Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Göteborgs Hamn 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 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.

Även om bolaget hamnar på samma risknivå som förgående år, noterar dataskyddsombudet att bolagets skattning är högre jämfört med år 2022. Dataskyddsombudet instämmer i bolagets bedömning att det har skett förbättringar inom kontrollpunkten under året.

Utifrån iakttagelser under året har dataskyddsombudet uppmärksammat att det sker ett omfattande arbete med att etablera en intern dataskyddsorganisation inom bolaget, vilket dataskyddsombudet ser som mycket positivt. Dataskyddsombudet uppmuntrar bolaget att fortsätta det goda arbetet och säkerställa att utvecklingen av den interna dataskyddsorganisationen fortskrider. Framåt rekommenderas bolaget att ge den interna dataskyddsorganisationen möjlighet att se över vilka resurser, vilken kompetens och vilka rutiner/anvisningar (kopplat till roller, ansvar och beslutsmandat) som behövs inom verksamheten för att kunna säkerställa dataskyddsperspektivet fullt ut.

Under året har dataskyddsombudet och dataskyddsgruppen haft regelbundna avstämningar, vilket är positivt och något som bolaget uppmuntras att fortsätta med.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

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 avseende risknivån, men har inte heller kontrollerat hanteringen av personuppgiftincidenter särskilt under året.

Både vid avstämning med verksamheten och i uppföljningen av den fördjupade kontrollen för år 2022 har dataskyddsombudet fått information om att bolaget under året genomfört interna kontroller avseende kunskapsnivån inom informationssäkerhetsområdet, där personuppgiftsincidenter har varit en del.

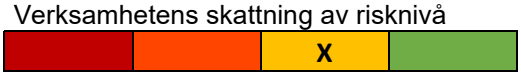
Verksamheten arbetar för närvarande med framtagandet av nya utbildningar för medarbetare, och personuppgiftsincidenter kommer ingå i dessa. Bolaget har även i uppföljningen angett att det sedan april 2023 finns en tydlig rutin på intranätet för hur medarbetare ska agera vid en personuppgiftsincident och att det finns ett formulär för rapportering till dataskyddskontakterna. Dataskyddsombudet ser det som positivt att bolaget under året har arbetat aktivt med kontrollpunkten.

Dataskyddsombudet vill även framhålla att det är viktigt att följa upp och säkerställa att bolagets vidtagna åtgärder och insatser får önskad effekt framåt. Efter genomförd utbildning bör bolaget utvärdera om antalet inrapporterade incidenter ökar samt om rapporteringen sker till rätt utpekade personer internt. Eftersom dataskydd i de flestas dagliga arbete är en mindre fråga kan det även finnas behov av att med visst intervall påminna medarbetare om vad en personuppgiftsincident är och hur man går till väga vid misstanke om att en sådan inträffat. Utifrån detta, och med hänsyn till att majoriteten av inträffade incidenter beror på den mänskliga faktorn, uppmuntras bolaget till att även framåt se över hur anställda kontinuerligt kan hållas informerade.

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

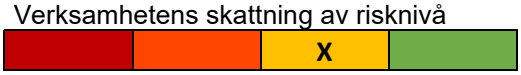
Likt förgående år anger bolaget i årets skattning att det saknas rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden i syfte att säkerställa att dessa uppfyller villkoren i biträdesavtal. Utifrån detta kvarstår rekommendationen som lämnades i årsrapporten för 2022, då efterlevnadskontroller är en viktig del i att uppfylla ansvarsprincipen i GDPR.

Dataskyddsombudet noterar även att bolaget uppskattar att andelen tecknade personuppgiftsbiträdesavtal med personuppgiftsbiträden är ca 50 % jämfört med år 2022 då det uppskattades till 75 %. I samband med genomgången av årsrapporten uppgav bolaget att den lägre skattningen inte beror på ändrade förhållanden inom bolaget, utan på att årets svar sannolikt bättre stämmer överens med de faktiska omständigheterna. Dataskyddsombudet ser att det är positivt att bolaget har identifierat detta. Att det finns en medvetenhet kring det ger bolaget goda förutsättningar att arbeta med kontrollpunkten. Bolaget rekommenderas att se över

för vilka biträden avtal saknas och säkerställa att sådana upprättas. Bolaget rekommenderas även att framåt säkerställa att personuppgiftsbiträdesavtal ingås i direkt anslutning till att ett personuppgiftsbiträde anlitas.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



