Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Gryaab AB

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

[1] Art kel 39 i GDPR
[2] Art kel 38.3 i GDPR

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

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 Delta V har granskats. Syftet med kontrollen är att granska om dataskyddsombudet ser risker i verksamhetens arbete med behörighetsstyrning utifrån kraven i artikel 32 GDPR.

Verksamheten lämnades följande rekommendationer:

- Definiera vad som kan utgöra ett larm som generar att loggar kontrolleras för att undvika övervakning av anställda.
- Kontrollera behörigheter även vid ändring av anställning inom bolaget för att förhindra att medarbetare kommer åt uppgifter de inte behöver vid en ny/ändrad anställning.
- Kontinuerligt se över de behandlingar som sker i systemet för att ha koll på de risker som förekommer, och i de fall det krävs, genomföra tröskelanalys och/eller 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.	

2.4 Gryaab 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

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

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:

Dataskyddsombudet har inget att invända mot bolagets skattning gällande den interna dataskyddsorganisationen. Det finns dock utmaningar i att två av tre inom dataskyddsorganisationen är nya i rollerna som dataskyddskontakt. Det är därför extra viktigt att bolaget lyfter dataskyddsfrågor även på en högre nivå samt att det finns dokumenterade rutiner som kan omhändertas av de som är nya. Eftersom arbetet har fungerat bra hittills ser dataskyddsombudet inga hinder i att de nya dataskyddskontakterna kan upprätthålla det goda interna arbetet. Bolaget behöver arbeta med att integrera dataskyddet i det dagliga arbetet i alla delar av verksamheten samt fastställa vilka befattningar/roller inom bolaget som har utpekat ansvar och mandat att fatta beslut i olika dataskyddsfrågor.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning inom kontrollpunkten indikerar att inga större risker föreligger men att arbete ändock kvarstår med personuppgiftsincidenter. Dataskyddsombudet har tidigare granskat bolagets hantering av incidenter och de rekommenderade åtgärderna har vidtagits, därför har dataskyddsombudet inga invändningar mot skattningen. Enligt uppgift har bolaget dokumenterat inträffade personuppgiftsincidenter under 2022 och ingen har behövt anmälas till tillsynsmyndigheten. Dataskyddsombudet rekommenderar att verksamheten regelbundet informerar i den egna organisationen om vad en incident är för att säkerställa att rutinerna är kända och följs. Samtidigt bör inträffade incidenter följas upp så verksamheten för att identifiera återkommande incidenter och kunna sätta in åtgärder i förebyggande syfte.

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:

Bolagets svar indikerar att stora risker fortfarande finns kopplat till bolagets arbete med biträdesavtal och andra överenskommelser. Årets skattning är något sämre än förra året trots att dataskyddsombudet granskade kontrollpunkten förra året där bolaget uppgav att alla åtgärder vidtagits. Dataskyddsombudet kopplar resultatet till att dataskyddsorganisationen ändrats och de nya dataskyddskontakterna är osäkra på vilka rutiner som finns inom bolaget. Bolaget behöver ta fram rutiner för att kontinuerligt genomföra efterlevnadskontroller, bedöma om andra överenskommelser/avtal behövs utifrån omständigheterna samt kunna bedöma hela kedjan av underbiträden. Dataskyddsombudets rekommendation är att bolaget bör se över vilka biträdessituationer som föreligger och ta fram biträdesavtal där det behövs om sådana saknas.

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:

Bolaget skattning skiljer sig något åt från förra året, men beror troligtvis på den nya dataskyddsorganisationen. Dataskyddsombudet har förståelse för att nya arbetssätt tar tid innan de sätter sig. Ett komplett och aktuellt register kan vara ett hjälpmedel för dataskyddsarbetet, vilket bolaget bör sträva efter. Dataskyddsombudet rekommendation är att verksamheten ser över, uppdaterar och använder registret kontinuerligt för att ha bra koll internt på personuppgiftsbehandlingarna. Eftersom bolaget uppger att det saknas dokumenterad ansvarsfördelning över vem/vilka som ansvarar för uppdatering av behandlingar i registerförteckningen i motsats till vad som uppgavs vid förra årets fördjupade kontroll, är rekommendationen att bolaget försöker reda ut huruvida en sådan rutin finns. Bolaget bör även säkerställa och

förtydliga vem/vilka inom verksamheten som ansvarar för kontinuerlig uppdatering av registret.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning på kontrollpunkten kopplat till övergripande strategi för dataskydd indikerar att en del risker föreligger i arbetet. Bolaget uppger att det i stort sett saknas en övergripande strategi för dataskydd och att inget systematiskt arbete med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet föreligger. Dataskyddsombudet bedömer att även detta är kopplat till den nya dataskyddsorganisationen.

