Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Got Event AB

2023-12-19

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 inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga.

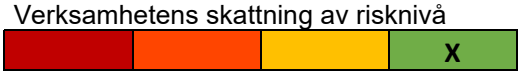
Den interna dataskyddsorganisationen utgör grunden för att bolaget ska kunna bedriva ett systematiskt dataskyddsarbete på ett effektivt och ändamålsenligt sätt. En intern dataskyddsorganisation utgör även en förutsättning för efterlevnaden av dataskyddslagstiftningen. En dataskyddsorganisation som består av en eller ett mycket litet antal personer kan medföra 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. För att minska sårbarheten för bolaget är dataskyddsombudets fortsatta bedömning att den interna dataskyddsorganisationen behöver ges ett ökat stöd och mer resurser för att kunna få rätt förutsättningar att utföra arbetet.

Dataskyddsombudet uppmärksammar även att bolagets skattning inom kontrollpunkten är lägre jämfört med förgående år, även om bolaget ligger kvar på samma risknivå. I samband med genomgången av årsrapporten uppgav verksamheten att det beror på att en tjänst för närvarande är vakant.

Bolaget rekommenderas även att framåt säkerställa att dataskyddsombudet på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.

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 inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som kräver åtgärder.

Dataskyddsombudet vill, likt förgående år, lyfta att ett bolag som hanterar den mängd personuppgifter som Got Event gör rimligtvis borde ha ett flertal inträffade incidenter varje år. Under året har dataskyddsombudet endast fått vetskap om och

involverats i en incident. I samband med genomgången av årsrapporten meddelade verksamheten även att några mindre allvarliga incidenter har inträffat under året.

Både vid avstämning med bolaget och i uppföljningen av den fördjupade kontrollen för år 2022 har dataskyddsombudet fått information om att bolaget arbetar med att uppdatera sin interna rutin för personuppgiftsincidenter, vilket dataskyddsombudet ser som positivt. Bolaget rekommenderas att färdigställa rutinen samt kommunicera rutinen med samtliga medarbetare. Bolaget har även i uppföljningen av den fördjupade kontrollen avseende personuppgiftsincidenter angett att det planeras en utbildning för samtliga anställda inom informationssäkerhet och dataskyddsfrågor där personuppgiftsincidenter kommer vara en del. Även detta ser dataskyddsombudet som positivt.

Dataskyddsombudet vill i sammanhanget framhålla att det är viktigt att följa upp och säkerställa att bolagets vidtagna åtgärder och insatser får önskad effekt framåt. Efter genomförd utbildning och när rutinen är färdigställd rekommenderas bolaget utvärdera om antalet inrapporterade incidenter ökar samt om rapporteringen sker till rätt utpekade personer internt.

Eftersom behovet av utbildning kan se olika ut för olika medarbetare är det även viktigt att bolaget framåt säkerställer att medarbetare får den utbildning som är lämplig utifrån arbetsuppgifter och befattning. Dataskyddsombudet noterar att det ligger på respektive chef och systemägare att fatta beslut kring personuppgiftsincidenter. Det är därmed viktigt att säkerställa att dessa funktioner får tillräcklig kunskap inom dataskyddslagstiftningen för att kunna dels genomföra riskbedömningarna, dels fatta korrekta beslut avseende när en personuppgiftsincident behöver anmälas och när de registrerade behöver informeras.

Personuppgiftsincidenter har varit föremål för en fördjupad kontroll under år 2022, vilket har följts upp under hösten år 2023. Bolaget svar framgår under avsnitt 3.3.1.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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 verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Utifrån verksamhetens skattning observerar dataskyddsombudet att det kvarstår risker kopplat till efterlevnadskontroller av anlitade personuppgiftsbiträden och till bedömning av hela kedjan av underbiträden. Dataskyddsombudets

rekommendationer från förgående år om att ta fram rutin/anvisning för utförandet av regelbundna efterlevnadskontroller av anlitade personuppgiftsbiträden samt en rutin för att kontrollera hela kedjan av underbiträden vid anlitande av ny leverantör kvarstår.

