Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Göteborg & Co AB

2023-12-18

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

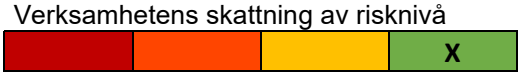
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga.

Dataskyddsombudets bedömning är att bolaget har goda förutsättningar för att kunna bedriva ett effektivt och fungerade dataskyddsarbete. Samtidigt ser dataskyddsombudet att en dataskyddsorganisation som består av en eller ett mycket litet antal personer medför sårbarhet. Det kan resultera i att dataskyddsarbetet inom bolaget blir personberoende. Det finns även risk för att den interna dataskyddsorganisationen inte hinner med alla de uppgifter som behöver göras. Framåt rekommenderas bolaget fortsätta stödja det goda arbete som redan bedrivs, samt ge den interna dataskyddsorganisationen möjlighet att se över vilka resurser och vilken kompetens man behöver inom verksamheten för att kunna säkerställa dataskyddsperspektivet fullt ut.

Under året har dataskyddsombudet haft en löpande dialog med verksamhetens dataskyddskontakt, vilket dataskyddsombudet ser som mycket 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 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 avseende risknivån.

Personuppgiftincidenter inom bolaget har tidigare år varit föremål för en fördjupad kontroll. Utifrån svaren från uppföljningen har ett flertal åtgärder vidtagits. Bland annat har bolaget beslutat om ett nytt styrdokument som avser rutiner för hantering av personuppgiftsincidenter. Bolaget uppger att fler personuppgiftsincidenter har identifierats under året vilket tyder på att bolagets utbildningar och informationsinsatser har gett effekt och att den generella kunskapen om incidenter har höjts. Dataskyddsombudet ser det som positivt och uppmuntrar bolaget att fortsätta sitt arbete under kontrollpunkten.

Dataskyddsombudet vill även i sammanhanget påminna om att behovet av utbildning kan se olika ut för olika medarbetare. Det är därför viktigt att bolaget framåt säkerställer att medarbetare får den utbildning som är lämplig utifrån arbetsuppgifter och befattning. Dataskyddsombudet noterar exempelvis att det ligger på respektive chef att fatta beslut kring personuppgiftsincidenter. Det är därmed viktigt att säkerställa att personerna 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. För att stödja chefer i sin bedömning, och utöver att löpande ge riktade utbildningar till dessa, rekommenderas bolaget att framåt ta fram en tydlig instruktion/metod för hur en bedömning av risker för de registrerades fri- och rättigheter ska göras.

Dataskyddsombudet noterar att bolaget i skattningen angett att 0 % av personuppgiftsincidenterna som kräver en anmälan har rapporterats i tid till tillsynsmyndigheten under året. Enligt uppgifter från bolaget rör det sig om en incident. Vid genomgången av årsrapporten med bolaget framgick att den incidenten som inte anmälts i tid gäller en incident som inträffat hos en intern tjänsteleverantör i Staden. Då bolaget inte har rådighet över den praktiska hanteringen hos biträdet ser dataskyddsombudet, utöver att säkerställa att hanteringen regleras i personuppgiftsbiträdesavtalen, att bolagets möjligheter till åtgärder är begränsade. Dataskyddsombudet vill i sammanhanget uppmärksamma bolaget på att tidsfristen för anmälan börjar löpa från det att bolaget får vetskap om incidenten. Framåt rekommenderas bolaget att anmäla incidenter så snart bolaget får vetskap om incidenten och får indikationer på att incidenten kan vara anmälningspliktig, även om bolaget vid tidpunkten inte kan göra en fullständig riskbedömning. Bolaget kan på så sätt säkerställa att tidsfristen hålls, och vid behov komplettera anmälan av incidenten i efterhand.

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, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

I likhet med förgående år uppger verksamheten att det saknas rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden. Rekommendationen från årsrapporten 2022 kvarstår därför i denna del.

Bolaget uppger att avtal har tecknats med ca 50 % av de biträden som anlitas av bolaget. I samband med genomgången av årsrapporten uppger bolaget att detta beror på att biträdesavtal saknas med stadens interna tjänsteleverantörer. Dataskyddsombudet har noterat att det är flera förvaltningar och bolag inom Göteborgs stad där detta förekommer. Dataskyddsombudet rekommenderar bolaget att föra dialog med stadens interna tjänsteleverantörer och kartlägga ansvarsförhållandena för att se över för vilka personuppgiftsbehandlingar som kräver att avtal tecknas.

