



Årsrapport för dataskyddsarbetet 2022

Got Event AB

2022-12-29

Innehåll

1	Dataskydd i kommunal verksamhet	3
1.1	Göteborgs Stads dataskyddsombud	3
2	Granskning av dataskyddsarbetet 2022.....	4
2.1	Dataskyddsombudets kontrollfunktion	4
2.2	Fördjupad kontroll.....	4
2.2.1	Kontroll av hantering av personuppgiftsincidenter 2021	4
2.2.2	Uppföljning av tidigare genomförda kontroller	5
2.3	Årlig kontroll av dataskyddsarbetet	5
2.3.1	Metod och risknivåer	6
2.4	Got Events dataskyddsarbete 2022	6
2.4.1	Kontrollpunkt 1: Dataskyddsorganisation	6
2.4.2	Kontrollpunkt 2: Personuppgiftsincidenter	7
2.4.3	Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	8
2.4.4	Kontrollpunkt 4: Personuppgiftsregister	8
2.4.5	Kontrollpunkt 5: Övergripande strategi för dataskydd	9
2.4.6	Kontrollpunkt 6: Utbildning	9
2.4.7	Kontrollpunkt 7: Integritetspolicy	10
2.4.8	Kontrollpunkt 8: E-post och dokumenthantering.....	10
2.4.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	11
2.4.10	Kontrollpunkt 10: IT-projekt och upphandling.....	12
2.4.11	Kontrollpunkt 11: IT-system och digitala verktyg	12
2.4.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	13
2.5	Sammanfattande rekommendationer.....	13
3	Bilagor	15

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 hantering av personuppgiftsincidenter 2021

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 bolagets rutiner/handlingsplaner får önskat genomslag i praktiken. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen lämnat följande rekommendationer:

- Komplettera rutinen med information i vilka fall dataskyddsombudet ska involveras.

- Komplettera rutinen med instruktioner/metod för hur en bedömning av risken för de registrerades fri- och rättigheter kan göras.
- Se över bolagets kunskap gällande vad en personuppgiftsincident är.
- Utbilda all personal om personuppgiftsincidenter och hantering av dessa.

2.2.2 Uppföljning av tidigare genomförda kontroller

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

Kontroll (2021): IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

- Slutföra rutinen för hur fritextfält ska hanteras i systemet Lime.
- Dokumentera informationsklassningen av behandlingar och IT-system.
- Förbättra informationen till registrerade i samband med avtalstecknande genom att tillhandahålla skriftlig information om bolagets hantering av personuppgifter.

Kommentarer och rekommendationer:

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

Kontroll (2021): IT-projekt och upphandling

Verksamheten gavs följande rekommendationer:

- Dokumentera hur dataskyddsperspektivet tas om hand vid upphandling och i IT-projekt.

Kommentarer och rekommendationer:

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





2.3 Årlig kontroll av dataskyddsarbetet

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

2.3.1 Metod och risknivåer

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

Beskrivning av risknivåer

Riskenivåer	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 Got Events 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 dataskyddsbudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsbudet 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.

Dataskyddsbudets kommentarer:

Resultatet visar att bolaget bedömer sig ha goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Av svaren framgår att roller och ansvar är tydligt utpekade och att information når rätt nivå inom bolaget. Skattningen visar samtidigt att det krävs ytterligare arbete för att

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

dataskydd ska bli en naturlig och integrerad del av det dagliga arbetet för alla medarbetare.

Även om bolaget har en intern dataskyddsorganisation bedömer dataskyddsombudet, utifrån gjorda iakttagelser under året, att den interna dataskyddsorganisationen behöver ges ett ökat stöd och mer resurser för att kunna få rätt förutsättningar att utföra arbetet. Bolaget rekommenderas därför se över vilka resurser och vilken kompetens man behöver inom verksamheten för att säkerställa dataskyddsperspektivet. Bolaget rekommenderas även framåt säkerställa att dataskyddsombudet på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter



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

Dataskyddsombudets kommentarer:

Av bolagets svar framgår att det finns dokumenterade rutiner och arbetssätt som ger goda förutsättningar för att upptäcka, utreda och analysera inträffade personuppgiftsincidenter samt informera de registrerade i händelse av en incident. Vidare har bolaget angett att personalen informeras om vad en personuppgiftsincident är samt hur de ska agera när en incident inträffar.

