Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Renova AB

2022-12-21

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 hanteringen av personuppgiftsincidenter 2021 (2022)

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 till verksamheten:

- Komplettera rutinen med instruktioner/metod för hur en bedömning av incident samt risken för de registrerades fri- och rättigheter kan göras.

- Komplettera rutinen med vem som beslutar gällande att bedöma om en anmälan till Integritetskyddsmyndigheten ska göras.
- Se över medarbetares kunskap gällande vad som är en personuppgiftsincident.
- Utbilda medarbetare om personuppgiftincidenter och hantering av dessa.
- Se över behovet av en rutin/plan för att regelbundet informera medarbetare om personuppgiftsincidenter och den interna incidenthanteringen.

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): Positioneringsteknik (GPS)

Verksamheten gavs följande rekommendationer:

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har frågor som kvarstår att hantera inom denna kontroll. En åtgärd som vidtagits är att bolaget har uppdaterat registret med alla aktuella behandlingar där rättslig grund och ändamål framgår, vilket är positivt. Bolaget har också påbörjat arbetet med ett antal konsekvensbedömningar, men på grund av brister i hantering, såväl som i kommunikationen emellan parterna, har dataskyddsombudet inte lämnat några rekommendationer på de underlag som tagits fram. Dataskyddsombudet bedömer det vara positivt att bolaget påbörjat arbetet med konsekvensbedömningar för riskfyllda behandlingar, och kommer under början av 2023 prioritera att ge en första återkoppling på de framtagna underlagen. Därefter kommer det vidare arbetet med dessa att fortsätta i samråd med bolaget 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 Renovas dataskyddsarbete 2022

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

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

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

Dataskyddsombudets kommentarer:

Skattningen visar att det inom punkten föreligger risker som behöver åtgärdas. Bolaget har angett att dataskydd inte är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten, samt att nuvarande dataskyddsorganisation inte har tillräckliga resurser. Dataskyddsombudets iakttagelse är att det dataskyddsarbete som bedrivs utgörs av punktinsatser med hjälp av konsulter, vilket bedöms utgöra en risk för bolaget.

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

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

behöver också 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:

Verksamhetens skattning visar på risker framför allt vad gäller att följa upp incidenter och informera medarbetare om vad en personuppgiftsincident är och vad medarbetare ska göra när en incident inträffar. Att enbart en incident inträffat 2021 indikerar att kunskapen om vad som utgör en personuppgiftsincident behöver öka inom verksamheten. Bolaget rekommenderas utifrån svaren fokusera på att informera medarbetare samt utveckla ett arbete med att systematiskt följa upp inträffade incidenter.

Fler rekommendationer lämnas inom ramen för den fördjupade kontrollen.

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:

Skattningen visar att det inom punkten föreligger risker som bedöms vara omfattande och/eller kräver omgående åtgärder. Biträdesavtal anges vara tecknade med ca 50% av anlitade biträden. Bolaget rekommenderas därför prioritera arbetet med att se över för vilka biträden avtal saknas och säkerställa att dessa upprättas. Enligt verksamhetens skattning finns även risker framför allt vad gäller att genomföra efterlevnadskontroller av personuppgiftsbiträden och att bedöma hela kedjan av underbiträden samt huruvida överenskommelser eller avtal behöver tecknas när en leverantör anlitas.

Utifrån skattningen rekommenderas bolaget att ta fram rutiner för:

- regelbundna efterlevandskontroller av anlitade personuppgiftsbiträden

- att bedöma ansvarsförhållanden utifrån GDPR vid anlitande av en leverantör
- att kunna kontrollera hela kedjan av underbiträden vi anlitande av nytt biträde

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 framåt kontrollera den gjorda skattningen för att se hur väl registret uppfyller kraven enligt dataskyddsförordningen.

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:

Bolagets skattning visar att det saknas en överblick och en tydlig styrning i hur dataskyddsarbetet bedrivs, vilket innebär en risk eftersom man då bland annat riskerar att fokusera sina resurser på fel frågor. Bolaget rekommenderas därför framåt att prioritera arbetet med att identifiera vilka som är de största riskerna inom verksamheten och se över hur arbetet med att hantera dessa ska prioriteras.

Bolaget rekommenderas även ta fram en övergripande strategi för arbetet med dataskydd men även en informationssäkerhetspolicy som anger hur personuppgifter kan behandlas i exempelvis IT-system, datorer och mobila enheter. Bolaget behöver även ta fram rutiner för hantering av fysiska och digitala sammankomster,

och se över möjligheten för att regelbundet genomföra interna kontroller för att se hur dataskyddsförordningen efterlevs inom verksamheten.

Bolaget uppger i dialog (december 2022) med dataskyddsombudet att det finns övergripande styrning och ledning, men att bristerna finns i att de saknas resurser för det operativa arbetet. På grund av detta handlar dataskyddsarbetet främst om att hantera akuta frågor, istället för att arbeta strategiskt. Som en del i att få mer styrning i arbetet har man under 2022 upprättat ett årshjul för dataskyddsarbetet.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Verksamheten behöver därför ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd.