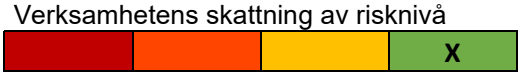
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten och har inte heller kontrollerat behandlingsregistret särskilt, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

Bolaget uppskattar att ca 75 % av bolagets personuppgiftsbehandlingar finns upptagna i nuvarande behandlingsregister. Det uppskattas även att ca 75 % av de registrerade behandlingar innehåller all den information som ska framgå av artikel 30 i GDPR. Utifrån svaren noterar dataskyddsombudet att bolagets skattning är oförändrad jämfört med år 2022. Utifrån detta kvarstår rekommendationen från årsrapporten 2022 om att se över och komplettera behandlingsregistret.

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 fått några direkta indikationer som medför en annan bedömning än den som bolaget gör. Dataskyddsombudet har även noterat att bolaget under året har arbetat mer aktivt med dataskyddsfrågor jämfört med tidigare år. Bolaget rekommenderas därför 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 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.

Dataskyddsombudet ser det som positivt att bolaget under året har genomfört en intern översyn av kunskapsnivån avseende personuppgiftsincidenter hos medarbetarna. Det är också positivt att bolaget arbetar aktivt med att planera utbildningar för medarbetarna, vilket bolaget uppmuntras att fortsätta med framöver. Bolaget rekommenderas även genomföra en översyn av den allmänna kunskapsnivån inom dataskydd bland medarbetarna. Särskilt kopplat till kontrollpunkt 12 om registrerades rättigheter.

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 fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat informationsplikten särskilt.

Under året har dataskyddsombudet och verksamheten haft en dialog om informationsplikten. Bolaget har i samband med detta uppgett att den externa integritetspolicyn på hemsidan inte är heltäckande, utan att ytterligare information ges till registrerade i olika sammanhang. Dataskyddsombudet har även fått uppfattningen att det finns planer framåt på att göra en översyn över vilken information som lämnas till registrerade vid olika behandlingar och, vid behov, uppdatera informationen. Dataskyddsombudet ser det som positivt och uppmuntrar bolaget att involvera dataskyddsombudet när arbetet genomförs.

Dataskyddsombudet vill även i sammanhanget lyfta att bolaget bör undvika att hänvisa till dokumenthanteringsplaner och gallringsbeslut i sin

integritetsinformation för att beskriva lagringstiden. Dataskyddsombudet bedömer det som tveksamt om hänvisning till dokumenthanteringsplaner och gallringsbeslut som den registrerade inte har tillgång till kan anses tillräckligt. Det kan vara tillräckligt att hänvisa till kriterierna för hur lagringstiden bedöms om exakt lagringstid inte anges. Den registrerade ska dock, utifrån sin egen situation, i så fall kunna bedöma lagringstiden utifrån kriterierna.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

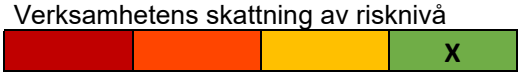
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras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

Dataskyddsombudet noterar att årets skattning indikerar att verksamhetens arbete har förbättrats sedan föregående år. Utifrån bolagets egen skattning kan dock dataskyddsombudet utläsa att det inom kontrollpunkten föreligger risker kopplat till att verksamheten saknar dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut.

Dataskyddsombudet rekommenderar därför, i likhet med rekommendationerna från årsrapporten 2022, bolaget att ta fram tydliga rutiner/anvisningar för att kontrollera och säkerställa att handlingar som innehåller personuppgifter gallras i enlighet med gällande gallringsbeslut, vilket utgör en viktig del i att uppfylla principen om lagringsminimering.

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 kräver omgående åtgärder.

