Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Familjebostäder i Göteborg AB

2023-12-20

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

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

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

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

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

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

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

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[1]

Risknivå	Beskrivning	Färgkod
Nivå 1	Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2	Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3	Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4	Inga direkta risker av betydelse identifierade. Indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete.	

3.2 Resultat från kontrollen 2023

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

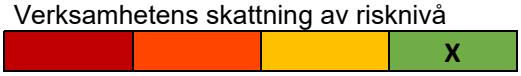
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Även om bolaget har en intern dataskyddsorganisation bedömer dataskyddsombudet, utifrån bolagets skattning och gjorde iakttagelser under året, att den interna dataskyddsorganisationen behöver ges ett ökat stöd och mer resurser för att få rätt förutsättningar att utföra arbetet. Bolaget uppger att det sker ett arbete internt med att försöka hitta formerna för att knyta ihop kompetensen inom bolaget, vilket dataskyddsombudet ser som positivt. Den interna dataskyddsorganisationen uttrycker även att det finns ett behov av att förtydliga roller och ansvar kring dataskydd och informationssäkerhet, särskilt avseende rollen som samordnare. Framåt rekommenderas bolaget att stötta den interna dataskyddsorganisationen i frågorna och se över hur olika roller kopplat till ansvar kan konkretiseras.

Bolaget uppmuntras även fortsättningsvis att regelbundet involvera dataskyddsombudet i dataskyddsfrågor.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



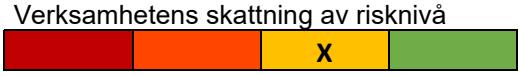
Dataskyddsombudets bedömning

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

Utifrån verksamhetens skattning kan dock dataskyddsombudet utläsa att inträffade incidenter sällan följs upp som en naturlig del i dataskyddsarbetet. Bolaget rekommenderas därför att se över hur inträffade incidenter kan följas upp framåt som en del i verksamhetens proaktiva dataskyddsarbete.

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 inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

I likhet med föregående år anger bolaget ett lågt värde för om det finns dokumenterade arbetssätt för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden i syfte att säkerställa att dessa uppfyller villkoren i biträdesavtalen. Bolaget anger även ett lågt värde avseende om det finns kompetens och/eller dokumenterade arbetssätt för att bedöma hela kedjan av underbiträden vid anlitande av ett nytt personuppgiftsbiträde. Utifrån detta kvarstår rekommendationerna från 2022 om att säkerställa att det finns kompetensen och dokumenterade arbetssätt för bedömning av hela kedjan av underbiträden samt för efterlevnadskontroller då det är viktiga delar i att uppfylla omsorgsplikten enligt art. 28 i GDPR och ansvarsskyldigheten i GDPR.

Vidare anger bolaget att personuppgiftsbiträdesavtal har tecknats med ca 75 % av de biträden som anlitas av bolaget. Det saknas således avtal med ca 25 % av anlitade biträden. Med hänsyn till att det är ett krav att reglera hanteringen av personuppgiftsuppgifter med biträdet rekommenderas bolaget att se över för vilka biträden avtal saknas och säkerställa att sådana upprättas.

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 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 informerats om att bolaget regelbundet arbetar med att följa upp behandlingsregistret. I arbetet försöker den interna dataskyddsorganisationen även att styra ut ansvaret på utsedda kontaktpersoner där

dataskyddskontakterna även kontinuerligt skickar ut påminnelser om att uppdatera behandlingsregistret. Dataskyddsombudet ser det som mycket positivt att verksamheten har rutiner och arbetssätt på plats i syfte att regelbundet uppdatera behandlingsregistret. Med beaktande av att bolaget uppger att ca 75 % av alla behandlingar finns upptagna i behandlingsregistret och att ca 75 % av den information som krävs finns med rekommenderar dataskyddsombudet att bolaget fortsätter arbetet med behandlingsregistret. Detta för att säkerställa att alla personuppgiftsbehandlingar tas upp i behandlingsregistret och att det innehåller all den informations som krävs enligt art. 30 i GDPR.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

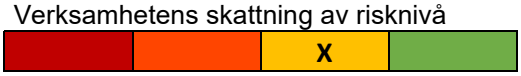
Dataskyddsombudets bedömning

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

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

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att 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 utbildningsnivån särskilt.