För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser måste 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:

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen.

Verksamheten bör säkerställa att policyn uppfyller kraven på information och att informationen är lättillgänglig oavsett i vilken del av verksamheten den registrerades personuppgifter behandlas. Det är också viktigt att integritetspolicyn uppdateras vid behov.

Dataskyddsombudet avser framåt kontrollera den gjorda skattningen för att se hur väl informationen i integritetspolicyn uppfyller kraven enligt dataskyddsförordningen.

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:

Dataskyddsombudet har inte involverats i frågor kopplat till e-post och dokumenthantering, men bedömer utifrån dialog med bolaget att skattningen inte riktigt överensstämmer med verkligheten. Det pågår ett stort arbete inom bolaget där arkivarie och registrator besökt arbetsplatsträffar för att berätta om dokumenthantering och gallring utifrån att bolaget själva identifierat att det är en fråga man behöver jobba med. Ett arbete pågår även med att uppdatera dokumenthanteringsplanen och under tiden råder gallringsförbud.

Det är positivt att bolaget själva har identifierat att området kräver åtgärder, samt att det tagits initiativ till en stor informationsinsats kopplat till dokumenthantering och gallring. Bolagets rekommenderas fortsätta arbetet med dokumenthanteringsplanen, samt även fortsättningsvis genomföra informationsinsatser med syftet att stärka medarbetarnas kunskaper inom området.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

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. Det är inte enbart för nya former av behandlingar som verksamheten behöver göra konsekvensbedömningar utan det finns behov av att säkerställa att konsekvensbedömningar har genomförts för alla befintliga riskfyllda behandlingar.

Under året har bolaget haft inne en konsult som arbetat med konsekvensbedömningar för ett antal behandlingar. Inom ramen för det arbetet kontaktades dataskyddsombudet under våren ett antal gånger med enstaka frågor.

Dataskyddsombudet var inte deltagande när konsekvensbedömningarna genomfördes, men fick den 30 augusti ta del av en ”slutrapport” för konsultens arbete där *utföra konsekvensbedömningar* var en del av uppdraget. I rapporten anges att det ska ha genomförts sex konsekvensbedömningar under 2022.

I samband med att rapporten översändes bilades inga konsekvensbedömningar, och dataskyddsombudet gjorde därför antagandet att dessa ej ännu fastställts av bolaget (men att de överlämnats från konsulten till bolaget i samband med att uppdraget avslutades). I efterhand, i samband med genomgången av årsrapporten med bolagets interna dataskyddsorganisation, har det kunnat konstateras att det inom ramen för uppdraget missats att dataskyddsombudet ska få ta del av de framtagna underlagen innan de färdigställs för att kunna lämna rekommendationer. Bolaget angav även att man var av uppfattningen att dataskyddsombudet hade rådfrågats. Det är enligt GDPR ett krav att involvera dataskyddsombudet i arbetet med konsekvensbedömningar, och i det ingår såväl löpande rådgivning som att lämna slutliga rekommendationer på det framtagna underlaget. Sammantaget kan dataskyddsombudet i detta fall konstatera att det brustit i hanteringen kopplat till att inhämta och dokumentera dataskyddsombudets synpunkter och rekommendationer. För att hantera detta har bolaget skickat över samtliga konsekvensbedömningar till dataskyddsombudet för påseende och dataskyddsombudet kommer återkoppla synpunkter och rekommendationer under början av 2023.

Framåt rekommenderas verksamheten ta fram rutiner för att inhämta och dokumentera dataskyddsombudets synpunkter och rekommendationer både vid riskanalyser/tröskelanalyser och konsekvensbedömningar.

2.4.9 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. 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 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.

2.4.10 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:

Skattningen visar att det inom punkten föreligger risker som bedöms vara omfattande och/eller kräver omgående åtgärder. Bolaget behöver kartlägga de kanaler som används inom verksamheten samt säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster så som gratis appar och sociala medier.

Därtill noterar dataskyddsombudet att bolaget använder flera sociala medier. Dataskyddsombudet vill därför 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.

Dataskyddsombudet delar vidare inte bolagets bedömning vad gäller användningen av cookies, då cookiebannern inte uppfyller kraven för ett giltigt samtycke enligt GDPR. Inte heller informationen om cookies bedöms vara tillräcklig. Utifrån detta rekommenderas bolaget prioritera arbetet med att se över och vidta åtgärder för att säkerställa att användningen av cookies på webbsidor sker i enlighet med dataskyddsförordningen.

2.4.11 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:

Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar inom bolaget.

Utifrån svaren kan det dock utläsas att bolaget behöver ta fram en dokumenterad rutin för att kunna hantera ett tillbakadragande av samtycke från en registrerad, samt för att bedöma hur en invändning mot behandling 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 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