Bolaget behöver också identifiera och värdera informationstillgångar utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet.

Verksamheten rekommenderas att se till att säkra egna styrande dokument som berör behandling av personuppgifter samt säkra att de är kända och följs, vilket inkluderar egna regelbundna efterlevnadskontroller av dessa.

Rutiner för hantering av personuppgifter vid anordnande av fysiska och digitala sammankomster är särskilt viktiga för bolaget att ta fram, bland annat eftersom bolaget enligt sin hemsida erbjuder skolklasser att besöka bolagets anläggningar. Enligt uppgift från bolaget behandlas dock inga uppgifter om barn då endast lärare kontaktas vid skolklassbesök.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i bolagets bedömning. Olika befattningar i verksamheten kan kräva olika utbildningsinsatser varför en kartläggning av behovet är viktigt.

Dataskyddsombudet rekommenderar att bolaget regelbundet utreder behovet av utbildningsinsatser, dokumenterar och använder olika typer av informationsinsatser för att säkerställa att man upprätthåller en god kunskap i dataskyddsfrågor.

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:

Bolagets skattning innebär att det inte föreligger några risker kopplat till integritetspolicyn. Bolaget rekommenderas att uppdatera informationen med jämna mellanrum för att säkerställa att den uppfyller kraven enligt GDPR. Dataskyddsombudet har inte granskat bolagets integritetspolicy i detalj, men en efter en snabb överflygning kan dataskyddsombudet konstatera att integritetspolicyn inte beskriver några behandlingar i detalj. Dataskyddsombudet rekommenderar att bolaget ser över policyn och säkerställer att information lämnas på annat sätt, om policyn inte är ämnad att vara heltäckande.

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:

Bolagets skattning är lägre jämfört med föregående år och dataskyddsombudet instämmer i bedömningen att det föreligger en del risker kopplat till kontrollpunkten. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att bolaget ska kunna säkerställa principen om lagringsminimering enligt GPDR. Bolaget är osäkra på hur stor andel av bolagets personuppgiftsbehandlingar som har informationsklassificerats utifrån stadens riktlinje för informationssäkerhet, och kan inte svara på om informationen är aktuell och har kontrollerats det senaste året. Bolaget saknar också anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Dataskyddsombudet rekommenderar att bolaget ser över och åtgärdar detta. Bolaget rekommenderades förra året att åtgärda sina rutiner för hantering av personuppgifter i e-post och eftersom skattning fortfarande är låg kvarstår denna rekommendation. Rutiner för hantering av personuppgifter i e-post rekommenderades bolaget åtgärda förra året, och eftersom skattningen fortfarande är låg kvarstår den rekommendationen.

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:

Bolagets skattning på kontrollpunkten visar att det finns en del risker kopplat till arbetet med konsekvensbedömningar som behöver åtgärdas. Dataskyddsombudet instämmer i den bedömningen eftersom så vitt dataskyddsombudet vet har bolaget hittills enbart genomfört en regelrätt konsekvensbedömning. Dataskyddsombudets bedömning är dock att det troligtvis finns fler behandlingar som kräver konsekvensbedömningar.

Dataskyddsombudet bedömer att i den mån bolaget framöver kommer införa nya behandlingar som kan innebära stora risker för de registrerade behöver verksamheten öka sin kunskap kopplat till konsekvensbedömningar. Efter att bolaget har identifierat och registrerat de behandlingar som redan utförs, bör bolaget också se över riskerna kopplat till dessa. Dataskyddsombudet är behjälpligt vid bedömningar och ska involveras i konsekvensbedömningar.

Eftersom konsekvensbedömningsarbetet är ett sätt för bolaget att hantera de risker som föreligger med behandlingar och är en del i strategin för övergripande dataskydd, är dataskyddsombudets rekommendation att bolaget tar fram ett arbetssätt för att säkerställa efterlevnaden av GDPR.

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:

Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Eftersom dataskyddsombudet inte blivit involverad i några IT-projekt eller upphandlingar under året, saknas insyn i hur verksamheten arbetar i dessa frågor. Dataskyddsombudet vill påminna bolaget om att dataskyddsombudet ska involveras i alla frågor som rör dataskydd från start. Dataskyddsombudet vill dock lyfta, i och med att kunskapen om dataskydd generellt behöver höjas inom verksamheten, att det finns risker att dataskyddsperspektivet missas vid uppstart av IT-projekt och initierande av upphandlingar. Inbyggt dataskydd och dataskydd som

standard behöver tas med i kravställningen för att säkerställa efterlevnad vid upphandlingsfasen och senare.

