Styrelsehandling nr 11
Datum 2024-05-07
Diarienummer BOS-2024-00338

Handläggare
Sara Fischer
Telefon: 031-731 50 10
E-post: sara.fischer@bostadsbolaget.se

Årsrapport för dataskyddsarbetet 2023

Informationsärende

Styrelsen Göteborgs stads bostadsaktiebolag föreslås

Årsrapport för Bostadsbolagets dataskyddsarbete antecknas.

Sammanfattning

Varje år genomför dataskyddsenheten på Intraservice en kontroll över bolagets dataskyddarbete. Kontrollen för år 2023 består av ett antal fasta kontrollpunkter samt uppföljning av tidigare fördjupad kontroll. Uppföljningen avseende fördjupade kontrollen 2023 omfattade kamerabevakning (CCTV). I årsrapporten presenteras resultat av kontrollen för 2023 och rekommendationer om hur bolaget ska förbättra arbetet med dataskydd enligt Dataskyddsförordningen (GDPR) samt resultatet av uppföljningen avseende inom kamerabevakning.

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte bedömts vara föremål för samverkan.

Bilagor

1. Årsrapport för dataskyddsarbetet 2023

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Göteborgs Stads Bostads 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.

Utifrån iakttagelser under året är dataskyddsombudets bedömning att bolaget har en god struktur för den interna dataskyddsorganisationen. Det är positivt att den interna dataskyddsorganisationen består av representanter från olika delar inom verksamheten och att dataskyddskontakten har en ledande och samordnande funktion. Samtidigt har dataskyddsombudet fått indikationer på att dataskyddsarbetet inte bedrivs i samma utsträckning när dataskyddskontakten är frånvarande, vilket indikerar att dataskyddsarbetet till viss del är personberoende och därmed sårbart. Framåt rekommenderas bolaget fortsätta utveckla och stödja det goda arbete som bedrivs, samt ge den interna dataskyddsorganisationen möjlighet att se över vilka resurser, vilken kompetens och vilka insatser som krävs för att undvika personberoende och för att kunna säkerställa dataskyddsperspektivet fullt ut.

Under året har dataskyddsombudet haft några avstämningsmöten 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 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 har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån.

Dataskyddsombudet ser det som positivt att bolaget har flera dokumenterade arbetssätt på plats under kontrollpunkten. Mot bakgrund av att bolaget under kontrollpunkt 6 har skattat sig lågt på frågan om den allmänna kunskapsnivån kan det föreligga risker kopplat till medarbetares förutsättningar att identifiera när en personuppgiftsincident inträffar.

Även om bolaget har fungerande arbetssätt för att omhänderta de incidenter som den interna dataskyddsorganisationen får kännedom om kan bristande kunskap om dataskydd bland medarbetare innebära att personuppgiftsincidenter inte upptäcks eller identifieras. Utifrån ovan rekommenderas bolaget att utvärdera om den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att identifiera personuppgiftsincidenter.

Under året har dataskyddsombudet informerats om att bolaget arbetar utifrån ett årshjul. I årshjulet ingår bland annat att informera medarbetare om hanteringen av personuppgiftsincidenter under APT:er, vilket dataskyddsombudet ser som positivt.

Utifrån verksamhetens skattning kvarstår behovet av att säkerställa att det finns rutiner för när och hur information till registrerade ska tillhandahållas vid en incident samt att systematiskt följa upp incidenter. Vid genomgång av årsrapporten informerades dataskyddsombudet om att det finns rutiner på plats, men att den låga skattningen beror på att rutinerna inte finns nedtecknade skriftligen eller att det finns osäkerhet kring hur väl implementerade rutinerna är i hela verksamheten. Bolaget rekommenderas att se över om det finns skriftliga rutiner på plats. Om det saknas rekommenderas bolaget framåt dokumentera befintliga rutiner samt säkerställa att rutinerna förankras inom verksamheten.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

		X	

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

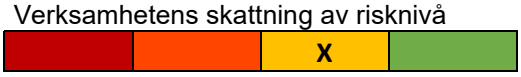
Även i år uppskattar bolaget att det finns tecknade biträdesavtal med ca 75 % av biträdena, vilket innebär att avtal saknas med ca 25 %. Under genomgången av årsrapporten lyfte verksamheten att en kartläggning har gjorts under året. Verksamheten uppger att det främst är leverantörer som har upphandlats på koncernnivå som biträdesavtal saknas. Bolaget rekommenderas att fortsätta arbetet med att upprätta och teckna avtal med de biträden där avtal saknas.

