Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Liseberg 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 kamerabevakning 2022 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 Lisebergs 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 10

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 13

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter 14

2.5 Sammanfattande rekommendationer 15

3 Bilagor 16

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 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 kamerabevakning 2022

Den fördjupade kontrollen har bestått av en kontroll av bolagets användning av kamerabevakning. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

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

- Utred och dokumentera bedömningar gällande ändamål/rättslig grund för kamerabevakning av köer till attraktionerna.
- Dokumentera gjorda bedömningar avseende tillståndsplikt.
- Genomför konsekvensbedömningar för behandlingen/behandlingarna, annars tydligt dokumentera varför de inte uppfyller kraven för detta enligt GDPR.

- Tydligt motivera och dokumentera varför lagringstid om 7 respektive 30 dagar är nödvändig (utifrån att huvudregeln är 72 h).
- Komplettera informationen som ges avseende kamerabevakningen med ändamål för bevakning av köer, samt förtydliga delarna gällande lagringstid och tredjelandsöverföringar.
- Se över personuppgiftsbiträdesavtal och instruktioner.

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): Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

- att dokumentera arbetssätt och eventuellt ansvar och mandat för bolagets dataskyddsorganisation.

Kommentarer och rekommendationer:

Verksamheten har angett att de har vidtagit samtliga åtgärder i enlighet med lämnade rekommendationer. Fortsatt uppföljning kommer att ske inom ramen för de fasta kontrollpunkterna om inget särskilt föranleder att punkten behöver följas upp separat.

Kontroll (2021): Personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Att i kommande utbildningsinsatser i dataskydd utbilda i vad som kan vara en personuppgiftsincident och hur medarbetarna ska agera när de misstänker att en personuppgiftsincident har skett.
- Tydliggöra vilka funktioner som har delegation avseende anmälan av personuppgiftsincidenter inom bolaget.

Kommentarer och rekommendationer:

Verksamheten har angett att de har vidtagit samtliga åtgärder i enlighet med lämnade rekommendationer. Samtidigt har dataskyddsombudet även i årets årsrapport kunnat se att det inom kontrollpunkten föreligger höga risker som kräver ytterligare åtgärder. Fortsatt uppföljning kommer därför att ske under 2023.

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 Lisebergs dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

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

Dataskyddsombudets kommentarer:

För att dataskydd ska kunna anses vara en integrerad del av det dagliga arbetet krävs att det på samtliga nivåer inom bolaget finns kunskap och medvetenhet om dataskydd. Det krävs också formella beslut i frågor rörande dataskydd och att dessa tas på rätt nivå för att ge riktning och vägledning åt bolaget i övrigt.

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. Trots detta visar skattningen samtidigt att den interna organisationen för dataskyddsarbetet inte bedöms ha tillräckligt med resurser till sitt förfogande för att kunna bedriva ett systematiskt dataskyddsarbete.

Bolaget rekommenderas därför se över vilka resurser och vilken kompetens man behöver inom verksamheten för att säkerställa dataskyddsperspektivet. Bolaget rekommenderas även att 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 personuppgiftincidenter.

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. Enligt verksamhetens skattning finns enbart kvarstående risker vad gäller att systematiskt följa upp inträffade incidenter i dataskyddsarbetet.

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 Liseberg gör borde rimligtvis ha ett flertal inträffade incidenter varje år. Trots detta har verksamheten enbart haft ett fåtal incidenter under 2021 och 2022. 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.

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 vad gäller att genomföra efterlevnadskontroller av anlitade biträden och rutiner för att bedöma behov av avtal eller överenskommelser vid nya samarbeten. Ytterligare en risk utgörs av att bolaget har angett att det för cirka 75 % av anlitade personuppgiftsbiträden finns tecknat biträdesavtal, vilket innebär att det saknas för cirka 25 %. Utifrån att det är ett krav att reglera ansvarsförhållandena vid anlitande av ett biträde rekommenderas bolaget att se över för vilka biträden som avtal saknas och säkerställa att sådana upprättas.

Utifrån skattningen rekommenderas bolaget även att ta fram en rutin för utförandet av regelbundna efterlevnadskontroller av anlitade personuppgiftsbiträden, samt en rutin/anvisning för att bedöma ansvarsförhållanden utifrån GDPR när leverantörer anlitas eller samarbeten sker.

