Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Higab 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 i GDPR
[2] Artikel 38.3 i GDPR

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

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

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

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

2.2 Fördjupad kontroll

2.2.1 Kontroll av personuppgiftsincidenter 2022

Den fördjupade kontrollen har bestått av personuppgiftsincidenter. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och har därför lämnat ett antal rekommendationer till verksamheten för åtgärd.

Organisationen behöver ta fram en dokumenterad instruktion för hanteringen av personuppgiftsincidenter, den bör minst innehålla följande:

- Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
- Rutiner för hur arbetstagarna inom organisationen ska agera om en incident inträffar.

- En utsedd person eller en grupp som är ansvarig för att hantera personuppgiftsincidenter.
- Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten
- Rutiner för anmälan av incident till Integritetsskyddsmyndigheten inom 72 timmar efter upptäckten.
- Rutiner för vilken information som ska inkluderas i en anmälan till tillsynsmyndigheten
- Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.

2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har följt upp vilka åtgärder som vidtagits med anledning av lämnade rekommendationer.

Kontroll: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

Utifrån den sårbarhet som utgörs av att dataskyddsarbetet centreras kring en person (dataskyddskontakten) rekommenderar dataskyddsombudet bolaget att utöka bemanningen och skapa en större dataskyddsorganisation.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har en ny dataskyddskontakt sedan senhösten 2021 och dataskyddsarbetet sker i samverkan mellan Higabs säkerhetsansvariga och dataskyddskontakten. Bolaget har därmed vidtagit åtgärder i enlighet med lämnad rekommendation. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna.

Kontroll: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

De förbättringar som bolaget kan vidta är att dokumentera informationsklassningen av behandling/IT-system så att det framgår hur bolaget har kommit fram till respektive nivå utifrån konfidentialitet, riktighet och tillgänglighet.

Ytterligare förbättringsområde är att införa regelbundna dokumenterade riskanalyser utifrån informationssäkerhet/dataskydd.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med lämnade rekommendationer. Fortsatt uppföljning kommer 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 Higabs 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

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

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 bedömer verksamhetens självskattning som rimlig. Bolaget har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation samt uppföljning enligt punkt 2.2.2.ovan. Som ett led i ett systematiskt arbetssätt kommer dataskyddsombudet tillsammans med verksamheten att följa upp arbetet under 2023. Med ledning i bolagets egen skattning rekommenderas dock verksamheten redan nu verka för att dataskyddsorganisationen tillförs tillräckliga resurser.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Kontrollpunkten har i år också varit föremål för dataskyddsombudets fördjupade kontroll. Med ledning i det som framkommit i den fördjupade kontrollen gör dataskyddsombudet en annan bedömning än bolaget. Dataskyddsombudets uppfattning är att Higab saknar fullgoda rutiner för att upptäcka och hantera personuppgiftsincidenter. Bolaget rekommenderas därför att ta fram heltäckande rutiner för sin hantering i enlighet med vad som anges i den fördjupade kontrollen (bilaga 2).

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:

Verksamhetens självskattning i år är sämre än förra året. Resultatet indikerar att det finns risker som verksamheten behöver hantera. Bolaget uppger att man saknar

rutiner för att kontinuerligt genomföra efterlevnadskontroller av att anlita biträden liksom rutiner för att identifiera om avtal behöver upprättas. Bolaget uppger också att man saknar kompetens att bedöma hela kedjan av underbiträden vid anlitande av personuppgiftsbiträden. Dataskyddsombudet rekommenderar att bolaget säkerställer att biträdesavtal finns med alla leverantörer liksom rutiner för att säkerställa att biträden långsiktigt agerar i linje med dataskyddsförordningen både i upphandlingsfasen och senare. Bolaget behöver också skapa en arbetsmetod för uppdatering av biträdesavtalen vid legala eller interna förändringar.