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:

Bolaget har skattat sitt arbete blandat på kontrollpunkten kopplat till IT-system och digitala verktyg. Kopplat till behörigheter har detta berörts i den fördjupade kontrollen och behandlas inte ytterligare här. Bolaget uppger att det saknas rutiner för att systematiskt kunna följa upp och kontrollera att användning av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policyer. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma att följa upp lämnade rekommendationer och bolagets arbete under 2023.

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:

Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar inom bolaget. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas. Bolaget uppger att det finns en rutin för tillbakadragande av samtycke. Verksamheten rekommenderas att ta fram en process för att kunna ta fram efterfrågad information vid 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:

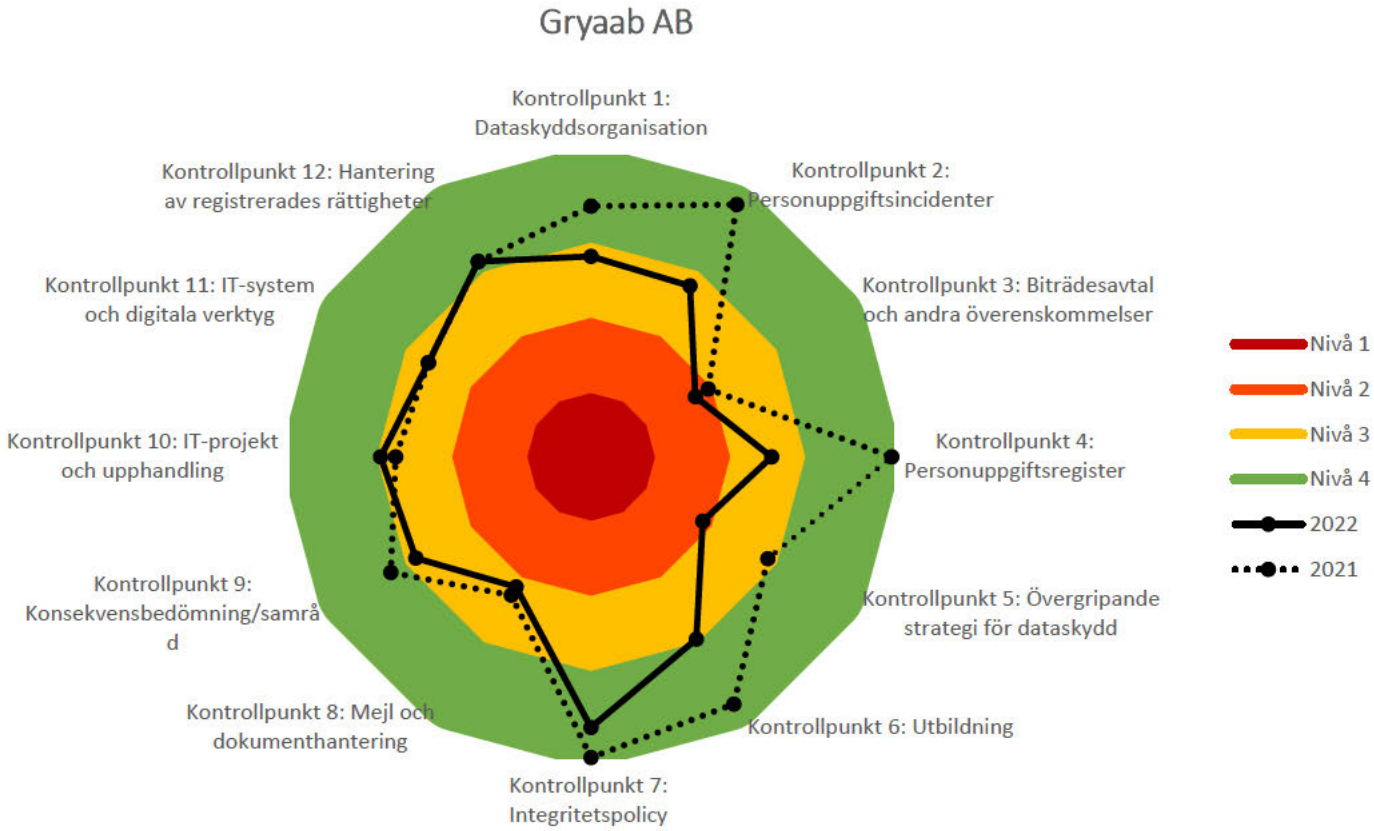
- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Verksamheten rekommenderas säkerställa att rutiner och åtgärder som vidtogs efter fördjupade kontrollen finns tillgängliga och är uppdaterade.
- Kontrollpunkt 5: Övergripande strategi för dataskydd
  Verksamheten rekommenderas att ta fram en övergripande strategi för dataskydd som utgår ifrån ett riskbaserat arbetssätt.
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Verksamheten rekommenderas implementera arbetet med konsekvensbedömningar i den övergripande strategin för dataskydd.