Bolaget uppger att det har skett förbättringar avseende att medarbetare regelbundet ges möjlighet att delta i utbildningar inom dataskydd och att det sker

behovsanpassad utbildnings- och informationsinsatser utifrån medarbetarnas befattning. Dataskyddsombudet ser det som positivt och rekommenderar bolaget att fortsätta säkerställa att medarbetare ges möjlighet till utbildning. Samtidigt noterar dataskyddsombudet, vid en jämförelse med skattningen år 2022, att skattningen är lägre avseende att verksamheten regelbundet genomför informationsinsatser för att utbilda och informera medarbetare inom dataskydd. I samband med genomgången av årsrapporten uppgav verksamheten att det har identifierats ett behov internt avseende att gå ut med mer information på APT:er. Dataskyddsombudet gör bedömningen att det är positivt att bolaget har identifierat behovet då det ger bolaget goda förutsättningar att arbeta med frågan.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

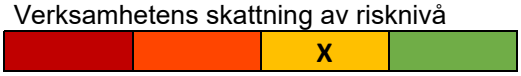
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, med gör till skillnad ifrån verksamheten bedömningen att det förekommer risker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

I årsrapporten 2022 lyfte dataskyddsombudet att en ordentlig översyn av informationsplikten som helhet bör genomföras kontinuerligt. Efter att ha kontrollerat bolagets nuvarande information på hemsidan och utifrån bolagets egen skattning gör dataskyddsombudet bedömningen att bolaget behöver utveckla informationen ytterligare för att uppfylla kraven enligt art. 13 och 14 i GDPR. Bolaget rekommenderas framåt att bland annat förtydliga vilka som är mottagare av personuppgifter vid olika behandlingar, vilka tredjelandsöverföringar som sker samt undvika att hänvisa till dokumenthanteringsplanen. Sammantaget bedömer dataskyddsombudet att den tidigare lämnade rekommendationen om att göra en översyn av hur informationsplikten hanteras som helhet kvarstår även för 2024.

Utifrån skattningen och dialogen vid genomgången av årsrapporten gör dataskyddsombudet bedömningen att det finns en medvetenhet inom bolaget avseende informationsplikten, varför dataskyddsombudet ser att det finns goda förutsättningar för bolaget att arbeta med kontrollpunkten.

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 inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat bolagets e-post och dokumenthantering särskilt.

Utifrån skattningen kan dock dataskyddsombudet utläsa att bolaget har en aktuell och fastställd dokumenthanteringsplan som omfattar samtliga av verksamhetens processer, vilket är en avsevärd förbättring jämfört med år 2022. Dataskyddsombudet ser det som positivt. Bolaget behöver dock säkerställa att gallring sker enligt dokumenthanteringsplanen. För ändamålet rekommenderas bolaget att ta fram dokumenterade arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut. Vidare rekommenderas bolaget att ta fram dokumenterade arbetssätt för att informera medarbetare om dokumenthantering samt gallring kopplat till kraven enligt GDPR (lagringsminimering).

Bolaget anger att ca 75 % av personuppgiftsbehandlingarna har informationsklassificerats och att ca 75 % av klassningarna är aktuell. I likhet med årsrapporten 2022 rekommenderas bolaget att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

Bolaget behöver också säkerställa att de registrerade, direkt vid upprättad kontakt med verksamheten, får information om hur deras personuppgifter hanteras. Bolaget rekommenderas exempelvis att se över möjligheten att i e-postsignatur infoga en länk till integritetsinformationen.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Vid en jämförelse med skattningen år 2022 kan dataskyddsombudet utläsa att bolaget har tagit fram dokumenterade arbetssätt för att uppdatera befintliga konsekvensbedömningar vid förändringar i ursprungsbehandlingarna och för att kunna inhämta de registrerades synpunkter. Dataskyddsombudet ser det som positivt.