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 skattning och bedömning är att det inte föreligger några risker kopplat till användningen av registret. Resultatet visar på en klar förbättring jämfört med föregående år vilket är positivt. Dataskyddsombudet ser dock en koppling till föregående kontrollpunkt, avseende biträdesavtalen, som bör finnas med i en aktuell och uppdaterad registerförteckning. Syftet med registerförteckningen är att det ska vara ett hjälpsamt verktyg för den interna dataskyddsorganisationen. Dataskyddsombudets rekommendation är att verksamheten också ser över, uppdaterar och använder registret kontinuerligt för att ha koll på verksamhetens personuppgiftsbehandlingar.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig. I den mån bolaget anordnar möten, sammankomster och liknande behöver rutiner för hantering av personuppgifter tas fram och beaktas. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet rekommenderar att bolaget regelbundet utreder behovet av utbildningsinsatser, dokumenterar och därigenom också säkerställer att man upprätthåller en god kunskap i dataskyddsfrågor. Olika befattningar kan kräva olika utbildningsinsatser i dess olika relevanta delar. Dataskyddsombudet uppmärksammade att ett flertal medarbetare deltog i dataskyddsenhetens utbildning för kommunikatörer vilket är positivt. Eftersom alla är olika och lär sig bäst på olika vis rekommenderas olika typer av informationsinsatser med jämna mellanrum.

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:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig. Verksamheten rekommenderas också säkerställa att de registrerade informeras om hur deras personuppgifter behandlas i alla digitala kanaler som bolaget använder. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten.

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 uppger en sämre skattning gällande rutiner för att kontrollera korrekt gallring i enlighet med gällande gallringsbeslut och dokumenthanteringsplan. För

att bolaget ska säkerställa principen om lagringsminimering är dataskyddsombudets rekommendation att bolaget tar fram en gallringsrutin samt även informerar medarbetarna att följa den.

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:

Över lag kvarstår en del förbättringsarbete under kontrollpunkten och bolaget behöver hantera riskerna kopplat till detta samt involvera dataskyddsombudet för att inhämta råd vid konsekvensbedömningar. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

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

Dataskyddsombudets kommentarer:

Verksamheten rekommenderas ha som rutin att dataskyddsombudet involveras från start i olika upphandlingar. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten

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:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten

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 uppger att man behöver öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas. Ytterligare förbättringsområde är att se över rutiner för att bedöma när en invändning mot en personuppgiftsbehandling är uppenbart ogrundad eller orimlig. Verksamheten behöver även säkerställa att det finns rutiner för att hantera ett tillbakadragande av samtycke. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma följa upp arbetet under 2023 tillsammans med verksamheten

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:

  Teckna personuppgiftsbiträdesavtal i samtliga fall där verksamheten bedömer att en biträdessituation föreligger.

  Ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet.

- Kontrollpunkt 6: Utbildning:

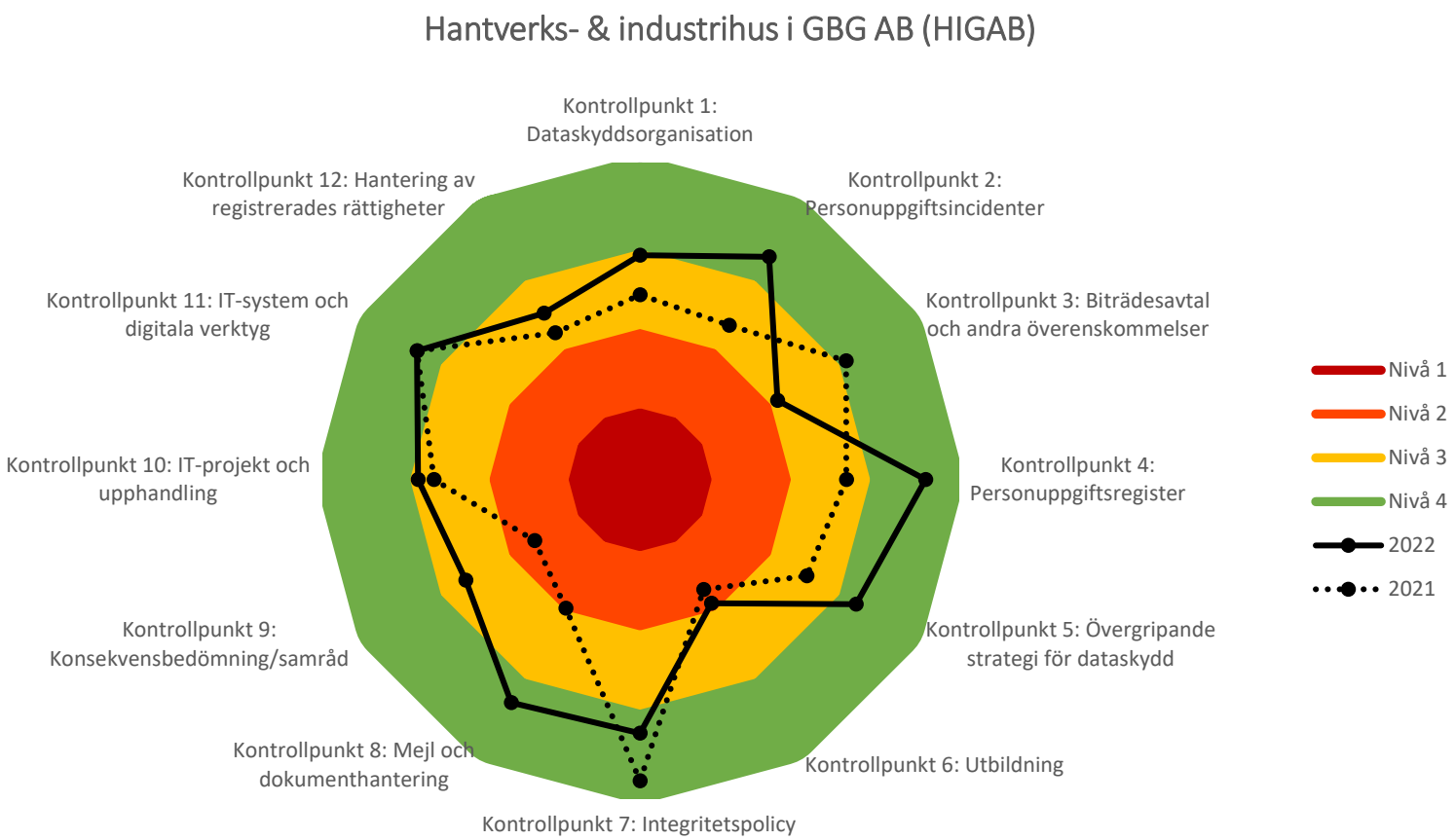
Higab rekommenderas att kartlägga och dokumentera behovet av och genomföra utbildningsinsatser för att öka medarbetarnas kunskap om dataskydd.

3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022

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



Fördjupad kontroll 2022: Higab

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Bakgrund

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om förvaltningens rutiner/handlingsplaner får önskat genomslag i praktiken. Kontrollen har genomförts i två delar där del ett har bestått av att verksamheten har ombetts att skicka in dokumentation av rutiner/handlingsplaner för hanteringen av incidenter och dokumentation över inträffade incidenter under 2021. Del två har bestått av frågor kopplade till organisationens incidenthantering.

lakttagelser från kontrollen

Personuppgiftsincidenter kan leda till allvarliga konsekvenser för registrerade personer och det är av stor vikt att de hanteras på ett korrekt sätt. Enligt dataskyddsförordningen ska vissa typer av personuppgiftsincidenter anmälas till tillsynsmyndigheten och i vissa fall ska även de registrerade informeras. Även de personuppgiftsincidenter som inte behöver anmälas till tillsynsmyndigheten ska dokumenteras.

IMY:s checklista vid personuppgiftsincidenter

Integritetsskyddsmyndigheten (IMY) har på sin hemsida publicerat en checklista för personuppgiftsansvariga att använda i sitt arbete med personuppgiftsincidenter. Den består dels av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter, dels vad som behöver göras vid redan inträffade incidenter. IMY lyfter bl.a. att de som behandlar personuppgifter behöver veta hur man identifierar en personuppgiftsincident och vikten av att rutiner och handlingsplaner finns på plats för att kunna begränsa och hantera en redan inträffad incident. Av rutinerna bör det framgå hur en bedömning av riskerna för de registrerade går till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten och om de registrerade ska informeras.