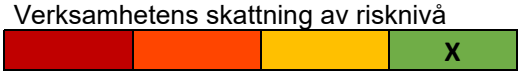
Vidare anger bolaget att personuppgiftsbiträdesavtal har tecknats med ca 75 % av de biträden som anlitats av bolaget. Det saknas således avtal med ca 25 % av anlitade biträden. Verksamheten uppger i dialog med dataskyddsombudet att det rör biträdesavtal med stadens interna tjänsteleverantörer. Dataskyddsombudet har noterat att det är flera förvaltningar och bolag inom Göteborgs stad där detta förekommer. Bolaget rekommenderas att föra dialog med stadens interna tjänsteleverantörer och kartlägga ansvarsförhållandena för att se över för vilka personuppgiftsbehandlingar som kräver att avtal, inklusive instruktioner, tecknas.

Dataskyddsombudet noterar att bolagets skattning är högre än förgående år på frågan om verksamheten har dokumenterade arbetssätt för att bedöma om det finns ett gemensamt personuppgiftansvar. Dataskyddsombudet ser det som positivt att bolaget under året har uppmärksammat och identifierat situationer där bolaget har ett gemensamt personuppgiftsansvar med en annan/flera andra aktör/er och härvid tecknat avtal för att reglera det gemensamma personuppgiftsansvaret. Det är även positivt att bolaget har haft en dialog med dataskyddsombudet i frågan och bolaget uppmuntras även framledes att involvera dataskyddsombudet då tveksamheter uppstår vid bedömningen av ansvarsförhållanden.

I sammanhanget vill dataskyddsombudet lyfta att även om bolaget kan identifiera när och vilken typ av avtal som ska tecknas med olika parter behöver bolaget också kunna säkerställa innehållet i avtalen. Innehållet i den här typen av avtal kan vara svårhanterligt och kräver oftast att flera olika kompetenser deltar i utformningen av avtalsinnehållet. Dataskyddsombudet rekommenderar därför att bolaget säkerställer att medarbetarna som arbetar med frågorna får rätt resurser och stöd till sitt förfogande.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 och som kräver åtgärder.

Enligt verksamhetens egen skattning är samtliga behandlingar dokumenterade i behandlingsregistret. Vid ett stickprov av verksamhetens behandlingsregister gör

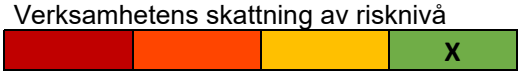
dataskyddsombudet bedömningen att verksamheten behöver se över om behandlingarna är avgränsade på ett ändamålsenligt sätt.

Bolaget uppger att det är ca 75 % av behandlingarna som innehåller all den information som krävs. Bolaget rekommenderas därför att komplettera behandlingsregistret med den information som saknas för att uppfylla artikel 30 i GDPR. Under året har dataskyddsombudet utfört en informationsinsats om behandlingsregister. Dataskyddsombudet har tillhandahållit såväl skriftligt som muntligt material och en ny mall för behandlingsregistret. Bolaget kan med fördel använda sig av materialet som stöd i arbetet framåt.

Förutom att det är ett lagkrav att fullständig information finns med, kan behandlingsregistret integreras i det löpande dataskyddsarbetet och på så sätt underlätta och effektivisera arbetet med dataskyddsfrågor.

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 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.

Dataskyddsombudet noterar dock att bolagets skattning ligger kvar på samma nivå som förgående år avseende bolagets interna kontroller för att säkerställa följsamheten gentemot GDPR. Utifrån skattningarna på övriga kontrollpunkter kan dataskyddsombudet utläsa att bolaget har flera rutiner på plats. För att tillförsäkra sig om att de utformade arbetssätten är ändamålsenliga och följs av medarbetare rekommenderas bolaget att framledes genomföra interna kontroller för att följa upp och kontrollera så att de rutiner och anvisningar som finns får genomslag i praktiken.

3.2.6 Kontrollpunkt 6: Utbildning

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 övergripande bedömning kan göras i frågan.