Utifrån skattningen har det skett förbättringar inom bolaget avseende att bedöma hela kedjan av underbiträden vid anlitande av ett nytt personuppgiftsbiträde samt att det har tagits fram dokumenterade arbetssätt för bedömning av om det finns ett gemensamt personuppgiftsansvar. Dataskyddsombudet ser det som positivt. Hur personuppgiftsansvaret ska fördelas är oftast en svår fråga och bolaget rekommenderas att även framåt involvera dataskyddsombudet vid tveksamheter eller osäkerhet.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå

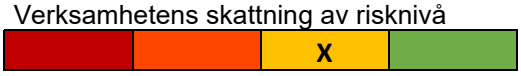
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat behandlingsregistret särskilt.

Utifrån verksamhetens skattning och vid jämförelse med förgående år kan dataskyddsombudet utläsa att det har skett ett omfattande och intensivt arbete med behandlingsregistret under året. Inför årsrapporten 2022 uppskattade bolaget att endast ca 25 % av bolagets samtliga personuppgiftsbehandlingar fanns dokumenterade i behandlingsregistret. I år uppskattar bolaget att samtliga personuppgiftsbehandlingar finns med i behandlingsregistret. Dataskyddsombudet ser det som positivt att bolaget har arbetat med behandlingsregistret under året. Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen och att framåt kontinuerligt uppdatera behandlingsregistret.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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.

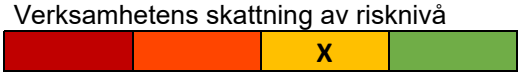
Under året har dataskyddsombudet noterat att verksamheten har arbetat med att ta fram ett flertal nya rutiner/anvisningar och gjort en översyn över verksamhetsområden där personuppgiftsbehandlingar förekommer. En prioriteringslista har därefter gjorts utifrån behandlingar/verksamhetsområden med hög risk där även ledningsnivån har varit involverad. Det visar på att bolaget har antagit ett riskbaserat arbetssätt och har en tydlig planering framåt. Dataskyddsombudet anser att bolagets arbetssätt i dessa delar har varit positiva.

Bolaget rekommenderas, utifrån sin skattning, att framåt se över hur interna kontroller kontinuerligt kan genomföras för att följa upp och säkerställa följsamhet gentemot GDPR samt kontrollera så att de rutiner och anvisningar som finns på plats får genomslag i praktiken.

Vidare visar skattningen att det kvarstår risker kopplat till att arbeta systematiskt med att integrera dataskyddsfrågor i det övriga informationssäkerhetsarbetet. Bolaget uppger exempelvis att det saknas styrande dokument för hur medarbetare ska hantera IT-system, datorer och mobila enheter och hur dessa får användas i det dagliga arbetet. Vidare uppger bolaget under kontrollpunkt 8 att det saknas rutin för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Det saknas även rutiner för att efterleva kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster. Eftersom informationssäkerhet är en central del i dataskyddsarbetet rekommenderas bolaget att se över nuvarande hantering och bedöma vilka åtgärder som behöver vidtas för att hantera riskerna. I samband med genomgången av årsrapporten uppger bolaget att det har saknats en funktion inom bolaget för arbetet med informationssäkerhet, men att det under året har startats ett arbete kring att se över informationssäkerhetsarbetet.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte kontrollerat kunskapsnivån inom bolaget särskilt, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

Utifrån verksamhetens skattning har det skett förbättringar avseende att verksamheten genomför regelbundna informationsinsatser för att utbilda och informera medarbetare inom dataskydd. Under året har dataskyddsombudet fått kännedom om att informationsinsatser har genomförts avseende personuppgifts-incidenter på arbetsplatsträffar. Därtill är dataskyddsenhetens digitala utbildning ”Dataskydd på jobbet” numera obligatorisk, vilket dataskyddsombudet ser som positivt. Bolaget rekommenderas att fortsätta med utbildnings- och informationsinsatser för att förbättra den allmänna kunskapsnivån inom bolaget, särskilt kopplat till kontrollpunkt 12 om registrerades rättigheter.

