Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Business Region Göteborg AB

2023-12-20

Innehåll

1 Inledning

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. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Enligt lag ska dataskyddsombudet rapportera till högsta förvaltningsnivå och i Göteborgs Stad innebär det att dataskyddsombudet rapporterar direkt till nämnder och styrelser. Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är 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.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen 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 inom Göteborgs Stad.

Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter. Verksamheterna behöver följa dataskydds-lagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskydds-perspektivet förbises i digitaliseringsarbetet. Fokus behöver därför skiftas från att betrakta reglerna i dataskyddslagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt.

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts 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.

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.[1]

Risknivå	Beskrivning	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 bedriver ett systematiskt dataskyddsarbete.	

3.2 Resultat från kontrollen 2023

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. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

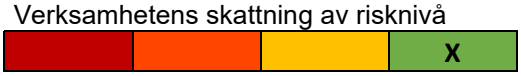
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker av betydelse inom kontrollpunkten.

Den interna dataskyddsorganisationen utgör grunden för att bolaget ska kunna bedriva ett systematiskt dataskyddsarbete på ett effektivt och ändamålsenligt sätt. En intern dataskyddsorganisation utgör även en förutsättning för efterlevnaden av dataskyddslagstiftningen. En dataskyddsorganisation som består av en eller ett mycket litet antal personer medför sårbarhet. Det kan resultera i att dataskyddsarbetet inom bolaget blir personberoende. Det finns även risk för att den interna dataskyddsorganisationen inte hinner med alla de uppgifter som behöver göras. Dataskyddsombudet uppmärksammar även att bolagets egen skattning inom kontrollpunkten är lägre än förgående år även om bolaget ligger kvar på samma risknivå. Exempelvis noterar dataskyddsombudet att skattningen är lägre jämfört med år 2022 på frågan om den interna dataskyddsorganisationen för dataskyddsarbetet har tillräckligt med resurser för att kunna bedriva ett systematiskt dataskyddsarbete. Under genomgången av årsrapporten uppger verksamheten dock att det snarare är tvärtom, och upplever att mer resurser har tillförts dataskyddsarbetet under året. Eftersom dataskyddsombudet får motstridiga svar rekommenderas bolaget att utreda hur det förhåller sig inom bolaget.

Dataskyddsombudet bedömer vidare att det finns behov av att se över hur bolaget arbetar tillsammans med dataskyddsombudet. Vid genomgången av årsrapporten uttrycker bolaget önskemål om ett ökat stöd, samtidigt som bolaget under året regelbundet tackat nej till de förfrågningarna om stöd/hjälp som dataskyddsombudet erbjudit. De möten som ändå har varit under året har dataskyddsombudet varit sammankallande till. Utifrån det önskemål om ökat stöd som bolaget lyfter ser dataskyddsombudet positivt på kommande initiativ från bolaget i frågan.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse

föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten.

Under året har dataskyddsombudet kontaktats och involverats i två inträffade personuppgiftsincidenter, vilket dataskyddsombudet ser som mycket positivt. Utifrån iakttagelser i samband med detta vill dataskyddsombudet lyfta bolagets goda arbete med att snabbt vidta åtgärder och sammankalla medarbetare för att hantera incidenten.

I årsrapporten 2022 identifierade dataskyddsombudet att det fanns risker kopplat till medarbetares förutsättningar för att kunna identifiera när en personuppgiftsincident inträffar. Även om bolaget har fungerande arbetssätt för att omhänderta de incidenter som den interna dataskyddsorganisationen får kännedom om, är dataskyddsombudets bedömning att antalet incidenter fortfarande ligger på en låg nivå. Detta med hänsyn till att tröskeln för när en personuppgiftsincident har skett är låg och att personuppgiftincidenter förekommer även i organisationer som har mycket väl utvecklade rutiner för att förhindra att personuppgiftsincidenter sker. Dataskyddsombudet rekommenderar därför att bolaget framåt följer upp och utvärderar om bolagets vidtagna åtgärder och insatser får önskad effekt. Bolaget bör exempelvis utvärdera om antalet inrapporterade misstänkta incidenter ökar samt om rapporteringen sker till rätt utpekade personer internt.