Under året har dataskyddsombudet involverats i arbetet med fyra konsekvensbedömningar och några tröskelanalyser vilket dataskyddsombudet ser som mycket positivt. Bolaget uppmuntras att även framåt involvera dataskyddsombudet. Vidare bedömer dataskyddsombudet, utifrån de konsekvensbedömningar och tröskelanalyser som dataskyddsombudets har involverats i, att flertalet av dessa har varit välskrivna.

Bolaget uppger samtidigt att endast 25 % av bolaget personuppgiftsbehandlingar har kontrollerats utifrån höga risker, vilket är lägre jämfört med år 2022 då andelen uppgavs vara 50 %. Inför årsrapporten 2022 uppgav bolaget att det fanns en planering för genomförande av konsekvensbedömningar för ca 50 % av de personuppgiftsbehandlingar där sådana krävdes, men anger i år att det inte finns en planering för genomförandet av konsekvensbedömningar framåt. I samband med genomgången av årsrapporten uppger verksamheten att det pågår ett arbete med att bygga upp organisationen kring ansvar kopplat till konsekvensbedömningsarbetet och att det därför inte finns en planeringering framåt.

Dataskyddsombudet ser det som positivt att bolaget arbetar med att se över ansvaret kopplat till konsekvensbedömningar och uppmuntrar bolaget att fortsätta arbetet. Bolaget uppskattar dock att det endast är ca 25 % av samtliga personuppgiftsbehandlingar som kräver en konsekvensbedömning som det finns en framtagen och fastställd konsekvensbedömning. Bolaget rekommenderas därför att gå igenom sina personuppgiftsbehandlingar och genomföra riskbedömningar för samtliga. Därefter rekommenderas bolaget att göra en långsiktig planering och prioritering för genomförandet av konsekvensbedömningar för behandlingar där sådana krävs.

Eftersom bolaget har skattat sig lågt på påståendet om att verksamheten har dokumenterade arbetssätt för att bedöma riskerna för de registrerade inom ramen för en personuppgiftsbehandling rekommenderas bolaget att se över om det finns arbetssätt för detta. För det fall det saknas rekommenderas bolaget att ta fram det då bedömning av risker för registrerade utgör en grundläggande del i arbetet med konsekvensbedömningar.

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 endast involverats i några enstaka frågor kopplat till kontrollpunkten, men delar verksamhetens bedömning att det föreligger risker som behöver åtgärdas.

Under året har dataskyddsombudet involverats i samband med arbetet avseende migrering av data till nytt lönesystem. Dataskyddsombudet involverades dock sent i projektet vilket resulterade i att dataskyddsperspektivet inte kunde säkerställas fullt ut. Baserat på arbetet med projektet är dataskyddsombudets bedömning att bolaget behöver säkerställa att det finns dokumenterade arbetssätt för att involvera dataskyddsombudet från start vid nya IT-projekt och införande av nya tjänster.

Utifrån bolaget skattning kan dataskyddsombudet utläsa att det finns ett behov av att säkerställa att det vid upphandling av nya system/tjänster tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. För att säkerställa att dataskyddsperspektivet tas med i alla delar av processen vid upphandlingar rekommenderas bolaget att se över om ytterligare resurser eller kompetens behöver involveras och/eller om särskilda informations- och/eller utbildningsinsatser krävs.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet har noterat att bolaget använder flera sociala medier som kommunikationskanaler. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Under 2022 uppgav bolaget att det pågick en koncerngemensam översyn av användningen av sociala medier. I samband med översynen rekommenderas bolaget att bland annat kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna. 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.