I likhet med förgående år identifierar verksamheten att det finns ett behov av att ta fram dokumenterade arbetssätt för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden samt att bedöma om det finns ett gemensamt personuppgiftsansvar när en leverantör anlitas eller när samarbeten sker. Rekommendationerna från årsrapporten 2022 kvarstår därmed i dessa delar.

Under genomgången av årsrapporten uppger verksamheten att det har inletts ett internt samarbete med inköpsdelen för att se över hur efterlevnadskontroller av personuppgiftsbiträden kan genomföras framåt, vilket dataskyddsombudet ser som positivt.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten. Utifrån verksamhetens skattning gör dock dataskyddsombudet bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och som kräver åtgärder.

Verksamheten anger, i likhet med år 2022, att ca 50 % av bolagets behandlingar finns registrerade i behandlingsregistret och att ca 50 % av dessa innehåller all den information som ska finnas med enligt art. 30 i GDPR. Med hänsyn till att det är ett krav att ha ett fullständigt behandlingsregister rekommenderas bolaget att komplettera registret med de behandlingar som saknas samt att säkerställa att registret innehåller all den information som krävs. Även om bolaget har dokumenterade arbetssätt för att hålla registret uppdaterat och en tydlig ansvarsfördelning för uppgiften på plats är det viktigt att säkerställa att de dokumenterade arbetssätten får genomslag i praktiken. Dataskyddsombudet rekommenderar att bolaget prioriterar arbetet med behandlingsregistret under år 2024.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

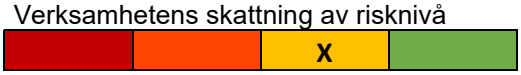
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året endast involverats i några enstaka frågor kopplat till kontrollpunkten, men har ingen anledning att göra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

På påståendet om bolaget har en övergripande strategi för arbetet med dataskydd och att verksamheten arbetar systematiskt med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet svarar verksamheten ”nej, stämmer inte bra”. Dataskyddsombudet kan även utläsa att det finns ett utvecklingsbehov avseende att anta ett riskbaserat arbetssätt i dataskyddsfrågor. Under året har verksamheten informerat dataskyddsombudet om att verksamheten har arbetat aktivt för att få de grundläggande bitarna för dataskyddsarbetet på plats. Arbetet har bland annat bestått i att sätta ramarna och strukturen kring den interna dataskyddsorganisationen. Det har även pågått ett aktivt arbete med att uppmärksamma dataskyddsfrågor inom bolagets olika verksamhetsområden. Dataskyddsombudet ser det som positivt eftersom det utgör grundläggande förutsättningar för att kunna bedriva ett systematiskt dataskyddsarbete. Bolaget rekommenderas att framåt se över vilka delar av den övergripande strategin för arbetet med dataskydd som behöver utvecklas.

Även om det utifrån skattning kan utläsas att det finns utvecklingsbehov avseende dokumenterade arbetssätt för att efterleva kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster rekommenderas bolaget att i första hand fortsätta prioritera arbetet med att säkerställa att det finns en tydlig och strukturerad styrning av dataskyddsfrågor samt att säkerställa att dataskyddsfrågorna integreras i det övriga 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 under året endast involverats i någon enstaka fråga kopplat till kontrollpunkten och har ingen anledning att göra en annan bedömning än den som verksamheten gör avseende risknivån.

Utifrån verksamhetens egen skattning bedömer dataskyddsombudet att den största risken som föreligger inom kontrollpunkten är kopplad till den allmänna kunskapsnivån inom verksamheten. En förutsättning för ett fungerande dataskyddsarbete är att medarbetare, utifrån sin roll och sina arbetsuppgifter, har tillräckliga kunskaper inom dataskydd. Bristande kunskap bland medarbetare kan få flera konsekvenser, bland annat kan det leda till att personuppgiftsincidenter inte identifieras eller att personuppgifter inte hanteras korrekt.