Utifrån gjorda iakttagelser kopplat till bolagets hantering av personuppgiftsincidenter ser dock dataskyddsombudet att det inom kontrollpunkten kan föreligga risker. I årsrapporten för 2022 lyfte dataskyddsombudet att det utifrån det låga antalet rapporterade personuppgiftsincidenter skulle kunna föreligga ett behov av att öka medarbetares kunskapsnivå inom detta område. Även om det planeras en utbildning för samtliga anställda inom informationssäkerhet och dataskyddsfrågor är det också viktigt att säkerställa att utbildningen genomförs.

Dataskyddsombudet vill även lyfta 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 bör 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 dataskyddsperspektiv 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 delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker av betydelse inom kontrollpunkten och som kräver åtgärder.

Vid genomgång av bolagets externa integritetspolicy på hemsidan är dataskyddsombudets bedömning att den inte uppfyller kraven på information enligt artikel 13 och 14 i GDPR. Dataskyddsombudet har i övrigt inte fått indikationer på att annan information som lämnas till registrerade är av den omfattning att bolaget uppfyller informationsplikten. Tvärtom har dataskyddsombudet noterat att bolagets kamerabevakningsskyltar inte innehåller den information som ska framgå av det så kallade ”första lagrets” information. Dataskyddsombudet har informerats om att verksamheten är medveten om bristerna med kamerabevakningsskyltarna. Skyltarna har dock inte prioriterats under året mot bakgrund av att resurserna har använts till att arbeta utifrån det rådande säkerhetsläget.

Det är positivt att bolaget under året har initierat dialog med dataskyddsombudet avseende arbetet med informationsplikten. I dialogen har dataskyddsombudet lämnat förslag på hur bolaget, med stöd av dataskyddsombudet, framåt kan arbeta för att förbättra informationsplikten.

Även om bolaget har en ambition att se över hanteringen av informationsplikten rekommenderas bolaget att upprätta en konkret handlingsplan och planering för hur arbetet ska utföras framåt. Under året har dataskyddsombudet utfört en informationsinsats om informationsplikten och tillhandahållit såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget kan använda sig av underlaget som stöd i arbetet med informationsplikten.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

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.

Utifrån bolagets egna svar har endast 25 % av personuppgiftsbehandlingar informationsklassificerats utifrån Göteborgs Stads riktlinjer för informationssäkerhet. Bolaget rekommenderas att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

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

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

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 verksamhetens bedömning om att det finns risker som behöver åtgärdas.

Enligt bolaget finns det framtagna och fastställda konsekvensbedömningar för ca 50 % av verksamhetens personuppgiftsbehandlingar som innebär hög risk. Inför årsrapporten 2022 angav bolaget att andelen var 25 %. Svaret indikerar att konsekvensbedömningar har genomförts under året. I samband med genomgången av årsrapporten förtydligar dock bolaget att inga nya konsekvensbedömningar har färdigställts under året även om det finns pågående konsekvensbedömningar.

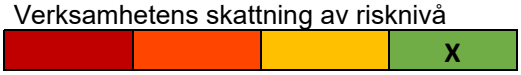
Framtagna och fastställda konsekvensbedömningar är därmed på samma nivå som år 2022.

Bolaget anger i skattningen att endast 25 % av personuppgiftsbehandlingarna har kontrollerats utifrån höga risker. Under genomgången av årsrapporten uppger bolaget dock att samtliga personuppgiftsbehandlingar har kontrollerats utifrån höga risker, även om det inte har gjorts i form av tröskelanalyser. Bolaget uppger även att det finns en dokumenterad planering för att genomföra konsekvensbedömningar för samtliga personuppgiftsbehandlingar som kräver en sådan, vilket dataskyddsombudet ser som positivt. Bolaget rekommenderas att framåt säkerställa att konsekvensbedömningarna faktiskt genomförs.

Utifrån iakttagelser under året har dataskyddsombudet noterat att bolaget har kamerabevakning på ett flertal platser. Med beaktade av att personuppgiftsbehandlingar som innefattar kamerabevakning kan leda till höga risker för registrerades fri- och rättigheter vill dataskyddsombudet särskilt framhålla att arbetet med kamerabevakningen bör prioriteras. Bolaget rekommenderas att säkerställa att bolaget har utfört och dokumenterat riskbedömningar. Bolaget behöver också säkerställa att det finns framtagna och fastställda konsekvensbedömningar för respektive behandling i de fall sådana krävs. Att bolaget har erhållit tillstånd för kamerabevakning innebär inte i sig att konsekvensbedömningar inte behöver genomföras. Dataskyddsombudet rekommenderar att arbetet med kamerabevakning i sin helhet prioriteras under år 2024.