Vidare delar dataskyddsombudet inte bolagets bedömning vad gäller användningen cookies. Bolaget behöver bland annat säkerställa att informationsplikten uppfylls vid användning av cookies. Informationen som lämnas behöver vara specifik, tydlig och fullständig och användaren ska ges förutsättningar för att förstå konsekvenserna av sitt samtycke. Bolaget behöver bland annat informera om vem som lagrar eller hämtar cookies, giltighetstid för cookies och om informationen delas med någon annan part. Dessutom ska information lämnas om användares rätt att när som helst återkalla ett samtycke till icke-nödvändiga kakor i samband med

och i samma vy som samtycke inhämtas. Utifrån detta rekommenderas bolaget prioritera arbetet med att se över informationen om cookies och att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl dataskyddsförordningen som LEK (lagen (2022:482) om elektronisk kommunikation).

Utifrån iakttagelser under året, särskilt i samband med arbete med konsekvensbedömningar, bedömer dataskyddsombudet att verksamheten bedriver ett gott arbete avseende behörighetsstyrning och att informera medarbetare om hur verksamhetenssystem ska användas. Bolaget rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen 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 risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

Utifrån verksamhetens svar kan dataskyddsombudet utläsa att det finns en bredare medvetenhet bland medarbetare om vilka rättigheter de registrerade har jämfört med 2022, vilket dataskyddsombudet ser som positivt.

Dataskyddsombudet kan dock även utläsa att det föreligger risker kopplat till att bolaget skattar sig lågt på om det finns dokumenterade arbetssätt för att hantera ett tillbakadragande av samtycke från registrerade. Avsaknaden av rutiner eller låg kunskap om befintlig rutin bland medarbetare 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 riskerar därmed att behandla personuppgifterna olagligt.

Bolaget rekommenderas att se över om det finns en rutin för att hantera situationen då ett samtycke från en registrerad dras tillbaka och säkerställa att rutinen är förankrad inom bolaget. Om det saknas rekommenderas bolaget att ta fram en sådan.

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): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Se över den generella lagringstiden ytterligare för att säkerställa att den verkligen är befogad i förhållande till ändamålen och omständigheterna kring hur lång tid det tar att upptäcka och hantera en incident.
- I samband med översynen av utförda konsekvensbedömningar, inhämta dataskyddsombudets rekommendationer.
- Förtydliga informationen om lagringstid på hemsidan.

Kommentarer och rekommendationer:

Bolaget uppger i samband med uppföljningen att bolaget har sett över och dokumenterat behovet av lagringstid för de olika placeringarna av kameror. Informationen om lagringstid för de olika placeringarna har uppdaterats på hemsidan. Vidare uppger bolaget att en särskild resurs har tillsats. Resursen har ett utpekat ansvar att hantera och administrera processen för kamerabevakning, vilket bedöms ge en kvalitetssäkring. Bolaget bedömer även att den utsedda resursen kan leda verksamheten genom de olika stegen och säkerställa att konsekvensbedömning utförs där det behövs, samt att dataskyddsombudets rekommendationer inhämtas framåt.

Uppföljningen visar att verksamheten har vidtagit flera åtgärder. Dataskyddsombudet ser det som mycket positivt att bolaget har tillsatt en särskild resurs för att hantera kamerabevakningen och att det görs en översyn av konsekvensbedömningar. Bolaget rekommenderas att fortsätta arbetet under 2024. Dataskyddsombudet avser att fortsätta följa upp arbetet med översynen av konsekvensbedömningar under 2024.

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

Fortsätt arbeta med att dokumentera bolagets personuppgiftsbehandlingar och kontrollera för respektive behandling att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