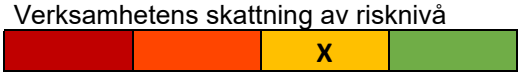
Enligt bolaget finns det framtagna och fastställda konsekvensbedömningar för ca 100 % av verksamhetens personuppgiftsbehandlingar som innebär hög risk. Inför årsrapporten 2022 angav bolaget att andelen var ca 50 %. Svaret indikerar att konsekvensbedömningar har genomförts under året. Dataskyddsombudet har dock

inte rådfrågats i arbetet med konsekvensbedömningar under året. Utifrån bolagets egen skattning går det att utläsa att verksamheten sällan involverar dataskyddsombudet för att inhämta råd och rekommendationer vid arbetet med konsekvensbedömningar. Enligt dataskyddsförordningen ska dataskyddsombudet rådfrågas vid genomförande av en konsekvensbedömning avseende dataskydd. Det är därmed inte valbart att involvera dataskyddsombudet. Om konsekvens-bedömningar har genomförts under året behöver bolaget inhämta dataskydds-ombudets råd och rekommendationer avseende dessa för att underlagen ska kunna anses uppfylla kriterierna för en godtagbar konsekvensbedömning enligt GDPR.

Utifrån ovan rekommenderas bolaget att framåt säkerställa att dataskyddsombudet involveras vid arbetet med konsekvensbedömningar. Bolaget rekommenderas även att ta fram rutiner/anvisningar för att inhämta och dokumentera dataskyddsombudets synpunkter i de fall verksamheten, efter att ha genomfört en riskanalys, bedömer att en konsekvensbedömning inte behöver göras.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



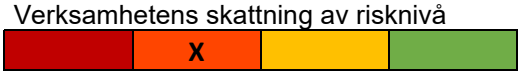
Dataskyddsombudets bedömning

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 särskild bedömning kan göras i frågan.

Dataskyddsombudet bedömer dock, i likhet med vad bolaget har identifierat, att bolaget behöver säkerställa rutiner för att involvera dataskyddsombudet från start vid införande av nya IT-projekt och införande av nya tjänster där personuppgifter kommer att hanteras. Bolaget rekommenderas därför att framåt säkerställa att så sker.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

I likhet med årsrapporten 2022 ser dataskyddsombudet risker kopplat till att bolaget saknar en tydlig överblick över bolagets kommunikationskanaler samt

bristen på rutiner för att säkerställa dataskyddsperspektivet vid införandet av kostnadsfria tjänster. Med anledning av detta kvarstår rekommendationerna från årsrapporten 2022 i dessa delar.

Dataskyddsombudet ser även risker kopplade till att bolaget inte vet om det finns dokumenterade arbetssätt för att systematiskt kunna följa upp och kontrollera att användning av system och/eller andra digitala verktyg följer antagna styrande dokument. Enligt skattningen kan bolaget inte svara på om det finns målgruppsanpassad information för de digitala verktyg som används och som tillhandahålls användarna. Bolaget uppger även att det saknas dokumenterade arbetssätt för tilldelning av behörigheter och åtkomster i IT-system. Dessa delar är nära sammankopplade med den personuppgiftsansvariges skyldighet att säkerställa att personuppgifter skyddas genom tillräckliga organisatoriska och tekniska säkerhetsåtgärder. Även om verksamheten regelbundet följer upp behörigheter och åtkomst till personuppgifter i IT-system behöver bolaget redan vid tilldelning av behörigheter och åtkomster säkerställa att medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetare ska kunna utföra sina arbetsuppgifter. Genom att ha dessa rutiner på plats kan även risken för personuppgiftsincidenter minska.

I samband med genomgången av årsrapporten uppgav bolaget att det pågår ett arbete med att uppdatera riktlinjer på policy-nivå och att bolaget tar ett område i taget. Enligt bolaget ligger det i planeringen att se över ovanstående delar, vilket dataskyddsombudet ser som positivt. Bolaget uppger även att det finns bra rutiner och arbetssätt för tilldelning av behörigheter och åtkomst till IT-system, men att mindre delar av rutinerna behöver uppdateras. Bolaget rekommenderas att fortsätta arbetet och komplettera rutinerna med de delar som den interna dataskydds-organisationen bedömer krävs för att rutinerna ska bli ändamålsenliga.