Dataskyddsombudet anser att det finns en diskrepans i bolagets svar om hur man arbetar med personuppgiftsincidenter och utfallet av inträffade incidenter hos bolaget. Ett bolag som hanterar den mängd personuppgifter som Got Event gör borde rimligtvis ha ett flertal inträffade incidenter varje år. Trots detta har verksamheten inte haft en enda rapporterad incident under 2021. Avsaknaden av incidenter indikerar att kunskapen om vad som utgör en personuppgiftsincident behöver öka inom verksamheten. Att ha få rapporterade incidenter behöver inte per definition innebära att allt fungerar som det ska, utan kan snarare tvärtom innebära att medarbetare inte kan identifiera när en incident inträffar. Det är viktigt att inträffade incidenter rapporteras så att de kan utredas och åtgärder vidtas för att liknande incidenter inte ska inträffa på nytt.

Bolaget rekommenderas därmed att utvärdera arbetssätt, rutiner och den information som medarbetarna har fått till sig för att bedöma eventuella åtgärder eftersom (den förväntade) effekten hittills tycks ha uteblivit. Bolaget behöver säkerställa att det finns tillräcklig kunskap hos medarbetare och rutiner på plats som ger förutsättningar för att identifiera, utreda och i förekommande fall anmäla incidenter. Det är också viktigt att det finns en kultur där rapportering av incidenter uppmuntras, för att säkerställa att mörkertal och underrapportering inte förekommer. Oavsett om det handlar om kunskap, rutiner, arbetssätt eller är en kulturfråga behöver verksamheten identifiera var det brister för att kunna arbeta

vidare med frågan, så att incidenter framledes identifieras, rapporteras, utreds och i förekommande fall anmäls till tillsynsmyndigheten.

Fler rekommendationer lämnas inom ramen för 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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Enligt verksamhetens skattning finns kvarstående risker framför allt vad gäller att genomföra efterlevnadskontroller av personuppgiftsbiträden, att bedöma hela kedjan av underbiträden samt huruvida överenskommelser eller avtal behöver tecknas när en leverantör anlitas.

Utifrån skattningen rekommenderas bolaget att ta fram en rutin för utförandet av regelbundna efterlevnadskontroller av anlitade personuppgiftsbiträden, en rutin/anvisning för att bedöma ansvarsförhållanden utifrån GDPR vid anlitan av en leverantör, samt en rutin för att kontrollera hela kedjan av underbiträden vid anlitan av ny leverantör.

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 har på denna punkt skattat sitt arbete högt. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget gjort, men avser att framåt kontrollera bolagets personuppgiftsbehandlingsregister för att se hur väl registret uppfyller kraven enligt GDPR.

Verksamheten rekommenderas säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret och att all nödvändig information då läggs in i registret. Det finns också ett behov av rutiner för att tillförsäkra att registret regelbundet uppdateras.

Den interna dataskyddsorganisationen rekommenderas även fundera över på vilket sätt personuppgiftsregistret kan användas som del i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd



Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolaget har genomgående skattat sitt arbete högt inom kontrollpunkten. Den risk som utifrån bolaget egna skattning kvarstår är kopplad till att bolaget inte regelbundet genomför interna kontroller för att säkerställa följsamhet gentemot GDPR. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning görs i frågan.

Utifrån skattningen rekommenderas bolaget att se över möjligheten för att regelbundet genomföra interna kontroller för att se hur dataskyddsförordningen efterlevs inom verksamheten, det vill säga följa upp och kontrollera så att de rutiner som finns får genomslag i praktiken.

2.4.6 Kontrollpunkt 6: Utbildning



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

Dataskyddsombudets kommentarer:

Utifrån bolagets skattning och gjorda iakttagelser under året bedömer dataskyddsombudet att det inom kontrollpunkten föreligger risker vad gäller den allmänna kunskapsnivån i dataskydd inom verksamheten.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Verksamheten rekommenderas därför fortsätta ge medarbetarna möjlighet att delta i utbildningar för att höja den allmänna kunskapsnivån om dataskydd. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser rekommenderas verksamheten även kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

Framåt uppmantras bolaget till att både använda dataskyddsenhetens e-utbildning ”Dataskydd på jobbet” som är tillgänglig för alla verksamheter i Göteborgs Stad, samt låta medarbetare delta vid de lärarledda utbildningar som enheten håller i.