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 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.

Bolaget rekommenderas att framåt involvera dataskyddsombudet vid uppstart av nya IT-projekt och/eller upphandlingar.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

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.

I årsrapporten 2022 rekommenderades bolaget att kartlägga sina behandlingar med koppling till användning av sociala medier och genomföra en konsekvensbedömning för att kontrollera att behandlingarna är förenliga med GDPR. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken, varför rekommendationen från årsrapporten 2022 om att kartlägga behandlingarna kvarstår. Bolaget rekommenderas bland annat att utreda 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. Vidare rekommenderas bolaget att utföra och dokumentera noggranna riskanalyser samt se över för vilka behandlingar kopplat till användningen av sociala medier som kräver en konsekvensbedömning. Verksamheten har i dialog med dataskyddsombudet uppgett att det sker ett samarbete på koncernnivå i frågan. Dataskyddsombudet ser det som positivt och rekommenderar att bolaget fortsätter att arbeta med frågan framöver.

Vid genomgång av bolagets användning av cookies har dataskyddsombudet noterat att bolaget har vidtagit åtgärder för att inhämta ett aktivt samtycke för cookies, vilket dataskyddsombudet ser som positivt. Samtidigt gör dataskyddsombudet bedömningen att bolaget fortsatt behöver arbeta med sin cookiehantering. För att det ska vara ett giltigt samtycke ska det bland annat vara lika lätt att återkalla som att lämna samtycket. Det råder osäkerhet om hänvisning till inställningar i webbläsaren kan anses uppfylla kravet. Bolaget rekommenderas därför att säkerställa att det finns funktioner för att återkalla ett samtycke. Därtill rekommenderas bolaget att se över informationen i övrigt för att säkerställa att användarna får tydlig information om att användaren när som helst kan återkalla sitt samtycke, vem informationen delas med och, om det är möjligt, vilka tredjeländer personuppgifter överförs till.

I övrigt har dataskyddsombudet ingen tydlig inblick i bolagets arbete med IT-system och behörighetsstyrning, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort i dessa delar.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

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.

Även om dataskyddsombudet har fått kännedom om två förfrågningar från registrerade under året har dataskyddsombudet inte involverats i någon fråga kopplad till kontrollpunkten. Dataskyddsombudet 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 information i vilka fall dataskyddsombudet ska involveras.
- Komplettera rutinen med instruktioner/metoder för hur en bedömning av risken för de registrerades fri- och rättigheter kan göras.
- Se över medarbetares kunskap gällande vad en personuppgiftsincident är.
- Utbilda all personal om personuppgiftsincidenter och hantering av dessa.

Kommentarer och rekommendationer:

Bolaget har vid uppföljningen uppgett att rutinen för personuppgiftsincidenter har uppdaterats för att följa stadens modell. Rutinen har kompletterats med information om att dataskyddsombudet ska involveras vid behov samt vad medarbetare ska tänka på när en riskbedömning görs. Utifrån dialog med verksamheten har dock dataskyddsombudet fått uppfattningen att rutinen ännu inte är helt färdigställd. Bolaget uppger även att en utbildning planeras för samtliga anställda. Utbildningen kombinerar informationssäkerhet och GDPR-frågor, och i denna kommer personuppgiftsincidenter att vara en del. Planen är att utbildningen kommer att ges till chefer under första kvartalet år 2024. Chefer ska därefter ta vidare informationen till alla medarbetare på arbetsplatsträffar.

Uppföljningen visar att arbete pågår med att vidta åtgärder utifrån dataskyddsombudets rekommendationer. Fortsatt uppföljning kommer att ske igen under år 2024. Vidare kommentarer och rekommendationer framgår av punkten 3.2.2.

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

Gör en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och för respektive behandling kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls.