Dataskyddsombudet kan även utläsa att det kvarstår risker kopplat till att kartlägga vilken nivå av dataskyddskunskaper som olika befattningars arbete kräver. Bolaget rekommenderar att kartlägga utbildningsbehovet och planera utbildnings- och informationsinsatser utifrån identifierade behov. 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 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 informationsplikten särskilt.

Under året har verksamheten informerat att en uppdatering av den externa integritetspolicyn pågår. Dataskyddsombudet ser det som positivt då dataskyddsombudet gör bedömningen att bolaget behöver utveckla informationen ytterligare för att uppfylla kraven enligt art. 13 och 14 i GDPR. Bolaget rekommenderas att fortsätta arbeta med den externa integritetspolicyn samt att säkerställa att den kontinuerligt ses över. I sammanhanget vill dataskyddsombudet även lyfta att kontrollpunkten i år har ändrats till att avse informationsplikten. Informationsplikten är långtgående och omfattar mer än enbart den externa integritetspolicyn.

För att informationsplikten ska anses vara uppfylld finns det krav på såväl när informationen ska lämnas, vilken information som lämnas och hur den lämnas. Personuppgiftsansvariga ska även informera om alla personuppgiftsbehandlingar som genomförs. Bolaget rekommenderas därför att säkerställa att även ytterligare information tillhandahålls registrerade i samband med behandlingar utöver det som lämnas i den externa integritetspolicyn.

Utifrån bolagets skattning rekommenderar dataskyddsombudet även att bolaget säkerställer att integritetsinformationen är enkel att nå från samtliga av verksamhetens digitala kanaler. Ett första steg för detta är att bolaget kartlägger sina kommunikationskanaler för att få en överblick över bolagets samtliga kommunikationskanaler (se kontrollpunkt 11).

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet ser dock att det är positivt att bolaget har arbetat utifrån rekommendationen i årsrapporten 2022 avseende att informera registrerade direkt i samband med upprättande av kontakt om hur deras personuppgifter hanteras.

Verksamhetens svar indikerar att det kvarstår risker kopplat till att det saknas rutiner för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut samt hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Vidare kvarstår risker kopplat till att det saknas rutiner för hur personuppgifter får hanteras i e-post. Dataskyddsombudets rekommendationer från årsrapporten 2022 kvarstår därför i dessa delar.

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 till viss del verksamhetens bedömning, men gör till

skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver åtgärder.

Utifrån bolagets egen skattning noterar dataskyddsombudet att det har skett förbättringar på flera områden under kontrollpunkten. Bland annat anger verksamheten att det numera finns dokumenterade arbetssätt för att identifiera personuppgiftsbehandlingar med hög risk samt att det finns dokumenterade arbetssätt för att genomföra och dokumentera konsekvensbedömningar.

Eftersom bolaget endast har en framtagen konsekvensbedömning är dataskyddsombudets bedömning att kontrollpunkten behöver prioriteras framöver utifrån att det i vissa fall är ett krav att konsekvensbedömningar genomförs. I dialoger med dataskyddsombudet under året har bolaget uppgett att det finns en framtagen planering för arbetet med konsekvensbedömningar och att det pågår ett arbete internt, vilket är positivt. Bolaget rekommenderas att fortsätta arbetet under kontrollpunkten och säkerställa att konsekvensbedömningar genomförs framåt.

Utifrån skattningen kan dataskyddsombudet utläsa att bolaget har utvecklingsbehov gällande att ta fram rutiner för att uppdatera konsekvensbedömningar vid förändringar i behandlingen. Dataskyddsombudet bedömer dock att bolaget bör prioritera arbetet med att genomföra konsekvensbedömningar.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

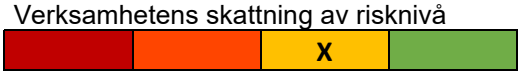
Dataskyddsombudets bedömning

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

I likhet med föregående år rekommenderas bolaget att säkerställa att dataskyddsombudet involveras i ett tidigt skede och på ett systematiskt sätt vid uppstart av nya IT-projekt, vid införande av nya system/tjänster eller i samband med upphandlingar.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och som kräver omgående åtgärder.

