantservice AB (GST) har gjorts av systemet Quinyx. I systemet behandlas personuppgifter i form av namn, födelsedatum, kontaktuppgifter, uppgifter om anhöriga, anställningsnummer och uppgifter om utbildning. Efter följdfråga till bolaget framkommer även att uppgifter om kostnad på personer förekommer, vilket dataskyddsombudet tolkar som en uppgift om lön. Enligt svaren från bolaget förekommer det 148 personer i systemet. Efter genomgång med bolaget framgår också att det finns en framtagen instruktion för hantering av systemet.

Behörighetsstruktur och roller i system

Dataskyddsombudet tolkar bolagets svar som att det finns det sex olika roller i Quinyx som används av bolaget. Dessa utgörs av rollen anställd, extra planerare läsrättighet, enhetschef, personalplanerare, gruppchef och kontoägare (i tidigare svar från bolaget kallat superuser). Av svaret framgår att det är tre personer som innehar rollen kontoägare vilket ger tillgång till all information i systemet samt medför möjlighet att göra systeminställningar samt kontakta leverantörens support. Det anges också att roller kan skapas för tillfälliga uppdrag men bolaget har inte angett huruvida detta är aktuellt eller om det används. Enligt bolaget ska rollerna enhetschef och gruppchef tas bort. Det framgår inte om dessa roller ersätts med något annat.

Tilldelning av och beslut om behörighet utifrån bedömning

Bolaget anger att det är enhetschef som beslutar vilken roll som medarbetare ska ha. De flesta anges få rollen ”anställd” men kan också tilldelas en högre nivå om arbetsuppgifterna kräver detta. Dataskyddsombudet tolkar bolagets svar som att det är personen som är avtalsägare och innehar rollen kontoägare som sköter den faktiska tilldelningen av behörighet efter dialog med gruppchefer och enhetschefer. Bolaget har inte angett vad som ingår i den faktiska bedömningen eller om det finns nedtecknade rutiner för vilka arbetsuppgifter eller yrkesutövningar som kräver vilken roll/behörighet.

Av Göteborgs Stads riktlinje för informationssäkerhet framgår det att det ska finnas dokumenterade regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst och att denna ska vara formellt beslutad. Bolaget har en instruktion som är menad att säkerställa säkerhet och kvalitet i systemet, och som tar upp frågan om behörigheter. Formuleringarna i instruktionen är generella och odetaljerade. Det anges bl.a. att tilldelning av behörigheter sker i dialog med enhetschefer och gruppchefer, utan någon vidare instruktion om vilka omständigheter som ska tas i beaktande eller hur en bedömning av vilken medarbetare som ska ha vilken behörighet går till. Bolaget rekommenderas att komplettera underlaget med konkreta instruktioner kring hur behörighetstilldelningen ska gå till. Denna bör också inkludera en beskrivning av vilka arbetsuppgifter som kräver vilken roll. Det bör även tydliggöras vem som har mandat att begära en viss roll/behörighet och vem som ansvarar för att den är korrekt tilldelad och följs upp.

Uppföljning av behörighet

Av instruktionen framgår att kontoägare i systemet ”har löpande kontroll” och att det under 2022 införs en årlig avstämning med gruppchefer och enhetschefer. Dataskyddsombudet anser att det är positivt att bolaget beslutat att införa rutiner för att årligen se över behörigheterna men vill också uppmana bolaget att ta fram skriftliga rutiner för hur detta ska gå till. Bolaget rekommenderas att ta fram och dokumentera rutiner för att i samband med avslut av tjänst/början av ny tjänst samt byte av tjänst kontrollera att roller är korrekt tilldelade.

Åtkomstkontroll/kontroll av loggar

Bolaget uppger att leverantören tillhandahåller granskningsloggar för schema, tid, lön och konfiguration och att dessa är tillgängliga för kontoägare och chefer. Eftersom det inte specificeras ifall det gäller för gruppchefer eller enhetschefer utgår dataskyddsombudet från att det gäller för båda. Loggar kontrolleras enligt bolaget om en medarbetare flaggar för att något har blivit ”tokigt” och vid misstanke om oegentligheter. Vid misstanke om oegentligheter ansvarar VD för kontrollen. Loggarna innehåller bl.a. uppgifter om datum och tid för olika ändringar samt vem som har gjort ändringen.