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 DeltaV hos Gryaab

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 i verksamheten.

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

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.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Tilldelning av behörighet utifrån bedömning och beslut om behörighet

Roller i systemet tilldelas enligt Gryaab utifrån att medarbetaren ska kunna utföra sitt jobb, vilket innebär att behörigheten främst baseras på vilken befattning man har. Ansvarig chef beslutar om behörigheten enligt en tabell i rutinen.

Utifrån underlaget bedömer dataskyddsombudet att det inom bolaget är tydligt vem som ska få vilken behörighet och anser att det är bra att en utpekad chef beslutar om behörigheten. Det säkerställer att inte vem som helst kan dela ut behörigheter inom bolaget och det är tydligt utpekat hur behörigheter sätts.

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.

Gryaab uppger att behörigheterna ses över varje gång någon slutar på bolaget, men också minst två gånger per år. Dataskyddsombudet anser att det är bra med översyn både vid avslut och två gånger per år, men rekommenderar också att bolaget gör en översyn ifall en medarbetare byter tjänst inom bolaget då det kan innebära ändring i behov av tillgång till personuppgifter.

Åtkomstkontroll/kontroll av loggar

[redacted]

Gryaab kunde inte på uppföljande fråga svara på vad ett exempel på larm kan utgöras av. Dataskyddsombudet kan därför inte bedöma hur när och hur ofta uppföljning eller

kontroll av loggar görs. Därför vill dataskyddsombudet uppmärksamma bolaget på att det är viktigt att detta tydligt regleras så att ingen onödig övervakning av de anställdas aktivitet sker i systemet. Bolaget rekommenderas att, där det är möjligt, identifiera vad ett larm kan vara och när bolaget ser ett behov av att kontrollera loggar för att undvika onödig kontroll av anställda i systemet.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

Gryaab har uppgett att ingen annan lagstiftning påverkar behörighetstilldelningen. Dataskyddsombudet ser ingen anledning att ifrågasätta bolagets bedömning.

Andra risker och åtgärder

Gryaab har uppgett att man vidtagit tekniska åtgärder för systemet men har inte identifierat några risker kopplat till obehörig åtkomst och felaktiga behörigheter.

[redacted]

Dataskyddsombudet anser att både tillgången till systemet och antalet personuppgifter som behandlas är begränsade till vad som är nödvändigt.

Gryaab har inte genomfört någon konsekvensbedömning då man anser att behandlingen inte innebär någon hög risk för de registrerade samt att man vidtagit flera åtgärder för att hålla säkerheten i systemet. Dataskyddsombudet instämmer, utifrån den information bolaget lämnat, i den här bedömningen.

Sammanfattade rekommendationer

- Definiera vad som kan utgöra ett larm som generar att loggar kontrolleras för att undvika övervakning av anställda.
- Kontrollera behörigheter även vid ändring av anställning inom bolaget för att förhindra att medarbetare kommer åt uppgifter de inte behöver vid en ny/ändrad anställning.
- Kontinuerligt se över de behandlingar som sker i systemet för att ha koll på de risker som förekommer, och i de fall det krävs, genomföra tröskelanalys och/eller konsekvensbedömning.

Bilagor

1. Informationsblad fördjupad kontroll behörighetsstyrning
2. Frågeutskick del 1
3. Frågeutskick 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 Delta V. 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 Delta V.

- 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 systemet?
- Hur många registrerades personuppgifter hanteras i systemet?
- Hur många personer har behörigheter (inom aktuella enheter, men inklusive personuppgiftsbiträde, administratörer)?
- Finns det ett personuppgiftsbiträde för behandlingen/systemet och finns det i sådana fall ett personuppgiftsbiträdesavtal?
- Hur kontrolleras personuppgiftsbiträdets behörigheter i systemet?
- Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
- Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
- Har ni identifierat specifika risker kopplat till nuvarande hantering av behörigheter? Varför/varför inte? Beakta såväl risker inifrån organisation som utanför (ex, intrång) för de registrerades rättigheter.
- Kan ni ge exempel på vad som kan trigga/utgöra ett larm som gör att ni kontrollerar loggarna?
- Vem ansvarar för att se över behörigheterna?

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.