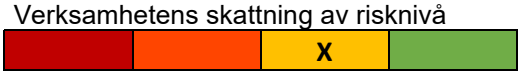
Vidare delar dataskyddsombudet inte bolagets bedömning vad gäller användningen av kakor (”cookies”) på bolagets hemsida, och bolaget bedöms bland annat behöva säkerställa att kraven på information till registrerade uppfylls kopplat till användningen. Informationen som lämnas behöver vara specifik, tydlig och fullständig och användaren ska ges förutsättningar för att förstå konsekvenserna av sitt samtycke. Av informationen ska bland annat framgå vem som lagrar eller hämtar cookies, giltighetstiden för cookies och om informationen delas med någon annan part. Utifrån detta rekommenderas bolaget prioritera arbetet med att se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl dataskyddsförordningen som LEK (lagen (2022:482) om elektronisk kommunikation).

Även vid årets genomgång av bolagets kommunikationskanaler noterar dataskyddsombudet att bolaget använder sociala medier. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget rekommenderas därför att 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. 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.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

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 hantering av registrerades rättigheter särskilt.

Utifrån verksamhetens egen skattning bedömer dataskyddsombudet att det föreligger risker kopplat till att den utbredda medvetenheten om registrerades rättigheter bland medarbetarna är låg och att bolaget saknar dokumenterade arbetssätt för att hantera ett tillbakadragande av samtycke från registrerade. En förutsättning för att registrerades rättigheter ska kunna tillvaratas är att medarbetare har kunskap om rättigheterna. Brister kunskapen hos medarbetarna kan det innebära att registrerade riskerar att inte kunna utöva sina lagstadgade rättigheter. Avsaknaden av rutiner för hur ett tillbakadragande av samtycke ska hanteras kan leda till att bolaget fortsätter att behandla den registrerades personuppgifter trots att den registrerade har dragit tillbaka sitt samtycke. Vid en sådan situation skulle det innebära att bolaget saknar rättslig grund för behandlingen.

Bolaget rekommenderas därför, i anslutning till kontrollpunkten 6 om utbildning, att se över hur medvetenheten om vilka rättigheter registrerade har kan stärkas inom bolaget. Bolaget rekommenderas även, i enlighet med rekommendationerna i årsrapporten för 2022, att ta fram en rutin för att hantera situationen då ett samtycke från en registrerad dras tillbaka.

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): Personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Förtydliga rutin och komplettera den med en instruktion eller stödmaterial/metod som anger vilken information som ska förmedlas till dataskyddskontakt samt tydliggöra arbetsgången inom bolaget vid upptäckten av en personuppgiftsincident.
- Se över medarbetares kunskap gällande vad som är en personuppgiftsincident.
- Utbilda medarbetare om personuppgiftsincidenter och hantering av dessa inom bolaget.

Kommentarer och rekommendationer:

Bolaget har i uppföljningen uppgett att det sedan våren 2023 finns en tydlig instruktion för hur medarbetare ska agera vid en personuppgiftsincident. Rutinen finns tillgänglig på bolagets intranät. På intranätet finns även ett formulär för rapportering av personuppgiftsincidenter till bolagets dataskyddskontakter.

Vidare har bolaget under året gjort en översyn av kunskapsnivån avseende personuppgiftsincidenter genom att ca 50 % av medarbetarna har intervjuats. Bolaget arbetar nu med att ta fram en ny utbildning som ska gå ut till alla anställda i slutet av året. Utbildningen kommer även att vara obligatorisk för nyanställda framåt.

Sammantaget visar uppföljningen att verksamheten har vidtagit åtgärder med anledning av dataskyddsombudets rekommendationer. Det framgår även att det finns ytterligare åtgärder i form av utbildning inplanerade framåt. Ytterligare kommentarer och rekommendationer lämnas under kontrollpunkt 2 i årsrapporten.

Då åtgärder vidtagits för att hantera identifierade risker kommer fortsatt uppföljning ske inom ramen för de fasta kontrollpunkterna, om inget särskilt föranleder att det behövs 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 behandlingar och den information som saknas.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Se över vilka behandlingar som det finns genomförda konsekvensbedömningar för, och inhämta dataskyddsombudets råd och rekommendation för genomförda konsekvensbedömningar där dataskyddsombudets synpunkter saknas.

Säkerställ att dataskyddsombudet involveras vid arbetet med konsekvensbedömningar, och ta fram rutiner/anvisningar för att inhämta och dokumentera dataskyddsombudets synpunkter i de fall verksamheten, efter att ha genomfört en riskanalys, bedömer att en konsekvensbedömning inte behöver göras.

