Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Business Region Göteborg AB

2022-12-29

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 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 instruktioner/metod för hur en bedömning av 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.
- Utbilda medarbetare om personuppgiftincidenter och hantering av dessa.
- Se över behovet av en rutin/plan för att kontinuerligt informera de anställda om personuppgiftsincidenter och den interna incidenthanteringen.

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 BRG:s dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande

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

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:

Resultatet visar att bolaget bedömer sig ha goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Av svaren framgår att dataskydd bedöms vara en naturlig och integrerad del av det dagliga arbetet för alla medarbetare.

Även om bolaget har en intern dataskyddsorganisation med goda kunskaper om dataskydd bedömer dataskyddsombudet, utifrån gjorda iakttagelser under året, att bolaget framåt behöver stärka kunskapen hos övriga medarbetare inom verksamheten. Bolaget rekommenderas därför se över vilka resurser och vilken kompetens man behöver inom verksamheten för att säkerställa dataskyddsperspektivet fullt ut. 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 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.

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 BRG 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 inga direkta risker är identifierade. Bolaget anger att det finns personuppgiftsbiträdesavtal tecknade med samtliga biträden, vilket är positivt. Enligt verksamhetens skattning finns mindre kvarstående risker gällande att genomföra efterlevnadskontroller av personuppgiftsbiträden samt att bedöma huruvida överenskommelser eller avtal behöver tecknas när en leverantör anlitas.

Utifrån skattningen rekommenderas bolaget att ta fram en rutin för regelbundna efterlevnadskontroller av anlitade personuppgiftsbiträder, samt en rutin/anvisning för att bedöma ansvarsförhållanden utifrån GDPR vid anlitande av en 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:

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 rutiner för att uppdatera personuppgiftsregister och använda registret i det löpande dataskyddsarbetet. Bolaget rekommenderas därför se över hur det framåt kan säkerställas att registret hålls uppdaterat vid förändringar i befintliga och/eller nya behandlingar.

Bolaget har på denna punkt skattat sitt arbete högt vad gäller omfattning (antal registrerade behandlingar) och innehåll (information om respektive behandling) i registret. 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.

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 har identifierat och värderas sina informationstillgångar utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet.

Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning görs i frågan.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Oaktat bolagets skattning bedömer dataskyddsombudet, utifrån gjorda iakttagelser under året, 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 att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

Framåt uppmuntras 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 hens 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 har 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 systemen 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:

Bolaget har på denna punkt skattat sitt arbete högt och svaren indikerar att bolaget har ett väl fungerande arbete med konsekvensbedömningar.

Även om bolagets skattning inte indikerar några omfattande risker är dataskyddsombudet bedömning att det inom punkten sannolikt föreligger risker som kräver åtgärder. Dataskyddsombudet har under året inte rådfrågats i någon konsekvensbedömning som bolaget har arbetat med, vilket skiljer sig från övriga verksamheter som dataskyddsombudet ansvarar för. Att genomföra konsekvensbedömningar är i många fall ett absolut krav och om detta inte genomförs riskerar man att missa att vidta åtgärder som behövs för att säkerställa de registrerades rättigheter. Vid en tillsyn kan det också innebära sanktionsavgifter från tillsynsmyndigheten. Arbetet med konsekvensbedömningar bör vara en del av den övergripande strategin för dataskyddsarbetet i verksamheten och den interna dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet av en konsekvensbedömning.

Vid genomgången av årsrapporten angavs att bolaget under 2022 inte genomfört någon konsekvensbedömning under året. Med anledning av detta, och kopplat till

de risker avsaknaden av konsekvensbedömningar medför, kommer dataskyddsombudet under 2023 kontrollera för vilka behandlingar som bolaget har genomfört konsekvensbedömningar, samt hur väl framtagna underlag uppfyller kraven enligt GDPR.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

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

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att inga direkta risker är identifierade.

Dataskyddsombudet har under året rådfrågats i enstaka frågor kopplat till nya IT-projekt och tredjelandsöverföringar. För att säkerställa att dataskyddsperspektivet finns med från start i arbetet med nya IT- och digitaliseringslösningar 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.

2.4.11 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. Kvarvarande risker inom detta område rör att följa upp medarbetares behörigheter och åtkomst till personuppgifter i IT-system, men sammantaget genererar verksamhetens svar ett resultat som innebär att inga direkta risker är identifierade.

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 enligt GDPR (eller best practice), samt då den information som tillhandahålls gällande användningen av cookies ej bedöms vara tillräcklig. 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:

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 fått några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig.

Då skattningen 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.

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 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