Dataskyddsombudet genomförde 2022 en fördjupad kontroll av incident-hanteringen och lämnade utifrån denna ett antal rekommendationer till bolaget. Uppföljningen av dessa rekommendationer lämnas under avsnitt 3.3.1.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

			X

Dataskyddsombudets bedömning

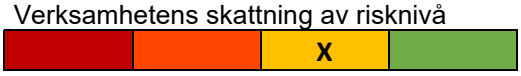
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har endast involverats i någon enstaka fråga kopplat till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Bolaget uppger i skattningen att det finns tecknade avtal, inklusive lämnade instruktioner, med samtliga biträden. I samband med genomgången av årsrapporten uppger dock bolaget att avtal saknas för stadens interna tjänsteleverantörer. Dataskyddsombudet har noterat att det är flera förvaltningar och bolag inom Göteborgs stad där detta förekommer. Bolaget rekommenderas att föra dialog med de interna tjänsteleverantörerna och kartlägga ansvarsförhållandena för att se över för vilka personuppgiftsbehandlingar som kräver att avtal och instruktioner tecknas.

Dataskyddsombudet noterar även att verksamheten har, jämfört med år 2022, skattat sig lägre på frågan om verksamheten har dokumenterade arbetssätt och kompetens för att bedöma hela kedjan av underbiträden vid anlitande av ett nytt personuppgiftsbiträde. I samband med genomgången av årsrapporten uppger bolaget att det inte har skett några förändringar inom bolaget som har bidragit till skillnaden i svaret. Verksamheten uppger samtidigt att det vid skattningen inte har gjorts en jämförelse med föregående års svar. Dataskyddsombudet vill med anledning av detta poängtera att även en ökad medvetenhet kan bidra till att skattningarna ändras över tid, då det medför att brister/risker kan identifieras. Bolaget rekommenderas därför se över hur bolagets svar förhåller sig till de faktiska förutsättningarna, med syftet att kunna utröna om, och i så fall vilka, åtgärder som kan behöva vidtas.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

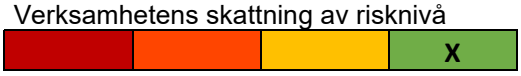
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat bolagets behandlingsregister särskilt.

Utifrån verksamhetens skattning kan dataskyddsombudet utläsa att ca 75 % av verksamhetens personuppgiftsbehandlingar finns dokumenterade i behandlingsregistret. Bolaget rekommenderas att komplettera behandlingsregistret med de personuppgiftsbehandlingar som saknas. Vidare observerar dataskyddsombudet, utifrån skattningen, att det finns ett behov av att upprätta rutiner för att tillförsäkra att behandlingsregistret regelbundet uppdateras och att det finns särskilt utpekade ansvariga för uppgiften. Bolaget rekommenderas därför att ta fram rutiner för att tillförsäkra att registret hålls uppdaterat och att det finns en tydlig ansvarsfördelning för uppgiften.

Förutom att behandlingsregistret är ett lagkrav, kan behandlingsregistret också vara ett värdefullt verktyg i samband med det löpande dataskyddsarbetet, exempelvis vid bolagets hantering av informationsplikten, vid konsekvensbedömningsarbetet och vid hantering av registrerades begäran om tillgång då registrerade utöver att få tillgång till sina uppgifter även ska få den information som framgår av artikel 15 i GDPR.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



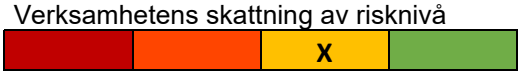
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

Utifrån dels det låga antalet identifierade personuppgiftsincidenter, dels vad som framgår under kontrollpunkt 9 relaterat till konsekvensbedömningar, bedömer dataskyddsombudet att det inom verksamheten sannolikt föreligger ett utbildningsbehov kopplat till dessa delar. Under året har dataskyddsombudet fått information om att utbildningsinsatser inom personuppgiftsincidenter och informationssäkerhet har genomförts. Dataskyddsombudet ser det som positivt och rekommenderar bolaget att framåt fortsätta med kontinuerliga informations- och utbildningsinsatser för att säkerställa att kunskapsnivån bibehålls och även höjs.