För att säkerställa att resurser sätts in där det främst behövs rekommenderas bolaget att kartlägga vilken nivå av dataskyddskunskaper som olika befattningar behöver ha. Bolaget rekommenderas därefter att ta fram en långsiktig utbildningsplan och utbilda medarbetare efter identifierade behov.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet noterar att bolaget har en omfattande och strukturerad integritetsinformation på hemsidan, vilket är positivt. Under året har dataskyddsombudet även fått information om att integritetsinformationen har setts över. I årsrapporten 2022 lyfte dataskyddsombudet att det fanns skäl att förbättra bolagets arbete med informationsplikten. Exempel på hur detta skulle kunna göras, till exempel vilken information som behöver förtydligas, lämnades i årsrapporten. Efter en kontroll av bolagets nuvarande information på hemsidan gör dataskyddsombudet bedömningen att informationen behöver utvecklas ytterligare för att uppfylla kraven i art. 13 och 14 i GDPR. Exempelvis är det inte tydligt vilken rättslig grund som vissa behandlingar stödjer sig på. Även om lagringstiden tydlig framgår för vissa behandlingar, saknas det för andra. Bolaget rekommenderas även att undvika att hänvisa till dokumenthanteringsplanen i integritetsinformationen.

Sammantaget bedömer dataskyddsombudet att bolaget behöver göra en översyn av hur informationsplikten hanteras som helhet, i detta arbete är integritetsinformationen på hemsidan en del. Bolaget rekommenderas att framåt säkerställa att de rekommendationer som lämnades i årsrapporten 2022 kopplat till den specifika informationen på hemsidan omhändertas.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

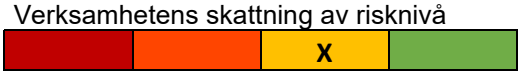
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning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

Vid en jämförelse med skattningen inför årsrapporten 2022 noterar dataskyddsombudet att bolaget har arbetat vidare med att informationsklassificera sina personuppgiftsbehandlingar, vilket är positivt. I övrigt är skattningen samma

som inför årsrapporten 2022. Verksamheten har skattat sig lågt på påståendena om verksamheten har dokumenterade arbetssätt för att kontrollera att handlingar gallras enligt gällande gallringsbeslut, för att informera medarbetare om dokumenthantering och gallring kopplat till kraven enligt GDPR samt för hur personuppgifter får hanteras i e-post. I samband med genomgången av årsrapporten förtydligar verksamheten att rutiner och arbetsprocesser i dessa delar finns framtagna inom bolaget, men att den låga skattningen i vissa fall beror på att det inte finns skriftligen eller att de finns osäkerheter kring hur väl implementerade rutinerna/arbetssätten är i verksamheten. Bolaget rekommenderas därför att fortsätta att arbeta för att arbetssätten förankras internt. I de fall arbetssätten inte finns skriftligen, rekommenderas bolaget att säkerställa att rutinerna/arbetssätten dokumenteras.

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 från verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och som kräver åtgärder.

Utifrån resultatet kan dataskyddsombudet utläsa att det har skett förbättringar under kontrollpunkten jämfört med år 2022. Bolaget skattar sig högre avseende att det finns dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas och att det finns dokumenterade arbetssätt för att uppdatera befintliga konsekvensbedömningar vid förändringar i ursprungsbehandlingen.

I likhet med förgående år uppger bolaget att endast 25 % av personuppgiftsbehandlingarna har kontrollerats utifrån höga risker. Vid genomgången av årsrapporten förtydligade bolaget att samtliga personuppgiftsbehandlingar som den interna dataskyddsorganisationen känner till har riskbedömts. Andelen som uppgavs i svaret baseras på att frågan är besvarad utifrån hur stor andel av behandlingarna som har bedömts genom så kallade tröskelanalyser. Bolaget uppgav även att det finns en bra arbetsgång för riskbedömningar av personuppgiftsbehandlingar.

Utifrån skattningen kan dataskyddsombudet utläsa att det finns en planering för genomförandet av konsekvensbedömningar för ca 50 % av bolagets personuppgiftsbehandlingar där en sådan krävs. Mot bakgrund av att bolaget inte har några genomförda och fastställda konsekvensbedömningar rekommenderas bolaget att säkerställa att det finns en långsiktigt plan och prioritering för genomförandet av konsekvensbedömningar för behandlingar där en sådan krävs.