Rutiner och handlingsplaner

Bolaget har som svar på del 1 av denna kontroll delgett dataskyddsombudet sin rutin för hantering av personuppgiftsincidenter. Hanteringen av incidenter är en del av Higabs allmänna instruktion för behandling av personuppgifter. Dokumentet är mycket översiktligt och även om det förklaras på ett pedagogiskt sätt vad som är en personuppgiftsincident så saknas det enligt dataskyddsombudets mening en rutin för hur incidenter faktiskt ska upptäckas och hur bolaget praktiskt hanterar dessa. Det saknas till exempel information om vem som ska bedöma incidenter, vem som ska fatta beslut om att anmäla till tillsynsmyndigheten och när och vem som ska informera de registrerade. Kort sagt så är bedömningen att bolaget saknar en fullgod rutin/handlingsplan för sin incidenthantering.

Dataskyddsombudets rekommendationer

Higab behöver ta fram tydliga rutiner/beskrivningar för vad som ska bedömas vara en incident, här kan verksamheten med fördel ange flera exempel för att underlätta förståelsen för medarbetare. I rutinen ska det även i detalj framgå hur medarbetaren ska gå till väga vid misstanke om incident. Denna rutin bör delges samtliga chefer och medarbetare samt finnas lätt tillgänglig för genomläsning vid behov. Vidare bör organisationen se till att ta fram tydliga rutiner/beskrivningar om hur bedömningen görs avseende om det ska betraktas som en incident eller inte, om anmälan ska göras till tillsynsmyndigheten, samt när den registrerade ska informeras.

Det är inte alltid helt enkelt att göra de olika bedömningarna som krävs varför det är nödvändigt att det finns rutiner på plats, dels som stöd vid bedömningarna, dels så att någon annan i organisationen kan ta vid för de fall dataskyddskontakterna är frånvarande eller personalomsättning sker. Det är viktigt att rutinerna innehåller ett utpekat ansvar. Det är inte lämpligt att det endast är, till exempel, dataskyddskontakterna som är ansvariga för hanteringen av personuppgiftincidenter i organisationen utan ansvaret bör fördelas på flera personer i verksamheten.

Exempelvis bör den som ytterst ansvarar för den av incidenten berörda behandlingen vara med i utredningen av incidenten då det ofta är där som sakkunskapen finns. Det är knappast möjligt för en enskild individ att ha sådan koll på alla behandlingar i bolaget som krävs för att kunna utreda incidenter. Berör incidenten ett system bör lämpligtvis även den person som är ansvarig för systemet bli inkopplad vid utredningen och bedömningen av de åtgärder som behövs vidtas för att eliminera incidenten. Det är bra att organisationen kontaktar dataskyddsombudet vid behov om råd i bedömningarna men det är önskvärt om organisationen även har som rutin att alltid informera dataskyddsombudet om de incidenter som sker i organisationen. Detta eftersom den/ de registrerade har rätt att vända sig direkt till dataskyddsombudet med frågor och synpunkter.

Bolaget har angett att de inte haft någon händelse som utretts som en misstänkt incident under 2021. I en organisation är det normalt att det sker ett flertal incidenter varje år och det är troligt att så även har skett hos Higab trots att dessa inte upptäckts, rapporterats och bedömts. Bristande kunskaper om vad som kan vara en incident hos medarbetare kan vara en orsak till att organisationen inte haft några incidenter under 2021. Detta accentueras av förvaltningens svar på dataskyddsombudets uppföljande frågor i del två av denna fördjupade kontroll; där verksamheten på frågan om *hur Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej*, hänvisar till den allmänna instruktionen om hantering av personuppgifter. Denna instruktion hänvisar verksamheten också till som grund för bedömningen om när incidenter ska anmälas till tillsynsmyndigheten.