Dataskyddsombudet vill även uppmärksamma att olika medarbetare kan ha olika behov av utbildnings- och informationsinsatser utifrån sin roll och sina arbetsuppgifter. För att säkerställa att resurser sätts in där det främst behövs rekommenderas bolaget kartlägga vilken nivå av dataskyddskunskaper som olika befattningar behöver ha och säkerställa att medarbetare löpande utbildas därefter. På så sätt ges medarbetarna rätt förutsättningar att integrera dataskyddsperspektivet i sitt dagliga arbete och att hantera personuppgifter korrekt utifrån sin roll inom bolaget.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Under året har verksamheten informerat dataskyddsombudet om att det pågår ett arbete med att uppdatera verksamhetens externa integritetspolicy. I samband med genomgången av årsrapporten uppgav bolaget att arbetet är avslutat och klart. Det är positivt att verksamheten har arbetat med kontrollpunkten under året, och dataskyddsombudet avser följa upp arbetet under 2024.

Dataskyddsombudet vill även lyfta att kontrollpunkten i år har ändrats till att avse informationsplikten. Informationsplikten är långtgående och omfattar mer än den externa integritetspolicyn. För att informationsplikten ska anses vara uppfylld finns det krav på såväl när informationen ska lämnas, vilken information som lämnas och hur den lämnas. Personuppgiftsansvariga ska även informera om alla personuppgiftsbehandlingar som genomförs. Bolaget rekommenderas därför att säkerställa att även ytterligare information tillhandahålls registrerade i samband med behandlingar utöver det som lämnas i den externa integritetspolicyn.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Vid jämförelse av verksamhetens skattning inom kontrollpunkten noterar dataskyddsombudet att verksamheten skattar sig lägre på flera frågor i år jämfört med år 2022. I samband med genomgången av årsrapporten uppger bolaget att det inte har skett några förändringar inom bolaget som har bidragit till skillnaden i svaren. Bolaget uppger samtidigt att det vid skattningen inte har gjorts en jämförelse med föregående års svar. Dataskyddsombudet vill med anledning av detta poängtera att även en ökad medvetenhet kan bidra till att skattningarna ändras över tid, då det medför att brister/risker kan identifieras. Bolaget rekommenderas därför se över hur bolagets svar förhåller sig till de faktiska förutsättningarna, med syftet att kunna utröna om, och i så fall vilka, åtgärder som kan behöva vidtas.

Av skattningen kan vidare utläsas att verksamheten behöver se över hur registrerade, vid kontakt med verksamheten, får information om hur deras personuppgifter hanteras. Bolaget rekommenderas att vidta åtgärder för att säkerställa att verksamheten informerar de registrerade direkt i samband med upprättande av kontakt om hur deras personuppgifter hanteras.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som är omfattande och som kräver åtgärder.

Dataskyddsombudet har under året haft en dialog med verksamheten om kontrollpunkten. I samband med avstämning har verksamheten meddelat att det inte finns några framtagna och fastställda konsekvensbedömningar inom bolaget. Verksamheten uppger att det beror på att bolaget inte har några personuppgifts-behandlingar som kräver konsekvensbedömningar. Dataskyddsombudet delar inte bolagets bedömning i frågan. Bolaget har ett flertal anställda och bör därmed rimligen ha behandlingar kopplat till HR-området som kan kräva konsekvensbedömningar, exempelvis kopplat till uppföljning av arbetsmiljö samt utredning av oegentligheter. Även behandlingar kopplat till bolagets hemsida och användningen av analysverktyg, samt bolagets uppdrag att lämna rådgivning och stöd till företag kan kräva konsekvensbedömningar beroende på vilka personuppgifter som hanteras.

Utifrån ovan bedömer dataskyddsombudet att bolaget behöver gå igenom sina personuppgiftsbehandlingar och kontrollera personuppgiftsbehandlingarna utifrån höga risker. I arbetet med att riskbedöma behandlingarna rekommenderas bolaget inhämta dataskyddsombudets synpunkter.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

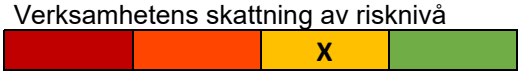
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året endast involverats i någon enstaka

fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Dataskyddsombudet vill dock framhålla att det är viktigt att dataskyddsperspektivet beaktas vid såväl IT-projekt som upphandlingar. Om dataskyddsperspektivet inte beaktas vid upphandlingar riskerar bolaget att upphandla en tjänst eller ett system som i förlängningen inte är möjlig att använda på ett ändamålsenligt sätt.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver åtgärder.