Bolaget uppgav även i samband med genomgången av årsrapporten att det pågår arbeten med konsekvensbedömningar inom bolaget, vilket dataskyddsombudet ser som positivt. Bolaget rekommenderas att framåt säkerställa att dessa konsekvensbedömningar blir genomförda.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

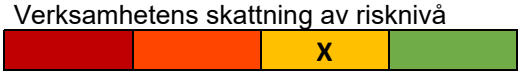
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året involverats i några enstaka frågor kopplat till kontrollpunkten och har ingen anledning att göra en annan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

Utifrån bolagets egen skattning framgår det att förbättringar har skett avseende att det finns dokumenterade arbetssätt för att genomföra en risk-/behovsanalys vid initierande av nya digitala lösningar. I övrigt har bolaget skattat sig som förgående år. Utifrån iakttagelser under året ser dataskyddsombudet att det är positivt att bolaget har involverat dataskyddsombudet i högre utsträckning jämfört med tidigare. Bolaget uppmuntras även att fortsättningsvis involvera dataskyddsombudet i ett tidigt skede vid uppstart av IT-projekt och upphandlingar.

Utifrån bolagets skattning kan dataskyddsombudet utläsa att det fortsatt 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 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.

Avseende bolagets kommunikationskanaler noterar dataskyddsombudet att bolaget använder sociala medier. Trots att förutsättningarna för överföringar till

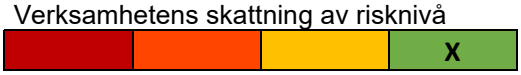
amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Under 2022 uppgav bolaget att det pågick en koncerngemensam översyn av användningen av sociala medier. I samband med översynen rekommenderas bolaget att bland annat kartlägga vilka behandlingar 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.

Av bolagets cookie-information på hemsidan framgår att bolaget endast använder nödvändiga cookies för hemsidans funktionalitet. Efter genomgången av årsrapporten har dock verksamheten förtydligat att även icke-nödvändiga cookies används på bolagets hemsida. Mot bakgrund av att icke-nödvändiga cookies används och att det finns krav på att inhämta giltiga samtycken för sådan cookie-användning rekommenderas bolaget att se över sin cookie-hantering. Bolaget behöver dels säkerställa att cookiebannern uppfyller kraven för ett giltigt samtycke enligt GDPR (eller best practice), dels säkerställa att informationsplikten kopplat till cookies uppfylls. Utifrån detta rekommenderas bolaget prioritera arbetet med att se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl GDPR som LEK (lagen (2022:482) om elektronisk kommunikation).

Utifrån bolagets skattning kan dataskyddsombudet utläsa att det fortsatt finns ett behov av att upprätta dokumenterade arbetssätt för att följa upp och kontroller så att IT-system och digitala verktyg används på rätt sätt. Bolaget har även ett behov av att ta fram dokumenterade arbetssätt för att säkerställa att dataskyddsperspektivet beaktas vid införandet och användandet av kostnadsfria tjänster, såsom gratisappar och sociala medier.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

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

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Förtydliga bedömningen kring varför bevakningen inte är tillståndspliktig i bolagets underlag.
- 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.
- Förtydliga informationen om lagringstid på hemsidan.

Kommentarer och rekommendationer:

I uppföljningen av den fördjupade kontrollen uppger bolaget att det har förtydligats varför bevakningen inte är tillståndspliktig i bolagets underlag. Underlaget har bland annat kompletterats med hänvisning till paragrafer i kamerabevakningslagen.

Vidare framgår det att bolaget har sett över och dokumenterat behovet av lagringstid i förhållande till ändamålet samt uppdaterat information om lagringstid på hemsidan. Enligt bolaget framgår det numera tydligt hur länge materialet sparas.

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med rekommendationerna. Fortsatt uppföljning kommer att ske inom ramen för den löpande dialogen som dataskyddsombudet har med bolaget om ingen särskilt föranleder att det behöver följas upp separat.

4 Rekommenderade fokusområden 2024

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

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

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Komplettera behandlingsregistret med personuppgiftsbehandlingar som saknas och den information som krävs enligt artikel 30 i GDPR.

- Kontrollpunkt 9: Konsekvensbedömningar

Säkerställ att det finns en långsiktigt plan och prioritering för genomförandet av konsekvensbedömningar för behandlingar där en sådan krävs. Bolaget rekommenderas att framåt säkerställa att konsekvensbedömningar genomförs i praktiken.