Dataskyddsombudets uppfattning efter att ha tagit del av dokumentet är dock att det endast innehåller en sådan allmänt hållen beskrivning av personuppgiftsincidenter att det svårligen kan anses utgöra en sådan rutin eller handlingsplan som vägleder medarbetarna i att identifiera och hantera personuppgiftsincidenter på ett korrekt sätt.

Andra orsaker till avsaknaden av incidenter kan vara att medarbetare vid mindre incidenter inte förstått/ansett det som värt att lägga tid på rapportering på grund av att det inneburit ringa konsekvenser för den registrerade. Ytterligare anledningar kan vara hög arbetsbelastning eller den allmänmänskliga känslan av att inte vilja skylta med sina tillkortakommanden. Avsaknaden av en dokumenterad rutin som medarbetarenkan följa vid misstanke om att en incident har skett kan också vara en orsak.

Sammanfattning

- Organisationen behöver ta fram en dokumenterad instruktion för hanteringen av personuppgiftsincidenter, den bör minst innehålla följande:
- Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
- Rutiner för hur arbetstagarna inom organisationen ska agera om en incident inträffar.
- En utsedd person eller en grupp som är ansvarig för att hantera personuppgiftsincidenter.
- Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten.
- Rutiner för anmälan av incident till Integritetsskyddsmyndigheten inom 72 timmar efter upptäckten.
- Rutiner för vilken information som ska inkluderas i en anmälan till tillsynsmyndigheten.
- Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.

Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022, hantering av personuppgiftsincidenter 2021 (del 1)
3. Fördjupad kontroll 2022, hantering av personuppgiftsincidenter 2021 (del 2)

Bilaga 1

Fördjupad kontroll 2022

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Personuppgiftsansvariga och personuppgiftsbiträden ska arbeta medvetet och proaktivt för att förhindra personuppgiftsincidenter. Om det ändå sker en incident ska det finnas förutsättningar för att hantera den snabbt och på rätt sätt. Den personuppgiftsansvarige är enligt artikel 33.5 GDPR skyldig att dokumentera samtliga inträffade incidenter, oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 GDPR, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska innefatta omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om det inte är osannolikt att en inträffad personuppgiftsincident medför en risk för registrerades fri- och rättigheter ska, enligt artikel 33 GDPR, den personuppgiftsansvarige anmäla incidenten till Integritetsskyddsmyndigheten inom 72 timmar efter det att personuppgiftsansvarig fått vetskap om incidenten. Den personuppgiftsansvarige behöver vid varje inträffad incident bedöma i vilken utsträckning som den uppkomna incidenten påverkar de registrerades fri- och rättigheter.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumentation av rutiner/handlingsplaner för att hantera incidenter samt er dokumentation avseende redan inträffade personuppgiftsincidenter. I del två ombeds ni att svara på ett antal frågor kopplade till er incidenthantering.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas in i juni.

Bilaga 2

Fördjupad kontroll 2022

Hantering av personuppgiftsincidenter under 2021

Del 1:

Dokumentation för er att skicka in till ert dataskyddsombud:

1. Rutiner/handlingsplaner/instruktioner för att hantera personuppgiftsincidenter
2. Dokumentation av inträffade personuppgiftsincidenter
    a. Dokumentation av incidenter som har anmälts till tillsynsmyndigheten
    b. Dokumentation av incidenter som endast har dokumenterats internt
3. Dokumentation av utredningar kring potentiella personuppgiftsincidenter

Underlaget ska ha inkommit till ert dataskyddsombud **senast den 7 mars 2022.**

Har du frågor, kontakta ditt dataskyddsombud.

Bilaga 3

Fördjupad kontroll 2022

Hantering av personuppgiftsincidenter under 2021

Del 2

Frågor att besvara:

1. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
2. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida incidenten ska anmälas till tillsynsmyndigheten.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
3. Hur ni säkerställer att era anställda vet vad en personuppgiftsincident är och hur de ska gå tillväga vid inträffade personuppgiftsincidenter.

Svar inkommit till ert dataskyddsombud **senast den 10 juni 2022.**

Har du frågor, kontakta ditt dataskyddsombud.