De risker som identifierats gäller främst användningen av sociala medier och bolagets cookiehantering, men bolagets egen skattning visar även att det fortfarande finns behov av att kartlägga vilka kommunikationskanaler som verksamheten använder för att få en tydlig överblick över bolagets kommunikationskanaler.

Dataskyddsombudet och bolaget har under året haft en dialog om användningen av sociala medier. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget har rekommenderats att bland annat kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna. Under året har verksamheten uppgett att en kartläggning över behandlingarna med koppling till sociala medier pågår, vilket dataskyddsombudet ser som positivt. I samband med genomgången av årsrapporten uppger bolaget att arbetet är färdigställt och att bolaget nu arbetar med en konsekvensbedömning för de identifierade behandlingarna. Även om dataskyddsombudet har fått underlag till sig så har dataskyddsombudet ännu inte blivit involverad i arbetet.

I årsrapporten för 2022 lyfte dataskyddsombudet att bolagets dåvarande cookiehantering inte levde upp till gällande lagkrav. Vid genomgång av bolagets användning av cookies har dataskyddsombudet noterat att bolaget har vidtagit åtgärder för att inhämta ett aktivt samtycke för cookies från besökarna. Dataskyddsombudet ser det som mycket positivt att bolaget har arbetat utifrån dataskyddsombudets rekommendationer. Samtidigt gör dataskyddsombudet bedömningen att bolaget fortsatt behöver arbeta med sin cookiehantering, bland

annat kopplat till informationen som lämnas till användare och vilka cookies som kan bedömas vara nödvändiga. Bolaget rekommenderas därför fortsätta att arbeta med frågan och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl GDPR som LEK (lagen (2022:482) om elektronisk kommunikation).

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån. Bolaget rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Hantering av personuppgiftsincidenter 2021

Verksamheten gavs 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 Integritetsskyddsmyndigheten ska göras.
- Utbilda medarbetare om personuppgiftsincidenter och hantering av dessa.
- Se över behovet av en rutin/plan för att kontinuerligt informera de anställda om personuppgiftsincidenter och den interna incidenthanteringen.

Kommentarer och rekommendationer:

Uppföljningen visar att bolaget under året har genomfört informationsinsatser kring personuppgiftsincidenter samt att ett större antal anställda har deltagit i stadens incidentutbildning. Även ytterligare utbildningsinsatser är planerade. Vidare har

bolaget kompletterat rutinen avseende personuppgiftsincidenter med hur bedömning av risker för de registrerades kan göras och vem som beslutar gällande om en personuppgiftsincident ska anmälas till tillsynsmyndighet. Det är positivt att bolaget har arbetat med rekommendationerna under året.

I sammanhanget, och utifrån den dialog som varit med bolaget i frågan, vill dataskyddsombudet även påminna om att personuppgifternas känslighet inte har betydelse för huruvida en personuppgiftincident har inträffat eller inte, även om det har viss betydelse vid bedömningen av om anmälningsskyldighet och informationsskyldighet föreligger. Dataskyddsombudets rekommendationer från den fördjupade kontrollen 2022 kvarstår därför avseende att komplettera nuvarande rutin med exempel på incidenter som innefattar personuppgifter som inte är av särskilt skyddsvärd eller känslig karaktär, samt inkludera fler konkreta beskrivningar av vad en personuppgiftsincident är för att anställda ska få en bredare bild av vad som utgör en incident. Det vore fördelaktigt om rutinen kompletterades med incidenter som sannolikt kan inträffa inom verksamheten, till exempel att ett e-postmeddelande innehållandes personuppgifter (oavsett typ) skickas till fel mottagare eller att en person får tillgång till fel mapp/lagringsyta med mera.

Då bolaget till stor del vidtagit åtgärder utifrån lämnade rekommendationer kommer fortsatt uppföljning att ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

4 Rekommenderade fokusområden 2024

Utifrån höga föreliggande risker för de registrerades fri- och rättigheter har dataskyddsombudet identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa listas i punktform enligt nedan. Detta är områden som dataskyddsombudet särskilt kommer att följa upp framåt. Uppföljningen kommer ske löpande under det kommande året, i dialog med verksamheten.