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, och sammantaget genererar verksamhetens svar ett resultat som innebär att inga direkta risker är identifierade. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget gjort, men avser att framåt kontrollera bolagets personuppgiftsregister för att se hur väl registret uppfyller kraven enligt GDPR.

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:

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 vad gäller avsaknaden av en övergripande strategi för arbetet med dataskydd, att man ej arbetar riskbaserat med dataskyddsfrågor samt att rutiner för att efterleva GDPR vid fysiska och digitala sammankomster saknas.

Ett systematiskt dataskyddsarbete bör bedrivas utifrån övergripande strategier för verksamheten avseende både dataskydd och informationssäkerhet. Då svaren indikerar att det inom bolaget saknas en överblick och tydlig styrning i hur dataskyddsarbetet ska bedrivas, rekommenderas bolaget se över hur dataskyddsfrågor kan integreras i det övriga informationssäkerhetsarbetet. Det är också viktigt att bolaget framåt identifierar vilka som är de största riskerna inom verksamheten och ser över hur arbetet med att hantera dessa ska prioriteras. Bolaget behöver även säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet.

Bolaget har i dialog med dataskyddsombudet angett att det inom verksamheten pågår ett arbete med att ta fram ett ”PU-direktiv” (personuppgiftsdirektiv), med syftet att stärka dataskyddsarbetet inom bolaget. Bolaget har under året även tagit fram ett årshjul för hur dataskyddsarbetet ska bedrivas internt. Det är positivt att bolaget vidtagit dessa åtgärder, och framåt rekommenderas bolaget involvera dataskyddsombudet i arbetet.

2.4.6 Kontrollpunkt 6: Utbildning

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

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 vad gäller att kartlägga vilken nivå av dataskyddskunskap som krävs för olika befattningars arbete samt planera för att genomföra informations- och utbildningsinsatser.

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Det är mycket positivt att bolaget, på olika sätt, arbetar med att utbilda och informera medarbetare i dataskyddsfrågor.

Verksamheten rekommenderas därför även fortsättningsvis ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd. Vidare, för att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser, rekommenderas verksamheten kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

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:

Bolaget har på denna punkt skattat sitt arbete högt och sammantaget genererar verksamhetens svar ett resultat som innebär att inga direkta risker är identifierade. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget gjort, men avser framåt kontrollera integritetspolicyn för att se hur väl informationen i denna uppfyller kraven enligt GDPR.

För att bolaget ska kunna bibehålla denna status är det viktigt att man fortsätter arbeta aktivt med att uppdatera informationen.

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:

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 vad gäller att informationsklassificera personuppgiftsbehandlingar och att informera registrerade. Utifrån skattningen är dataskyddsombudets bedömning att verksamheten inom dessa punkter behöver vidta åtgärder.

Vidare anger bolaget att de har informationsklassificerat ca 25 % av sina personuppgiftsbehandlingar och att för ungefär hälften av dessa är informationen aktuell (som innebär att de har kontrollerats senaste året). För att kunna ange hur information ska hanteras i olika lagringsytor är det viktigt att informationsklassificera sina personuppgiftsbehandlingar och att regelbundet säkerställa att informationen är aktuell. Annars riskerar personuppgifter att hanteras på ytor som inte uppnår en tillräcklig säkerhetsnivå. Bolaget rekommenderas därför framåt se över hur det kan säkerställas att informationsklassificeringar genomförs samt regelbundet kontrolleras/följs upp.

Bolaget behöver också säkerställa att de registrerade, vid kontakt med verksamheten, får information om hur deras personuppgifter hanteras. Bolaget rekommenderas ta del av Göteborg Stads mall för e-postsignatur, där det framgår att en länk till hanteringen av verksamhetens personuppgifter ska infogas i signaturen, och lägga till en sådan länk i bolagets e-postsignatur.

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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bedöms vara omfattande och kräver omgående åtgärder. Enligt verksamhetens skattning finns kvarstående risker vad gäller avsaknad av rutiner och metod för arbetet med konsekvensbedömningar. Riskerna gäller både genomförande och uppdatering av konsekvensbedömningar, samråd med dataskyddsombudet, beslut om att acceptera risker samt uppföljning av beslutade åtgärder.

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Det är därför mycket viktigt att verksamheten säkerställer att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingar och att det finns rutiner för att genomföra och dokumentera konsekvensbedömningar.