Under året dataskyddsombudet och bolaget haft en dialog om användningen av sociala medier och analysverktyget Google Analytics. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. I dialog mellan dataskyddsombudet och verksamheten har dataskyddsombudet rekommenderat bolaget att bland annat kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier/analysverktyg, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna. I samband med avstämningar har verksamheten uppgett att bolagets användning av sociala medier finns med i planeringen framåt. Verksamheten har även meddelat att frågan om användning av Google Analytics ska diskuteras mer ingående internt.

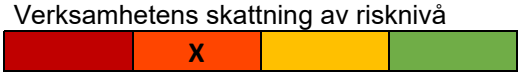
Dataskyddsombudet har även noterat att bolaget använder Facebook-pixeln, varför ovan rekommendation även omfattar användningen av pixeln.

Därutöver kan dataskyddsombudet utläsa, utifrån bolaget skattning, att det kvarstår behov av att bolaget kartlägger vilka kommunikationskanaler som verksamheten använder för att få en tydlig överblick över bolagets kommunikationskanaler.

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



Dataskyddsombudets bedömning

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

Av skattningen kan dataskyddsombudet utläsa att den utbredda medvetenheten inom verksamheten om vilka rättigheter de registrerade har är låg. Därtill saknas det dokumenterade arbetssätt för 1) att bedöma när en invändning mot en personuppgiftsbehandling från den registrerade är uppenbart ogrundad eller orimlig, 2) hur en begäran om registerutdrag ska hanteras samt 3) att hantera ett tillbakadragande av samtycke från en registrerad. Dataskyddsombudet har dock fått indikationer på att det pågår ett arbete inom verksamheten för att åtgärda riskerna, och det har bland annat tagits fram ett utkast på rutin för hantering av registrerades rättigheter. Rutinen har översänts till dataskyddsombudet för råd och rekommendationer. Dataskyddsombudet ser det som positivt att verksamheten

arbetar med frågan och rekommenderar bolaget att fortsätta det påbörjade arbetet inom kontrollpunkten. Bolaget rekommenderas även, i anslutning till kontrollpunkt 6 om utbildning, att se över hur medvetenheten om vilka rättigheter registrerade har kan stärkas inom bolaget för att säkerställa att registrerades rättigheter kan tillgodoses.

Dataskyddsombudet vill även framhålla att det är positivt att bolaget har identifierat risken under den nämnda punkten. Det är först i samband med att risken har identifierats som åtgärder kan vidtas. Mot bakgrund av ovanstående rekommenderas bolaget att fortsätta prioritera arbetet med hantering av registrerades rättigheter under 2024.

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:

- Bolaget behöver ta fram en dokumenterad instruktion för hantering av personuppgiftsincidenter vilket bör, utöver den befintliga information som den idag innehåller, minst innehålla följande:
  - Rutiner för att kunna avgöra vad som är en personuppgiftsincident.
  - Rutiner för hur arbetstagarna inom organisationen ska agera om en incident inträffar.
  - Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten.
  - Rutiner för anmälan av incident till Integritetsskyddsmyndigheten inom 72 timmar efter upptäckten.
  - Rutin för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- Komplettera rutinen med vem som beslutar gällande att bedöma om en anmälan till Integritetsskyddsmyndigheten ska göras.
- Se över medarbetares kunskap gällande vad som är en personuppgiftsincident.
- Utbilda alla medarbetare om personuppgiftsincidenter och hantering av dessa.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit ett antal åtgärder under året. I uppföljningen uppger bolaget att det har beslutats om ett nytt styrande dokument, ”Göteborg & Co AB:s rutin för hantering av personuppgiftsincidenter”. Vidare

uppger bolaget att dataskyddsenhetens utbildning, ”Dataskydd på jobbet – Bolag i Göteborgs Stad”, numera är en obligatorisk utbildning och att det framgår i bolagets anvisning för dataskydd att alla nyanställda på bolaget ska genomgå utbildningen. I början av 2023 skickades information om den obligatoriska utbildningen till samtliga medarbetare och medarbetare fick även tillfälle att genomgå utbildningen. För att säkerställa att samtliga medarbetare fullföljde utbildningen fick medarbetarna rapportera in deltagandet i bolagets HR-system. I samband med utskicket fick medarbetarna riktad information om vad de ska göra om en personuppgiftsincident inträffar på bolaget.