- Kontrollpunkt 11: IT-system och digitala verktyg

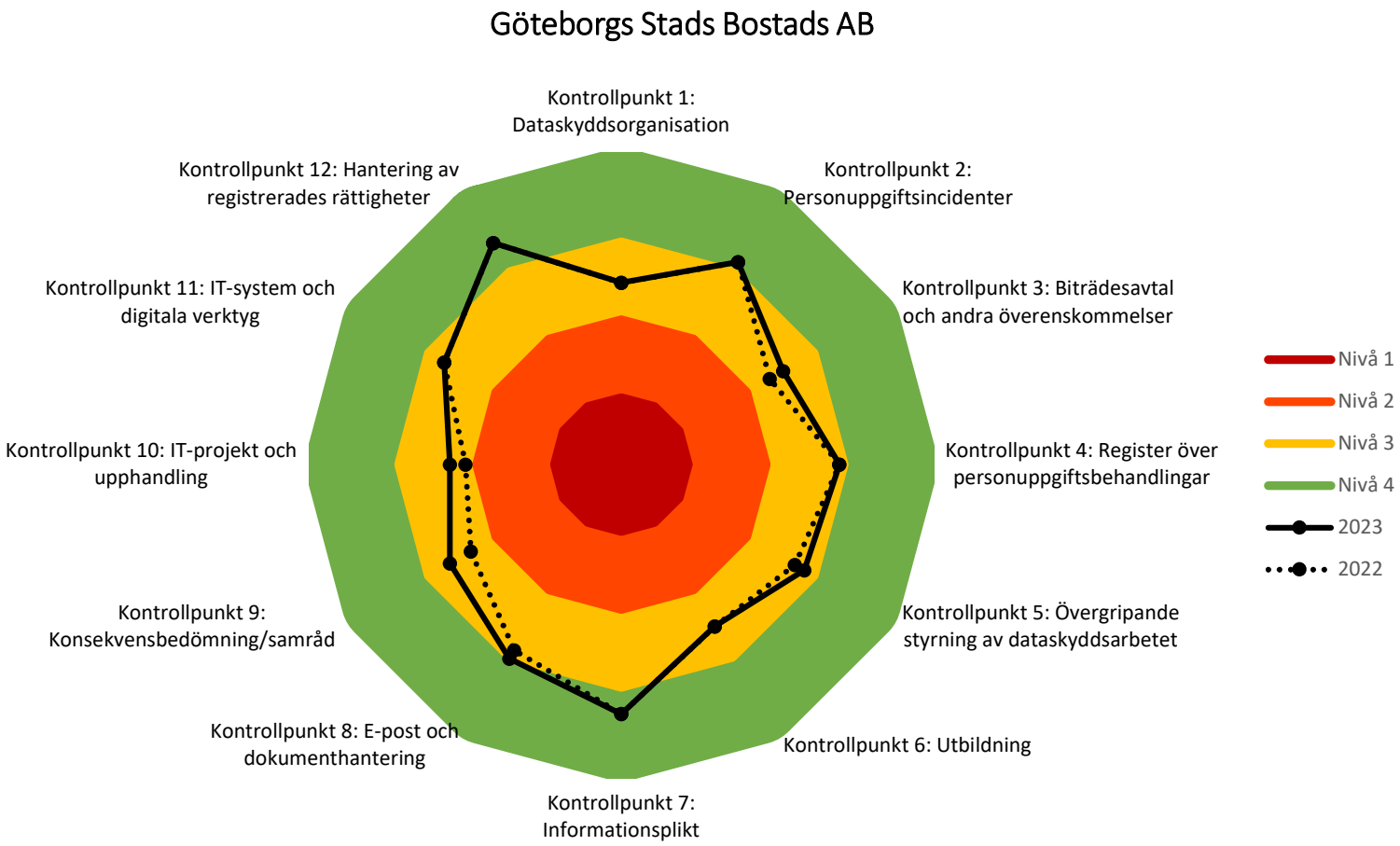
Se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl GDPR som LEK (lagen (2022:482) om elektronisk kommunikation).

5 Bilagor

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

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

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



Göteborgs Stad

Göteborgs Bostads AB (Bostadsbolaget)

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.