Uppdatera kamerabevakningsskyltarna och se över vilken information som lämnas till registrerade med koppling till kamerabevakningen.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

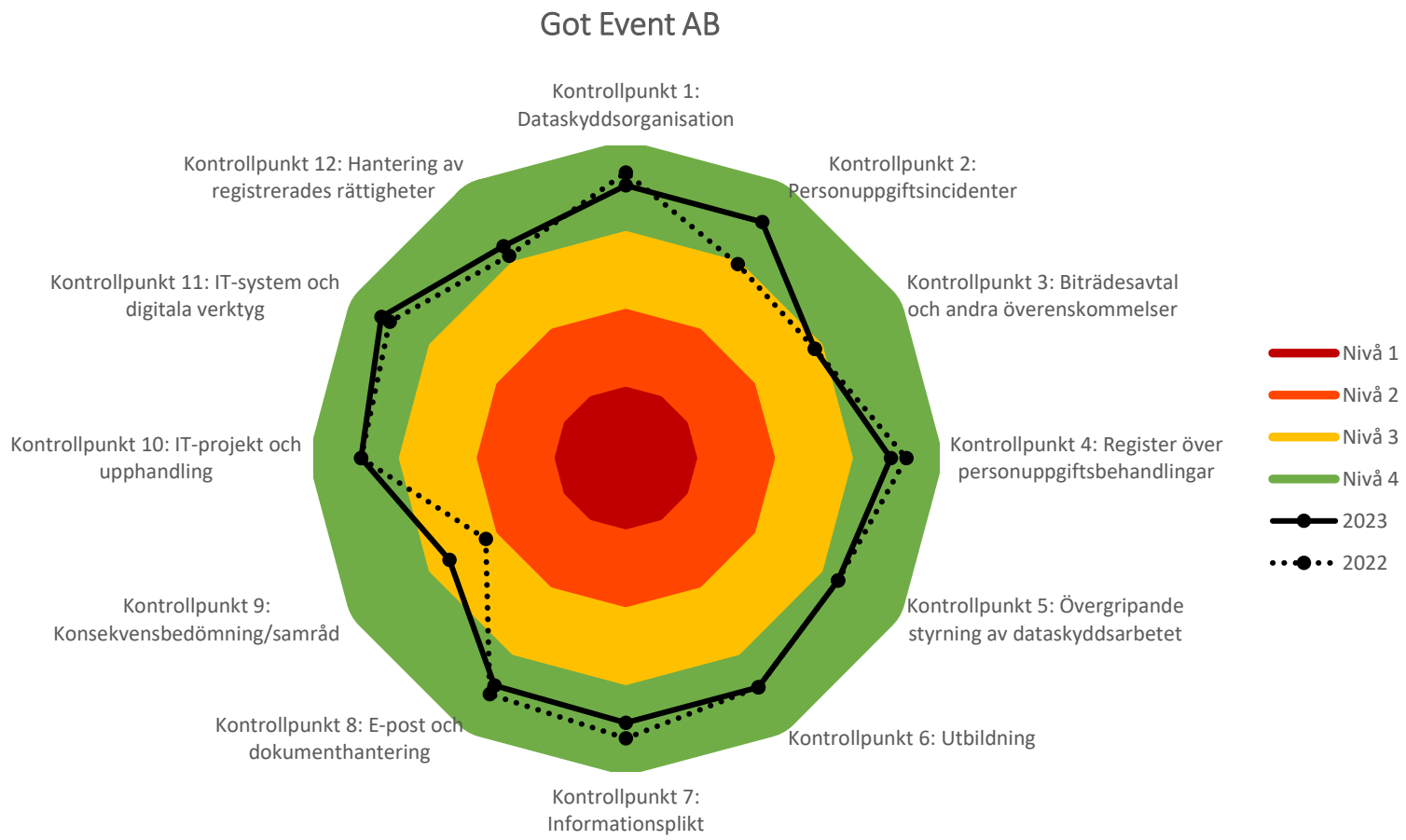
Säkerställ att bolaget har utfört och dokumenterat riskbedömningar avseende behandlingar kopplade till kamerabevakningen. Säkerställ även att det finns framtagna och fastställda konsekvensbedömningar för respektive behandling i de fall sådana krävs.

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

Got Event 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.