Uppföljningen visar att verksamheten har vidtagit åtgärder med anledning av dataskyddsombudets rekommendationer. Fortsatt uppföljning kommer 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 9: Konsekvensbedömningar

Arbeta utifrån bolagets framtagna prioriteringslista och säkerställ att konsekvensbedömningar framåt genomförs.

- Kontrollpunkt 12: Hantering av registrerades rättigheter

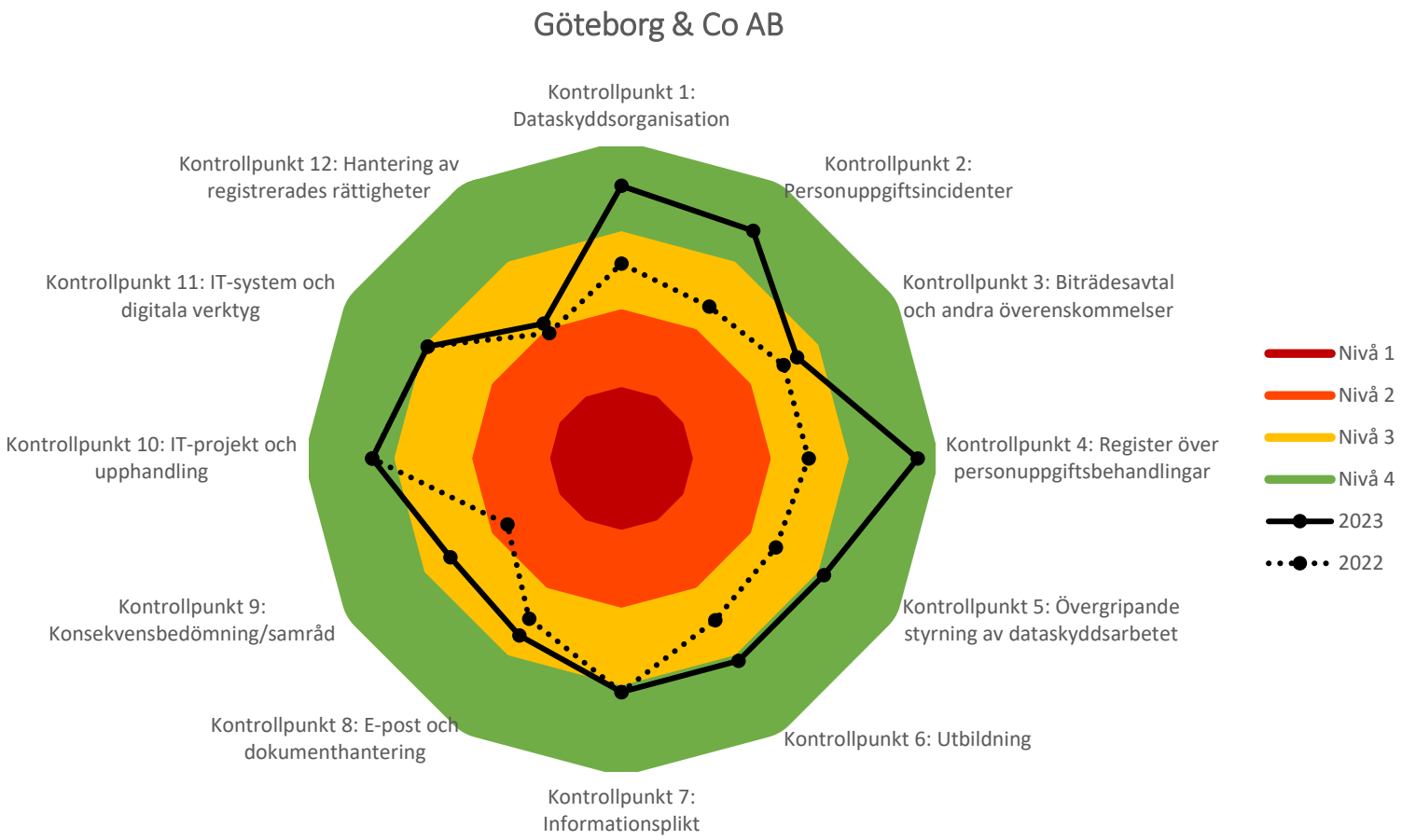
Öka medvetenheten och kunskapsnivån om registrerades rättigheter bland medarbetare genom att se över vilka utbildnings- och informationsinsatser som krävs.

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

Göteborg & Co 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.