- Fördjupad kontroll: Kamerabevakning

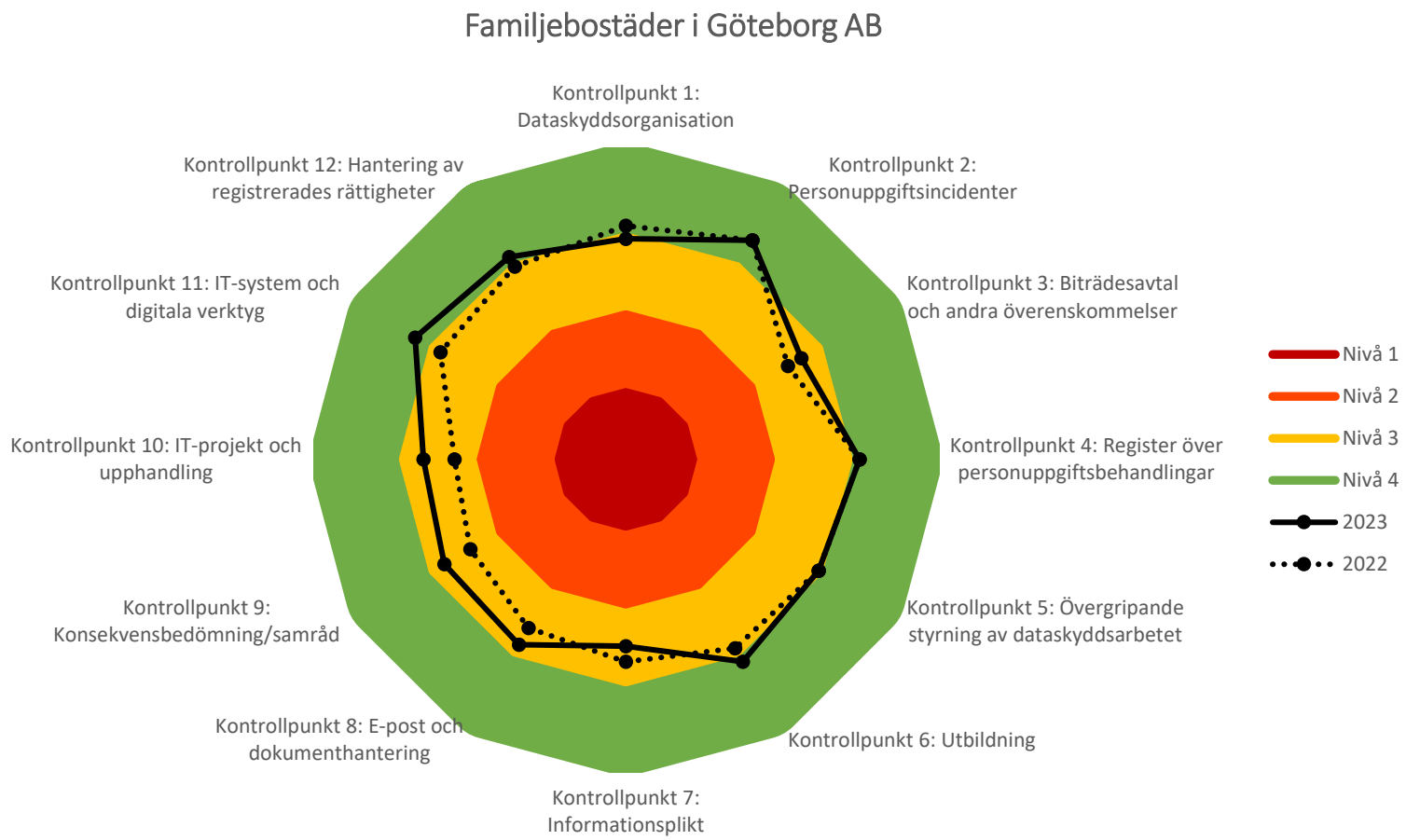
Gör en översyn av konsekvensbedömningar kopplat till kamerabevakning. Inhämta dataskyddsombudets råd och rekommendationer för de konsekvensbedömningar där dataskyddsombudets rekommendationer saknas.

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

Familjebostäder i Göteborg AB

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera personuppgifter.

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

1.1 Ny utformning av kontrollarbetet

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

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

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

2 Kontrollarbetet 2023–2024

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

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

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

2.1 Kontrollarbetets delar

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

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

2.2 Tidplan för kontrollarbetet 2023–2024

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

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

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

3 Kontroller

3.1 Fasta kontrollpunkter

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

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

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

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

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

3.2 Fördjupad kontroll

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

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

3.3 Uppföljning av genomförda kontroller

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

4 Rapportering

4.1 Årsrapport

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

4.2 Särskilt yttrande

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

5 Kontakt

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

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

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

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

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras person-uppgifter 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.