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:

Informationskravet utgör en av grunderna i GDPR och handlar om att den registrerade ska få information hur hans personuppgifter behandlas. Dataskyddsombudets bedömer, oaktat bolagets skattning, att det inom kontrollpunkten föreligger risker som kräver åtgärder. Den högsta risken utgörs av att nuvarande integritetspolicy inte bedöms uppfylla kraven på information enligt artikel 13 och 14 GDPR, och att bolaget därför inte lever upp till informationsplikten. Ytterligare en risk utgörs av att de registrerade inte kan nå integritetspolicyn från samtliga av verksamhetens digitala kanaler på ett enkelt sätt.

För att bolaget ska kunna uppfylla sin informationsplikt rekommenderas verksamheten framåt prioritera arbetet med att se över integritetspolicyn och uppdatera den så att informationen uppfyller kraven enligt GDPR.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering



Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Principerna om uppgifts- och lagringsminimering är grundläggande i dataskyddsförordningen. Det ställs också höga krav på att hantera uppgifter tillräckligt säkert. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som bolaget gjort avseende risknivå kopplat till dokumenthantering, gallring och e-posthantering.

I sammanhanget rekommenderas dock bolaget följa upp och kontrollera så att utförandet av den faktiska gallringen, i olika system och på bolagets lagringsytor, genomförs i enlighet med vad som anges i dokumenthanteringsplanen.

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:

Skattningen på kontrollpunkten indikerar utifrån den övergripande risknivån att det finns identifierade risker som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. Dataskyddsombudet gör dock en annan bedömning. Utifrån skattningen på de olika områdena inom kontrollpunkten bedöms det finnas omfattande risker som kräver omedelbara åtgärder. Vidare noterar dataskyddsombudet att flera av svaren tycks vara motsägelsefulla och inte spegla de faktiska omständigheterna. Till exempel anges att bolaget har rutiner för att säkerställa att konsekvensbedömningar genomförs innan en riskfylld behandling påbörjas och att bolaget regelbundet involverar dataskyddsombudet för att inhämta råd vid konsekvensbedömningar, trots detta har inte en enda konsekvensbedömning genomförts. Det framgår även att bolaget endast har kontrollerat ca 25% av sina personuppgiftsbehandlings utifrån höga risker för de registrerades fri- och rättigheter. Det saknas dessutom planering för hur bolaget framåt ska genomföra konsekvensbedömningar för dessa behandlingar. Bolaget saknar även en dokumenterad rutin för att genomföra och dokumentera konsekvensbedömningar.

Trots att bolaget får en placering inom risknivå tre anges att inte en enda konsekvensbedömning genomförts, vilket får anses vara den viktigaste delen i kontrollpunkten. Att bolaget till viss del har rutiner på området spelar väldigt liten roll om inte konsekvensbedömningar också görs. I samband med genomgången av årsrapporten har dataskyddsombudet fått information om att det finns ett par pågående konsekvensbedömningar inom bolaget, vilket, även om det inte minskar risken, är positivt.

Sammantaget anser dataskyddsombudet att det inom kontrollpunkten finns omfattande risker som omgående behöver åtgärdas. Dessa utgörs både av risker för de registrerade, eftersom behandlingar där deras personuppgifter ingår inte har bedömts och risker för bolaget i form av förtroendeskada eller sanktionsavgifter vid en eventuell tillsyn. Dataskyddsombudet rekommenderar därför att bolaget framåt prioriterar arbetet med att genomföra konsekvensbedömningar. För att få en överblick och kunna planera arbetet framåt rekommenderas bolaget att som ett första steg kontrollera verksamhetens personuppgiftsbehandlings utifrån höga risker och bedöma för vilka behandlingar konsekvensbedömningar behöver genomföras.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling



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

Dataskyddsombudets kommentarer:

Dataskyddsombudet har under det gångna året inte involverats i någon upphandling som bolaget själva har hanterat. Om detta beror på att inga upphandlingar på detta område har skett under året är för dataskyddsombudet oklart, men utifrån detta kan dataskyddsombudet inte göra någon egen bedömning.