Det specificeras inte i vilka situationer som det blir aktuellt att kontrollera loggarna och det verkar utifrån bolagets svar inte heller finnas ledning i vad ”misstanke om oegentlighet” kan vara. Att det finns loggning och spårbarhet kan vara en viktig del i säkerhetsarbetet och vid t.ex. incidentutredningar men måste ske på ett kontrollerat och strukturerat sätt som inte får anställda att känna att de övervakas. Eftersom en kontroll kan utgöra en personuppgiftsbehandling måste den också ha ett tydligt och avgränsat ändamål. Enligt svaret har både administratörer och chefer tillgång till dessa uppgifter

vilket enligt dataskyddsombudet får anses vara en relativt stor grupp i förhållande till antalet medarbetare som finns registrerade i systemet.

Dataskyddsombudet rekommenderar att bolaget tar fram tydliga rutiner som reglerar vilka som har mandat att ta fram loggar och i vilka situationer som detta kan bli aktuellt. Om det även ska vara aktuellt att ta fram loggar vid misstanke om oegentligheter behöver det specificeras vad som kan utgöra en misstanke om oegentlighet och hur förfarandet ser ut om en sådan misstanke uppstår.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

Dataskyddsombudet kan av GST:s svar inte utläsa att det finns annan lagstiftning eller andra bestämmelser som direkt påverkar behörighetstilldelningen. Dataskyddsombudet har inte heller kännedom om eventuell övrig och specifik lagstiftning eller bestämmelser som skulle omfatta bolaget eller påverka bolagets behörighetstilldelning.

Andra åtgärder

För åtkomst till det aktuella systemet krävs enligt svar från bolaget inloggningsuppgifter och ett aktiverat konto. Dataskyddsombudet tolkar bolagets svar i denna del som att inga andra åtgärder vidtagits för att säkerställa att obehörig åtkomst till systemet inte sker. Dataskyddsombudet rekommenderar att bolaget klassar den information som hanteras i systemet och därefter gör en bedömning av om det krävs ytterligare säkerhetsåtgärder för att förhindra obehörig åtkomst till informationen.

Konsekvensbedömning och risker

GST har inte genomfört någon konsekvensbedömning för behandlingarna som sker i Quinyx. Anledningen anges vara att systemet infördes 2015. Dataskyddsombudet utgår från att det bolaget menar är att systemet infördes före det att dataskyddsförordningen trädde i kraft och att kravet på konsekvensbedömningar då inte fanns. Kravet på att genomföra konsekvensbedömningar finns emellertid för alla behandlingar, oaktat om de påbörjades före det att förordningen infördes eller inte.

Dataskyddsombudet rekommenderar att bolaget definierar vilka personuppgiftsbehandlingar som sker i Quinyx och bedömer ifall kraven för en konsekvensbedömning för dessa behandlingar är uppfyllda. Är kraven uppfyllda rekommenderas det att bolaget genomför en konsekvensbedömning.

Sammanfattade rekommendationer

- Dataskyddsombudet rekommenderar att bolaget konkretiserar instruktionen för Quinyx och tydligt anger hur och när behörigheter ska tilldelas/ändras. Det bör i denna instruktion även framgå vilken roll som har behörighet att begära att roller/behörigheter tilldelas och ändras.
- Konkretisera och komplettera instruktionen med rutiner för uppföljning av tilldelade behörigheter.
- Komplettera instruktion med rutiner för hur och när det är aktuellt att ta fram loggar i systemet. Det bör också förtydligas vad som utgör misstanke om oegentlighet och när kontroll ska ske utifrån en sådan misstanke.

- Bolaget rekommenderas att definiera sina personuppgiftbehandlingar i Quinyx, bedöma om de uppfyller kraven för när en konsekvensbedömning ska göras samt i förevarande fall genomföra en konsekvensbedömning.

Bilagor

- Information om fördjupad kontroll 2022
- Frågeunderlag fördjupad kontroll 2022, del 1 och 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 Quinyx. 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 Quinyx.

- 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 15 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 Quinyx? (t.ex. personnummer, löneuppgifter, uppgifter om hälsa osv.)
- Hur många registrerades personuppgifter hanteras i systemet?
- Ange vad skillnaden är mellan de angivna rollerna/behörigheterna (vilka olika uppgifter de får tillgång till och vad de t.ex. kan se eller ändra)
- Hur många personer har respektive behörighet/roll?
- Föreligger det inbyggda svårigheter i Quinyx att begränsa behörigheterna på så vis att personer enbart kan se sådana uppgifter som tillhör till det egna bolaget? Varför/varför inte?
- Hur kontrolleras personuppgiftsbiträdens behörigheter i systemet?
- Finns det instruktioner till personuppgiftsbiträdet/biträdena? Om ja, översänd dessa. Om nej, varför inte?
- Det anges i svar på del 1 att kontroll av loggar kan ske när misstanke om oegentligheter finns. Ange vad som kan utgöra ” misstanke om oegentligheter”.
- 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.