Utifrån identifierade risker är dataskyddsombudets sammanfattande rekommendationer till bolaget att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Se över och komplettera behandlingsregistret med de personuppgiftsbehandlingar som saknas, och kontrollera för respektive behandling att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

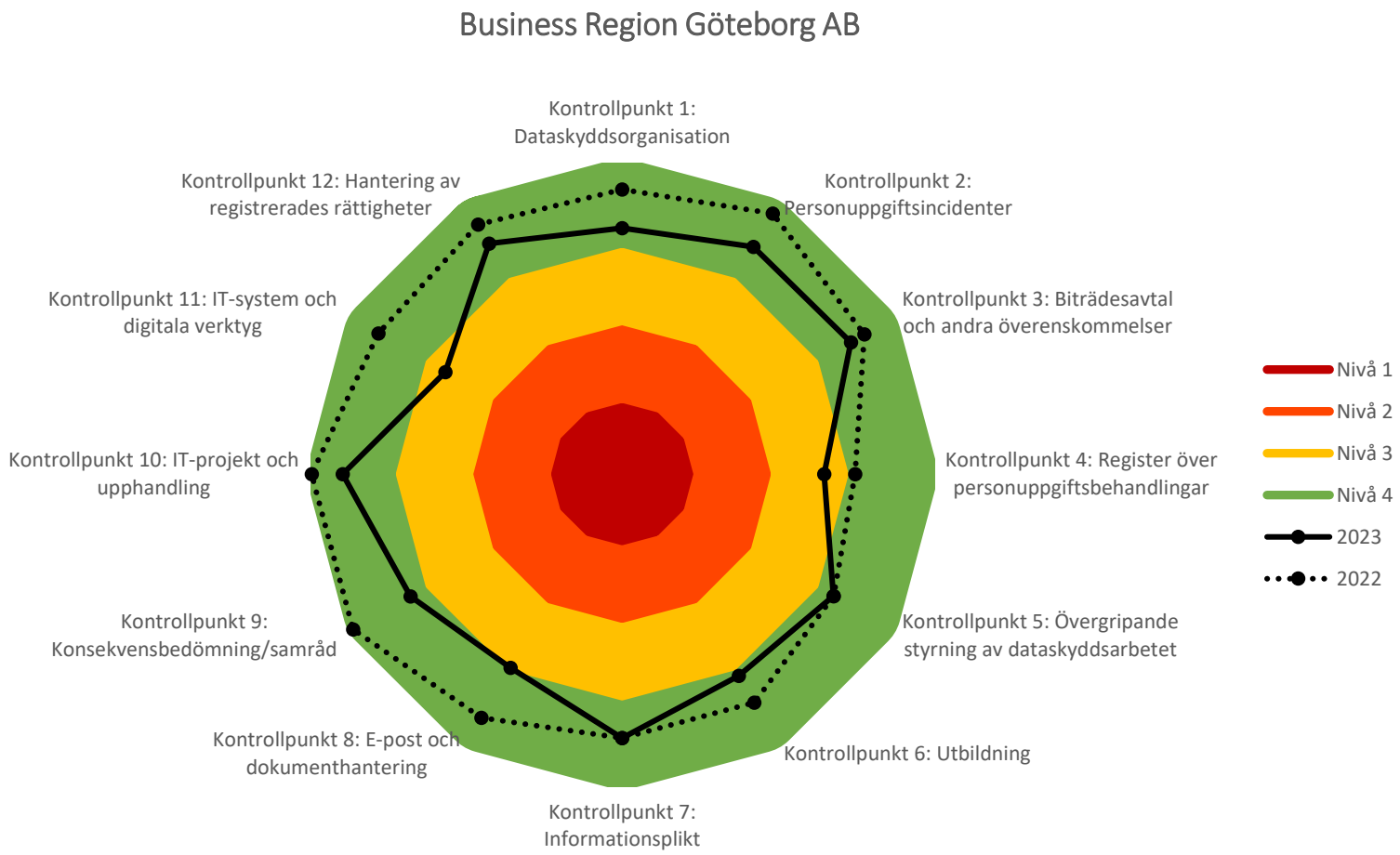
Bedöm befintliga personuppgiftsbehandlingar utifrån höga risker för att få en överblick över vilka behandlingar som kräver att en konsekvensbedömning genomförs. Ta fram en planering och prioritering för genomförandet.