Utifrån de höga risker som föreligger inom kontrollpunkten bedömer dataskyddsombudet att verksamhetens arbete med konsekvensbedömningar under 2023 behöver prioriteras. Verksamheten rekommenderas i arbetet fokusera på att kontrollera verksamhetens personuppgiftsbehandlingar utifrån höga risker och bedöma för vilka behandlingar konsekvensbedömningar behöver genomföras, samt ta fram en plan för arbetet framåt. Inom ramen för arbetet behöver bolaget även komplettera nuvarande rutin med de delar som saknas, inkl. att tydliggöra vem/vilka befattningar som har mandat att fatta beslut inom ramen för arbetet med konsekvensbedömningar, hur dessa beslut ska dokumenteras samt att dataskyddsombudet ska rådfrågas/involveras vid genomförandet av en konsekvensbedömning.

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:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året rådfrågats i enstaka frågor inom kontrollpunkten, men har ej varit involverad i någon upphandling som bolaget själva hanterat och kan därför inte göra någon egen bedömning i frågan.

Dataskyddsombudet rekommenderar verksamheten att säkerställa att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Vidare, då bolaget själva identifierat att det saknas rutiner för att involvera dataskyddsombudet från start i dessa processer, rekommenderas verksamheten att 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 har genomgående skattat sitt arbete högt inom kontrollpunkten. Den risk som utifrån bolagets egna skattning kvarstår gäller att systematiskt följa upp att användningen av system och digitala verktyg följer antagna rutiner/riktlinjer/policys.

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 vidare bolaget från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

Vidare delar dataskyddsombudet inte bolagets bedömning vad gäller användningen av cookies, då cookiebannern inte uppfyller kraven för ett giltigt samtycke (eller best practice) enligt GDPR. Vidare har dataskyddsombudet kunnat konstatera att bolaget använder sig av analysverktyg som tillhandahålls av amerikanska biträden (genom till exempel Google Analytics och Facebook pixel), vars användning bedömts vara oförenliga med GDPR i tillsynsbeslut från flera europeiska tillsynsmyndigheter. Därtill har den svenska tillsynsmyndigheten IMY vid tiden för denna rapport (december 2022) flera pågående tillsynsärenden gällande användningen av Google Analytics. I dialog med bolaget har dataskyddsombudet informerats om att det internt ska ha fattats beslut om att fortsätta använda Google Analytics trots identifierade risker och avrådan från dataskyddsombudet, då fördelarna med verktyget bedömts vara högre än riskerna. Dataskyddsombudet har efterfrågat den dokumentation som finns kopplat till beslutet, till exempel underlag

och beslutsformulering, men någon sådan dokumentation anges ej finnas. Då ett beslut om fortsatt användning av en tjänst som konstaterats oförenlig med gällande lagstiftning i praktiken innebär ett beslut om att frångå lagen är dataskyddsombudet bedömning att detta (förutsatt att ett sådant beslut kan fattas) behöver fattas, alternativt informeras om, på högsta ansvarsnivå. Bolaget rekommenderas därför säkerställa att högsta ansvarsnivå, i detta fall styrelsen, är informerad om beslutet samt att beslutet, med tillhörande underlag, dokumenteras internt.

Oaktat ovan kvarstår dataskyddsombudets tidigare lämnade rekommendation till bolaget avseende att upphöra med behandlingarna omedelbart. Rekommendationen att upphöra med behandlingarna baseras på den höga risk användningen av dessa funktioner innebär för såväl registrerade som bolaget.

Under 2023 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:

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 vad gäller att ta reda på om det finns en utbredd medvetenhet om inom verksamheten om när de registrerades rättigheter begränsas, samt rutiner för att hantera detta och för att bedöma när en registrerads invändning mot en personuppgiftsbehandling är uppenbart ogrundad eller orimlig.

Då skattningen även visar att medarbetares kunskaper om vilka rättigheter som registrerade har enligt GDPR skulle kunna förbättras ytterligare, rekommenderas bolaget att ta med denna fråga i kommande utbildnings- och informationsinsatser. Även övriga identifierade risker (kopplat till medarbetares kunskaper) inom kontrollpunkten skulle med fördel kunna hanteras på samma sätt. Utöver det rekommenderas bolaget även att komplettera nuvarande rutin för hantering av registerutdrag, med anvisningar för hur en uppenbart ogrundad eller orimlig invändning ska hanteras.

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 (analysverktyg) på hemsidan.
- 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