- Kontrollpunkt 11: IT-system och digitala verktyg

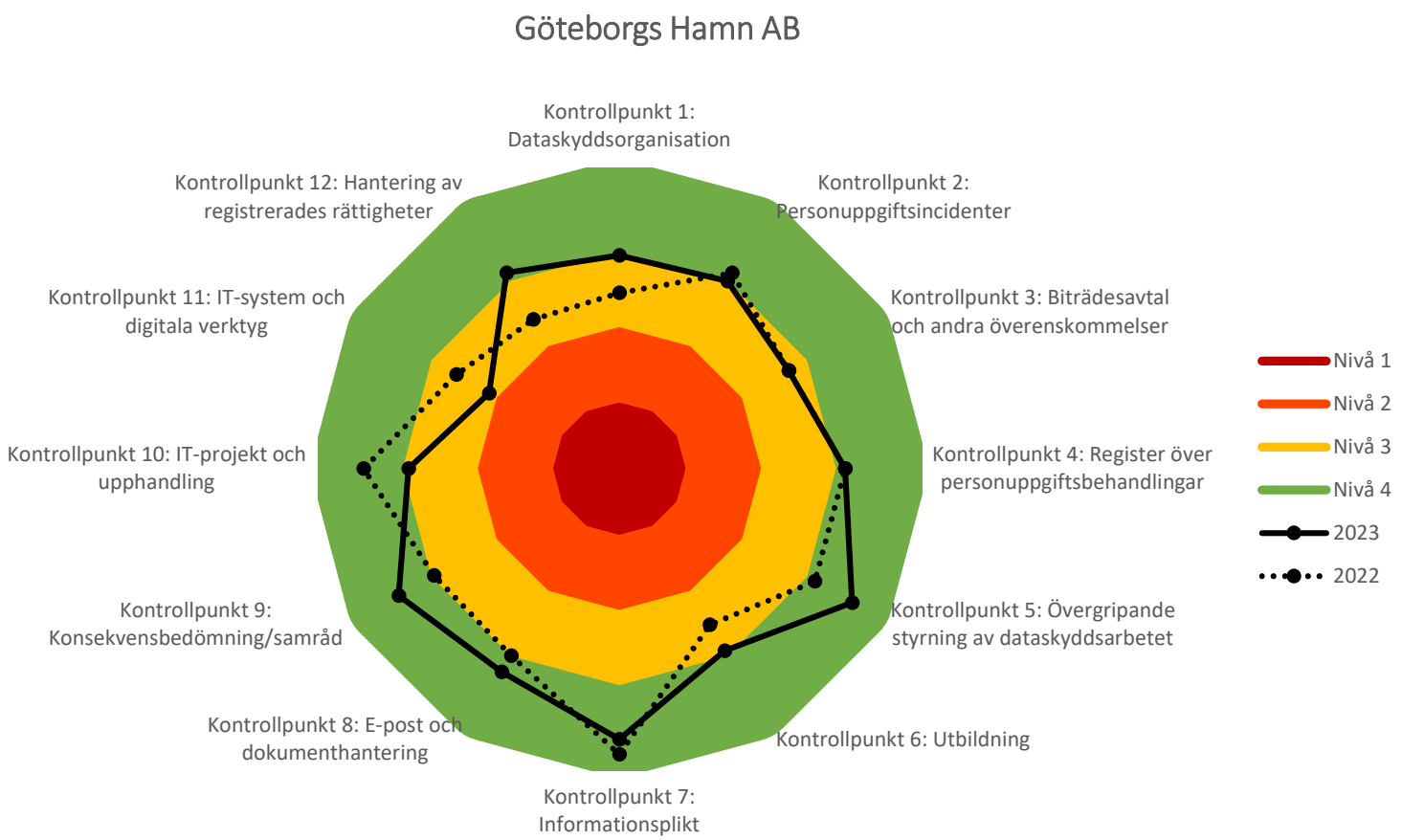
Se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl dataskyddsförordningen som LEK (lagen (2022:482) om elektronisk kommunikation).

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

Göteborgs Hamn 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.