Tjänsteutlåtande
Styrelsen 2024-01-22
Ärendenummer GSHAB-2023-00014

Handläggare: Karin Lange, administrativ chef
Telefon: 031 – 368 54 59
E-post: karin.lange@gshab.goteborg.se

Dataskyddsenhetens årsrapport för dataskyddsarbetet 2023

Förslag till beslut

I styrelsen för Göteborgs Stadshus AB:

Information avseende dataskyddsenhetens årsrapport för dataskyddsarbetet 2023 enligt bilaga 1 till tjänsteutlåtandet antecknas.

Ärendet

Ärendet avser anmälan till styrelsen av dataskyddsenhetens årsrapport för datasskyddsarbetet 2023 för Göteborg Stadshus AB.

Det är stadens nämnder och styrelser som har det yttersta ansvaret för att dess verksamhet följer dataskyddslagstiftningen. Dataskyddsenheten är dataskyddsombud för verksamheterna i Göteborgs Stad och lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad.

Dataskyddsenheten har från och med 2023 en ny utformning av kontrollarbetet som framgent kommer löpa över tvåårsperioder. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan 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. Göteborg Stadshus AB (Stadshus) och kommunstyrelsen har samma huvudansvariga dataskyddsombud och bolaget samverkar med stadsledningskontoret i sitt dataskyddsarbete.

Kontrollarbetet under 2023 för Stadshus har resulterat i bilagda årsrapport vilken innehåller resultatet från de fasta kontrollpunkterna, resultat från uppföljning av tidigare kontroller samt rekommendation om två fokusområden för 2024.

Stadshus kommer i sitt fortsatta dataskyddsarbete beakta det som dataskyddsombudet lyft i sin granskning.

Styrelsen föreslås att anteckna årsrapporten.

Bedömning ur ekonomisk, ekologisk och social dimension

Ärendet avser anmälan av den årsrapport som dataskyddsenheten lämnat. Bolaget har inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Bilaga

1. Dataskyddsenhetens årsrapport för dataskyddsarbetet 2023

Eva Hessman

Vd, Göteborgs Stadshus AB

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Göteborgs Stadshus AB

2023-12-18

Innehåll

1 Inledning

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

1.1 Dataskyddsombud i Göteborgs Stad

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

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

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

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

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

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

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

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

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

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

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

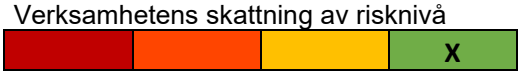
3.2 Resultat från kontrollen 2023

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

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

Den interna dataskyddsorganisationen utgör grunden för att bolaget ska kunna bedriva ett systematiskt dataskyddsarbete på ett effektivt och ändamålsenligt sätt. En intern dataskyddsorganisation utgör även en förutsättning för efterlevnaden av dataskyddslagstiftningen. En dataskyddsorganisation som består av en eller ett mycket litet antal personer kan medföra sårbarhet. Det kan resultera i att dataskyddsarbetet inom bolaget blir personberoende. Det finns även risk för att den interna dataskyddsorganisationen inte hinner med alla de uppgifter som behöver göras. I årsrapporten 2022 rekommenderades bolaget att kontinuerligt utvärdera den interna organisationen med syftet att säkerställa att den har rätt förutsättningar för att bedriva ett effektivt dataskyddsarbete. Dataskyddsombudet kan utifrån bolagets svar 2023 utläsa att arbetet stärkts inom flera delar av kontrollpunkten, bland annat gällande beslutsmandat och rapporteringsvägar, samt omfattningen på resurser tillgängliga för den interna dataskyddsorganisationen.

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

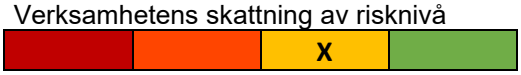
Den risk dataskyddsombudet identifierat lyftes även till bolaget i årsrapporten för 2022 och gäller det låga antal incidenter som bolaget dokumenterat. Som lyftes i årsrapporten 2022 är tröskeln för när en personuppgiftsincident har skett låg och personuppgiftsincidenter kommer ofrånkomligen att inträffa även i organisationer

som har mycket väl utvecklade rutiner för att förhindra att personuppgiftsincidenter sker.