Bolaget rekommenderas framåt se över hur det kan säkerställas att dataskyddsombudet involveras i ett tidigt skede i uppstart av nya IT-projekt, vid införande av nya system/tjänster eller i samband med upphandlingar.

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 skattar genomgående samtliga områden inom kontrollpunkten högt, och den enda kvarstående risken utgörs, enligt bolaget egna skattning, av att bolaget ej har en målgruppsanpassad information för de digitala verktyg som används och som tillhandahålls kunder.

Vid genomgång av bolagets kommunikationskanaler har dataskyddsombudet noterat att bolaget använder flera sociala medier. Dataskyddsombudet vill här lyfta att denna hantering strider mot de rekommendationer som dataskyddsombudet lämnat gällande användningen av sociala medier (med amerikanska moderbolag). Frågan om användning av sociala medier bör även i grunden ses över. I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även Instagram och Youtube är exempel på sociala medier som överför personuppgifter till USA. Ingen av dessa

plattformar har angett att de vidtagit några extra skyddsåtgärder och utifrån det saknar alla överföringar som görs inom dessa tjänster laglig grund. När det gäller användningen av sociala medier rekommenderar dataskyddsombudet att bolaget kartlägger dessa behandlingar och genomför en konsekvensbedömning för att kontrollera att behandlingarna är förenliga med GDPR. Dataskyddsombudet avråder bolaget från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

Då bolaget angett att det finns en pågående konsekvensbedömning för behandlingen som innebär en användning av sociala medier rekommenderas bolaget så snart som möjligt involvera dataskyddsombudet i arbetet med denna.

Vidare delar dataskyddsombudet inte bolagets bedömning vad gäller användningen av cookies, då cookiebannern inte uppfyller kraven för ett giltigt samtycke enligt GDPR (eller best practice) samt då information om användningen av cookies ej tillhandahålls. Utifrån detta rekommenderas bolaget prioritera arbetet med att se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets webbsida uppfyller kraven enligt dataskyddsförordningen.

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:

Skattningen på kontrollpunkten indikerar utifrån den övergripande risknivån att det finns identifierade risker som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. Sammantaget bedömer bolaget att det finns goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet har inte blivit tillfrågad angående någon begäran från registrerade rörande deras möjlighet att utöva sina rättigheter, men har inte heller några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig.

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:

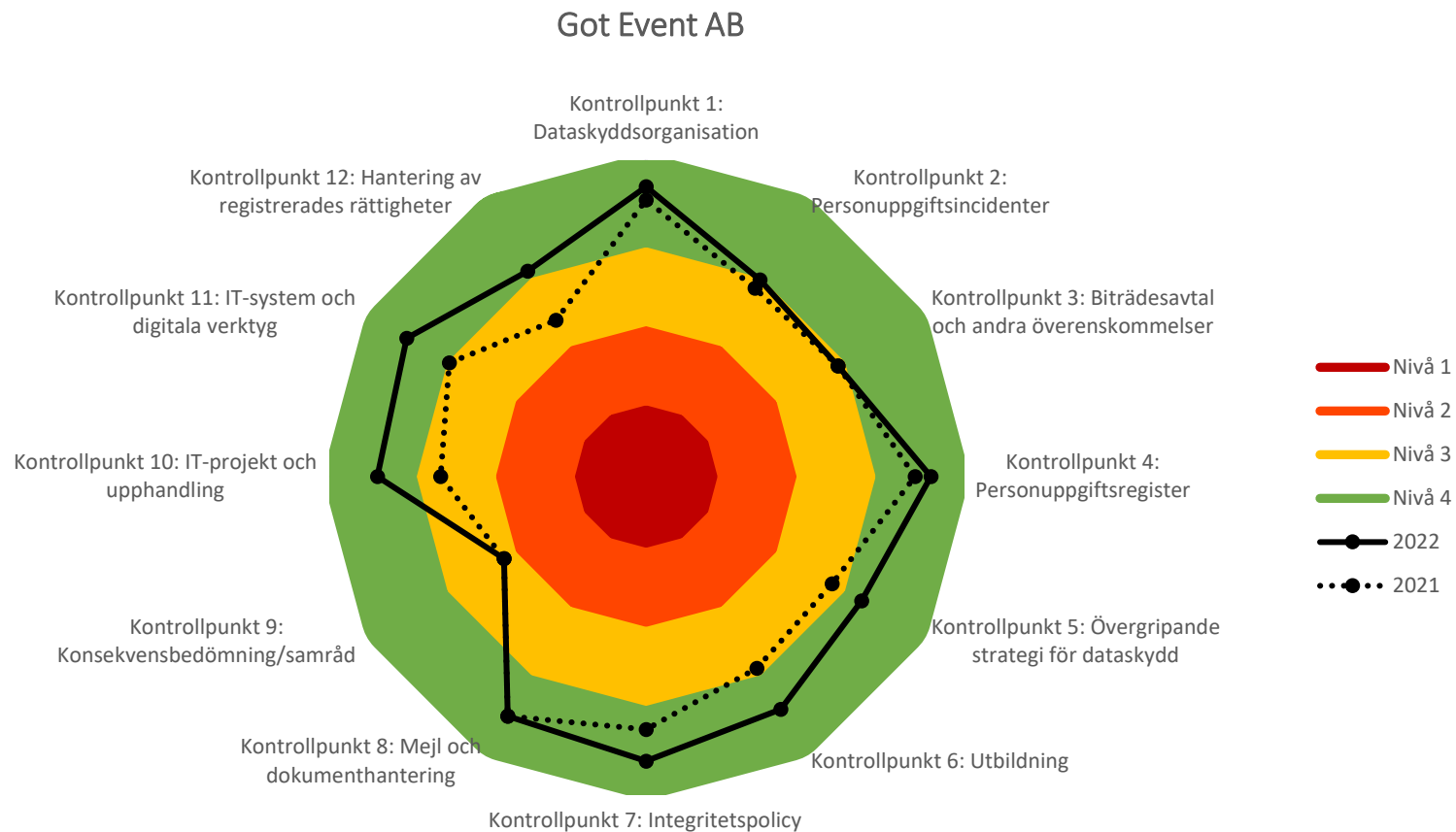
- Kontrollpunkt 11: IT-system och digitala verktyg
: Säkerställ användningen av cookies på hemsidan.
- Kontrollpunkt 7: Integritetspolicy
: Uppdatera nuvarande integritetspolicy så att informationen uppfyller kraven enligt GDPR.
- Kontrollpunkt 9: Konsekvensbedömningar/Samråd
: Kontrollera verksamhetens personuppgiftsbehandlingar utifrån höga risker och planera för genomförandet av konsekvensbedömningar i det fall detta krävs.
- Kontrollpunkt 6: Utbildning
: Öka den generella kunskapsnivån inom dataskydd hos medarbetare, inkl. hantering av personuppgiftsincidenter.

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

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 bolagets 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.

Iakttagelser 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 bl.a. av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter och vad som behöver göras vid redan inträffade incidenter. IMY lyfter att det av rutinerna bör framgå hur en bedömning av riskerna för de registrerade ska gå till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten. Det bör också framgå hur man bedömer om de registrerade ska informeras, hur det ska gå till och vad informationen ska innehålla.

Got Event AB:s hantering av personuppgiftsincidenter

Rutiner och handlingsplaner

Got Event AB (bolaget) har en rutin för hantering av personuppgiftsincidenter som gäller för alla anställda på bolaget. Rutinen innefattar en beskrivning av vad en personuppgiftsincident innebär och ett antal listade exempel. Det är vidare beskrivet hur anställda, vid misstänkta incidenter, ska hantera en personuppgiftsincident. Den anställda ska kontakta sin närmsta chef samt dataskyddskontakten. Rutinen innehåller en lista över vad den anställde ska sammanfatta för information för att sedan mejla den till dataskyddskontakten så snart som möjligt. Rutinen fastställer även att det är dataskyddskontakten som beslutar om incidenten ska anmälas till Integritetsskyddsmyndigheten och dokumenteras.

Personuppgiftsincidenter under 2021

Av det inskickade underlaget framgår att bolaget under år 2021 inte haft några personuppgiftsincidenter, däremot en personuppgiftsincident under 2020.