5 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.



Göteborgs Stad

Business Region Göteborg AB

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. 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 personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ny utformning av kontrollarbetet

För att ytterligare stärka kvaliteten i verksamheternas dataskyddsarbete kommer dataskyddsombudets kontrollarbete att framgent löpa över tvåårsperioder. Tidigare har kontrollarbetet planerats årsvis, vilket ändras från och med år 2023. För att också underlätta verksamheternas egen planering kommer en ny kontrollplan att skickas ut varje år, som omfattar både innevarande och nästkommande kalenderår.

Kontrollarbetet kommer även fortsättningsvis bestå av tre delar, men frekvensen för den fasta respektive fördjupade kontrollen ändras. Framåt kommer dessa kontroller att ske vartannat år och under 2023 kommer en kontroll av de fasta kontrollpunkterna att genomföras. Genom att alternera den fasta respektive fördjupade kontrollen mellan åren får verksamheterna mer tid till att omhänderta resultaten från kontrollerna, vilket bedöms kunna bidra till ökad kvalitet på vidtagna åtgärder såväl som lagefterlevnad. Detta ligger också i linje med önskemål från flera verksamheter som har signalerat att tätt liggande kontroller gör det svårt att hinna med att arbeta med de lämnade rekommendationerna.

Den nya utformningen innebär även att tid frigörs för dataskyddsombudet, vilken kommer att läggas på att ytterligare stärka arbetet med informations- och utbildningsinsatser för stadens förvaltningar och bolag.

2 Kontrollarbetet 2023–2024

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av dataskyddslagstiftningen görs i Göteborgs stad genom ett antal kontroller. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2023 och 2024. Enligt GDPR ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsombudets bedömning avseende risker kopplat till personuppgiftsbehandlingar i verksamheten.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

Del	Beskrivning	Frekvens
Fasta kontrollpunkter	En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter.	Vartannat år fr.o.m. 2023
Fördjupad kontroll	En fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.	Vartannat år fr.o.m. 2024
Uppföljning	Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.	Årligen

2.2 Tidplan för kontrollarbetet 2023–2024

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2023–2024 för stadens förvaltningar och bolag.

2023	Aktivitet
Januari - april	Årsrapport 2022 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2023–2024 lämnas till nämnd/bolag.
September	Utskick av enkät för fasta kontrollpunkter.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

2024	Aktivitet
Januari - april	Årsrapport 2023 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2024–2025 lämnas till nämnd/bolag.
Augusti - november	Fördjupad kontroll.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

3 Kontroller

3.1 Fasta kontrollpunkter

De fasta kontrollpunkterna utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

De fasta kontrollpunkterna kontrolleras genom en enkät som framöver kommer att vara återkommande vartannat år. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av

påståenden och/eller skattningsfrågor. Det är verksamheten som ansvarar för att enkäten fylls i. För att uppskattningarna ska bli så korrekta som möjligt kan det krävas att olika personer från olika delar i verksamheten deltar i arbetet med att fylla i enkäten. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som även åskådliggör de förändringar som vidtas över tid.

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

Fasta kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Register över personuppgiftsbehandlingar
5. Övergripande styrning av dataskyddsarbetet
6. Utbildning
7. Informationsplikt
8. E-post och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.2 Fördjupad kontroll

Den fördjupade kontrollen ska utgå från verksamhetens specifika risker och kommer framöver att genomföras vartannat år. Dataskyddsombudet kommer att fastställa fokusområde för den fördjupade kontrollen i dialog med verksamheten.

Information om fokusområde för 2024 kommer att tillhandahållas nämnd/bolag i kontrollplanen för 2024–2025.

3.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer och utvecklat sitt dataskyddsarbete inom varje kontrollpunkt.

4 Rapportering

4.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig presenteras årsrapporten för nämnd/styrelse vid sammanträde/möte.

4.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

5 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till verksamhetens huvudansvariga kontaktperson inom dataskyddsenheten.

Frågor kan också alltid ställas till dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

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.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

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.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

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 dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

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.

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 dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.