Dataskyddsombudet genomförde 2022 en fördjupad kontroll av incidenthanteringen och lämnade utifrån denna ett antal rekommendationer till bolaget. Uppföljningen av dessa rekommendationer lämnas under avsnitt 3.3.1 i årsrapporten. Förbättringsåtgärder utifrån verksamhetens svar och som dataskyddsombudet identifierat inom ramen för kontrollpunkten gäller bland annat att stärka medarbetarnas kunskaper om personuppgiftsincidenter genom att systematiskt följa upp inträffade personuppgiftsincidenter i förebyggande syfte.

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. Bolagets skattning på frågorna inom denna punkt ger ett lägre resultat än tidigare år. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat hanteringen särskilt.

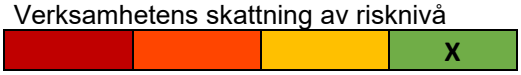
De risker som identifierats utifrån bolagets skattning gäller genomförande av efterlevnadskontroller, samt avsaknaden av dokumenterade arbetssätt och kompetens för att bedöma hela kedjan av underbiträden vid anlitande av ett nytt personuppgiftsbiträde. Gällande bedömning av underbiträden anger bolaget i år ett lägre värde på frågan än 2022. Utifrån det ansvar bolaget har vid anlitande av biträden enligt artikel 28 i GDPR, den så kallade ”omsorgsplikten”, föreligger här en risk för att verksamheten inte kan uppfylla kraven enligt GDPR.

Bolaget anger också ett lägre värde för hur stor andel personuppgiftsbiträden som verksamheten uppskattningsvis har tecknat personuppgiftsbiträdesavtal med, samt gällande rutiner för att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam/annan delad hantering av personuppgifter när en leverantör anlitas eller när samarbeten sker.

Bolaget rekommenderas se över nuvarande hantering för att kunna bedöma vilka åtgärder som behöver vidtas för att hantera riskerna.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

I svaren anger bolaget att samtliga av bolagets personuppgiftsbehandlingar finns med i behandlingsregistret, och att större delen av dessa behandlingar innehåller den information som ska finnas med enligt artikel 30 i GDPR.

Dataskyddsombudet genomförde 2021 en fördjupad kontroll av behandlingsregistret och lämnade utifrån denna ett antal rekommendationer till bolaget. Uppföljningen av dessa rekommendationer lämnas under avsnitt 3.3.1 i årsrapporten och av denna framgår att bolaget har påbörjat arbetet med att omhänderta rekommendationerna, men att det fortfarande kvarstår delar som behöver åtgärdas kopplat till informationen i behandlingsregistret.

Bolaget rekommenderas därför att komplettera behandlingarna i registret med den information som saknas samt, som en del i detta arbete, säkerställa att (om bolaget väljer att ange rättslig grund) enbart en rättslig grund finns angiven per behandling.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

			X

Dataskyddsombudets bedömning

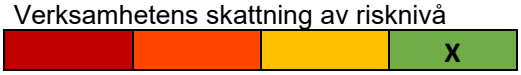
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten.

Dataskyddsombudet kan utifrån bolagets skattning utläsa att bolaget under året omhändertagit den rekommendation som lämnades 2022 gällande att ta fram rutiner för att efterleva kraven enligt GDPR vid fysiska/digitala sammankomster.

Sammantaget indikerar bolagets svar att det inom verksamheten finns förutsättningar för att hantera frågorna, och bolaget har vid genomgången av årsrapporten uppgett att det skett ett arbete med styrande dokument under hösten. Bolaget rekommenderas att fortsatt arbeta för att bibehålla och stärka de förutsättningar som finns enligt skattningen.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



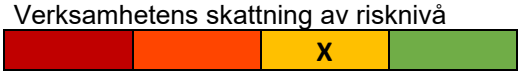
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning men kan, likt 2022, utifrån bolagets svar se att förbättringsmöjligheter finns.