Information till anställda

Bolaget har i underlaget svarat att dataskyddsgruppen inom bolaget tar upp olika frågor och under våren 2021 var ämnet personuppgiftsincidenter. Information om personuppgiftsincidenter har även getts på chefsforum och chefer har uppmanats att ta upp ämnet vid APT inom bolaget.

Dataskyddsombudets rekommendationer

Rutiner och handlingsplaner

Bolaget har en rutin som inledningsvis redogör för vad en personuppgiftsincident innebär. Den innehåller exempel på händelser som utgör en incident, vilket är positivt. Förutsatt att anställda har grundläggande kunskaper i dataskydd bör denna beskrivning vara tillräcklig för att kunna identifiera en personuppgiftsincident. Det är även positivt att det finns tydligt beskrivet vem en anställd ska kontakta och vilken information som ska finnas dokumenterad. Rutinen saknar dock information gällande att involvera dataskyddombudet för bedömning av risk och aktuell hantering. Vidare saknar även rutinen hantering gällande i vilka fall som de registrerade ska informeras, vem som ska besluta om det samt vad informationen ska innehålla.

För att göra hanteringen mer lättillgänglig för verksamheten kan det enligt dataskyddsombudet finnas skäl att utöka rutinen med mer konkreta beskrivningar av hur en incident och risken för de registrerade ska bedömas. Att tydliggöra detta skulle göra det enklare att upptäcka och hantera incidenter korrekt inom verksamheten. Med tanke på att personuppgiftsincidenter kan vara komplicerade och svårutredda kan det också finnas anledning att komplettera rutinen med instruktioner kring att, i de fall det är lämpligt, kontakta andra roller inom bolaget för att på ett tillräckligt sätt kunna utreda incidenten. Sammantaget rekommenderar dataskyddsombudet att bolaget konkretiserar sin rutin och kompletterar den med en instruktion eller stödmaterial/metod som anger hur en incident och risken för de registrerade kan bedömas.

Personuppgiftsincidenter under 2021

Bolaget har angett att de inte haft någon personuppgiftsincident under 2021. Inom en verksamhet är det normalt att det sker ett flertal incidenter varje år och det är troligt att så även har skett hos bolaget, trots att det inte upptäckts, dokumenterats och bedömts. Ett felskickat mejl är exempelvis den vanligast förekommande personuppgiftsincidenten, vilket inte hade varit förvånande om bolaget hade haft vid ett eller flera tillfällen under året 2021.

Information till anställda

Vad gäller information till anställda, och hur det säkerställs att anställda vet vad en personuppgiftsincident innebär så är det viktigt att bolaget aktivt arbetar med frågan att utbilda sin personal om personuppgiftsincidenter och hantering av dessa. Det framgår emellertid inte av underlaget att det finns en rutin för att säkerställa att informationen om personuppgiftsincidenter når alla som behandlar personuppgifter och som behöver kunna identifiera en incident. Med beaktande av att det inte finns några dokumenterade personuppgiftsincidenter ställer sig dataskyddsombudet tveksam till om anställda har tillräcklig kunskap om vad en incident kan vara. Dataskyddsombudet rekommenderar därför att bolaget ser över att ytterligare utbilda sina anställda i vad en



personuppgiftsincident kan vara och hur den ska hanteras, för att säkerställa att incidenter inte missas.

Sammanfattning

- Komplettera rutinen med information i vilka fall dataskyddsombudet ska involveras.
- Komplettera rutinen med instruktioner/metod för hur en bedömning av risken för de registrerades fri- och rättigheter kan göras.
- Se över medarbetares kunskap gällande vad en personuppgiftsincident är.
- Utbilda all personal om personuppgiftsincidenter och hantering av dessa.

Bilagor

- Information om fördjupad kontroll 2022.
- Frågeunderlag fördjupad kontroll 2022, del 1 och del 2.

Information om 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. Dokumentationskyldigheten 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 årsrapporten.

Fördjupad kontroll 2022

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

Del 1: Dokumentation för er att skicka in till dataskyddsombudet:

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 dataskyddsombudet **senast den 15 mars 2022**.

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.



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.

Svaren ska ha inkommit till ert dataskyddsombud **senast den 10 juni 2022**.

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.