Med syftet att stärka bolagets dataskyddsarbete ytterligare kvarstår rekommendationen från 2022 gällande att utvärdera utbildningsnivån hos medarbetare för att säkerställa att den är tillräcklig för att bedriva ett effektivt dataskyddsarbete.

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, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver åtgärder.

I årsrapporten 2022 bedömde dataskyddsombudet, utifrån de krav som ställs på personuppgiftsansvariga att tillhandahålla, konkret, enkel, exakt och tydlig information, att bolagets integritetspolicy inte uppfyllde kraven enligt artikel 13 och 14 i GDPR. Utifrån gjorda iakttagelser rekommenderades bolaget att kartlägga vilka behandlingar som skulle täckas in av policyn via hemsidan och komplettera policyn med den obligatoriska informationen som ska finnas med för dessa behandlingar. För de behandlingar som inte ska ingå i policyn rekommenderades bolaget säkerställa att information lämnades på annat sätt.

Efter kontroll av bolagets information under rubriken ”Så behandlar Göteborgs Stadshus AB personuppgifter” på hemsidan i november 2023 bedömer dataskyddsombudet att denna fortfarande inte uppfyller kraven enligt artikel 13 och 14 i GDPR. Dataskyddsombudet bedömer vidare att bolaget är medvetna om detta, vilket visas bland annat genom att bolagets svar på frågan om verksamhetens integritetsinformation uppfyller kraven i är ”Nej, stämmer inte bra” tillskillnad från 2022 då svaret var ”Ja, stämmer helt”.

Sammantaget bedömer dataskyddsombudet att bolaget behöver göra en översyn av hur informationsplikten hanteras som helhet. I detta arbete är informationen på

hemsidan en del, och bolaget rekommenderas framåt säkerställa att de rekommendationer som 2022 lämnades kopplat till den specifika informationen i integritetspolicyn omhändertas.

Under året har dataskyddsombudet utfört en informationsinsats om informationsplikten och tillhandahållit såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget kan med fördel använda sig av underlaget som stöd i arbetet med informationsplikten.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

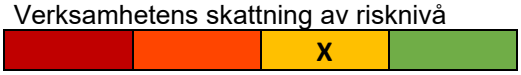
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan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

Skattningen visar att bolaget under året arbetat med frågor inom ramen för kontrollpunkten och till exempel anges att en fullständig dokumenthanteringsplan fastställts samt att det har dokumenterats hur personuppgifter får hanteras i e-post, särskilt med hänsyn till känsliga och särskilt skyddsvärda personuppgifter. Båda delarna är mycket positiva utifrån ett dataskyddsperspektiv. Bolagets skattning visar samtidigt att det inom kontrollpunkten föreligger vissa risker kopplat till att hålla informationsklassificeringen uppdaterad. Utifrån de risker som en oreglerad informationshantering innebär rekommenderas bolaget att framåt ta fram en planering för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

Eftersom principerna om lagring- och uppgiftsminimering är grundläggande i dataskyddsförordningen rekommenderar dataskyddsombudet, likt 2022, att bolaget kontinuerligt fortsätter informera medarbetare om dokumenthantering och gallring.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

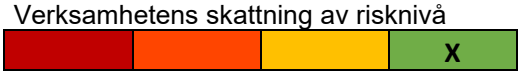
I årsrapporten för 2022 ifrågasatte dataskyddsombudet bolagets skattning gällande andelen genomförda och fastställda konsekvensbedömningar, utifrån att det angavs föreligga för majoriteten av bolagets behandlingar som krävde det. I årets skattning anger bolaget ett betydligt lägre värde både vad gäller andelen genomförda och fastställa konsekvensbedömningar, och för hur stor andel av bolagets personuppgiftsbehandlingar, som innebär en hög risk, det finns en dokumenterad planering för genomförandet av en konsekvensbedömning. Att bolagets svar avviker från tidigare år tyder på en ökad medvetenhet i frågan, vilket är positivt även om riskerna kvarstår. Bolaget behöver framåt omhänderta de rekommendationer som tidigare lämnats gällande att kartlägga vilka behandlingar som kräver en konsekvensbedömning och ta fram en plan för hur arbetet ska kunna genomföras.

Utöver det visar bolagets skattning även att bolaget behöver fortsätta arbeta med att riskbedöma verksamhetens behandlingar utifrån höga risker för de registrerades fri- och rättigheter, samt ta fram arbetssätt för att kunna inhämta de registrerades synpunkter på en behandling inom ramen för en konsekvensbedömning.

Under året har dataskyddsombudet involverats i bolagets arbete med tröskelanalyser och konsekvensbedömningar. De underlag som tagits fram har hållit god kvalitet, och dataskyddsombudet bedömer att bolaget har goda förutsättningar i det fortsatta arbetet inom ramen för kontrollpunkten.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

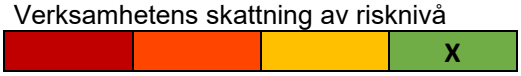
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

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

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

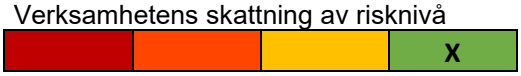
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten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

Bolaget rekommenderades i årsrapporten för 2022 att ta fram dokumenterade arbetssätt för att systematiskt kunna följa upp och kontrollera att användningen av system och/eller andra digitala verktyg följer antagna styrande dokument. Då bolagets skattning på frågan är fortsatt låg kvarstår rekommendationen för 2024.

Även vid årets genomgång av bolagets kommunikationskanaler noterar dataskyddsombudet att bolaget via Brysselkontoret använder sociala medier (Facebook, LinkedIn). Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget rekommenderas bland annat att kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder mellan bolaget och sociala medieplattformarna 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. Dataskyddsombudet uppfattning är att det inte går att utesluta att användningen av sociala medier sannolikt kan leda till en hög risk för de registrerades fri- och rättigheter.

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

Bolaget rekommenderas 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 (2021): Personuppgiftsregister

Verksamheten gavs följande rekommendationer:

- Klargöra roller, ansvar och arbetssätt i bolagets rutin.
- Se över rättslig grund för de behandlingar som utförs hos bolaget.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har fortsatt arbeta med frågan och påbörjat arbetet med att omhänderta de rekommendationer som lämnats. Bland annat anger bolaget i uppföljningen att det klargjorts vilka roller som ansvarar för registret och dess uppdatering. Vidare anges att bolaget gör en gemensam insats tillsammans med stadsledningskontoret gällande arbetssätt kopplat till registret, och att bolaget framåt kommer övergå till att föra registret i den Excel-mall som dataskyddsenheten utarbetat som grund. Utifrån övergången till Excel-mallen sker ett omtag i arbetet med att se över rättsliga grunder och inom ramen för detta kommer avstämning ske så korrekta grunder anges för de behandlingar som bolaget utför.

Dataskyddsombudet bedömer att bolaget är på god väg i arbetet med registret och fortsatt uppföljning kommer därför ske inom ramen för de fasta kontrollpunkterna om inget särskilt föranleder att det behöver följas upp separat.

Kontroll (2022): Hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Bolaget rekommenderas att komplettera mall/checklista med konkret information om hur medarbetare ska hantera personuppgiftsincidenter om dataskyddskontakterna inte är på plats.
- Mall/checklista bör kompletteras med instruktioner i hur en bedömning av personuppgiftsincidenter ska bedömas samt instruktioner om när och hur information till registrerade ska ges.
- I mall/checklista tydliggöra vilka andra personer/roller som kan behöva involveras vid utredning av incidenter.
- Bolaget rekommenderas att utreda behov av ytterligare utbildning av medarbetare.

Kommentarer och rekommendationer:

I uppföljningen anger bolaget att det har vidtagits åtgärder i enlighet med lämnade rekommendationer. Bolaget anger att mallen har kompletterats, och att medarbetare kontinuerligt informeras om behov av ökad medvetenhet, att information finns tillgänglig och var de finner den samt om de utbildningar som finns tillgängliga via utbildningsportalen. Det planeras även utbildningsinsatser kopplat till arbetet som pågår rörande informationssäkerhet i ett större perspektiv.

Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om inget 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

Fortsätta arbetet med översynen av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och för respektive behandling kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

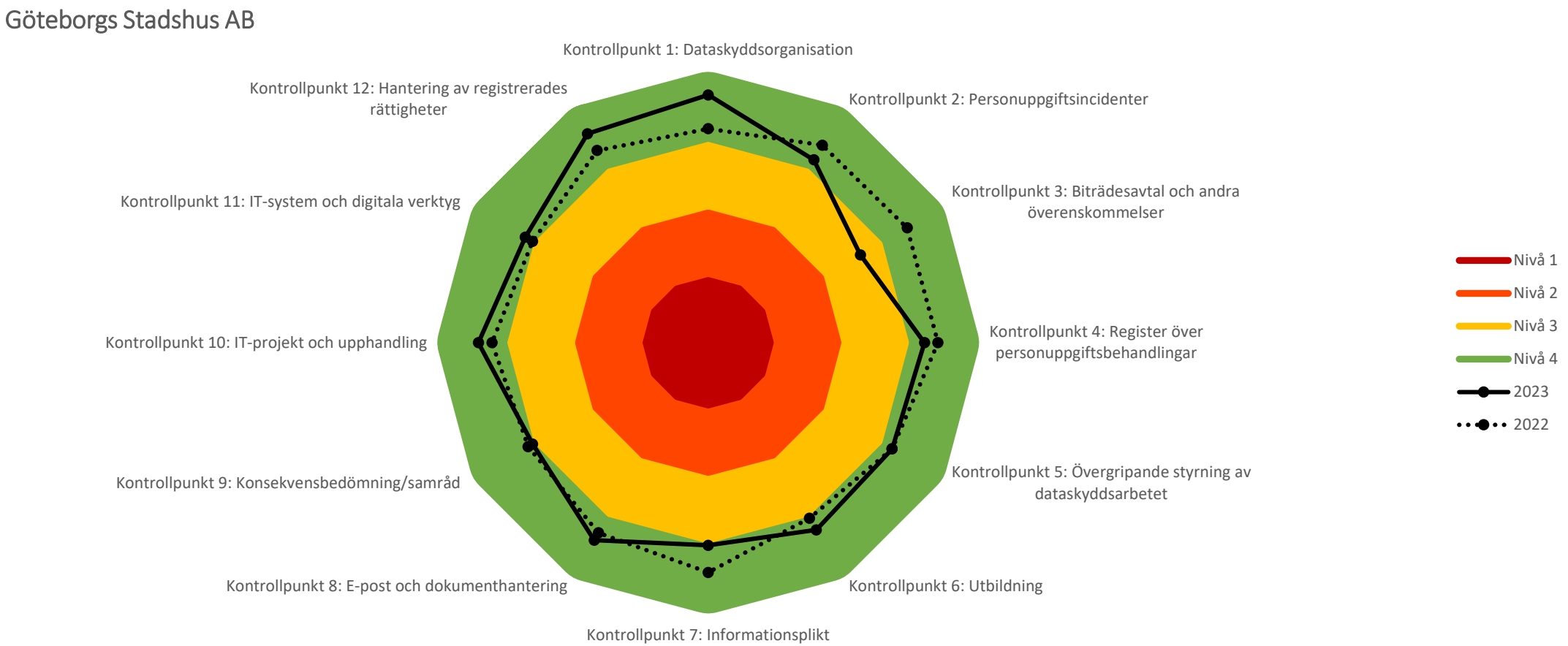
Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn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

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 Stadshus AB

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund

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

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

1.1 Ny utformning av kontrollarbetet

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

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

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

2 Kontrollarbetet 2023–2024

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

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

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

2.1 Kontrollarbetets delar

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

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

2.2 Tidplan för kontrollarbetet 2023–2024

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

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

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

3 Kontroller

3.1 Fasta kontrollpunkter

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

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

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

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

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

3.2 Fördjupad kontroll

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

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

3.3 Uppföljning av genomförda kontroller

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

4 Rapportering

4.1 Årsrapport

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

4.2 Särskilt yttrande

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

5 Kontakt

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

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

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

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

Kontrollpunkt 2: Personuppgiftsincidenter

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

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.