

Återrapportering av uppdrag - ta fram en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022

2023-10-26

Anna-Lena Björk – Informationssäkerhetschef (CISO)

Dataskyddsbuds årsrapport 2022

Dataskyddsbuds årsrapport 2022

- Förvaltningen återkommer i ärendet med en uppdaterad handlingsplan för de åtgärder som behöver vidtas kopplat till informationssäkerhet.

Dataskyddsombuds årsrapport 2022

- 2023-06-01 startade projektet Etablera processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet.
- Projektets mål är att omhänderta brister som redovisas i dataskyddsombuds årsrapport 2021 och 2022 och Stadsrevisionens rapport 2022.
- Projektet har inletts med en förstudie. Förstudien presenterar vilka åtgärder som behöver vidtas, tidsuppskattning för dessa, samt vilka kompetenser som krävs för att lyckas med genomförandet.
- Som ett resultat av det arbete som utförts inom förstudien finns 2023-10-09 en uppdaterad version av handlingsplan med tillhörande tidplan.

Dataskyddsombuds årsrapport 2022

- **Handlingsplanen är uppdelad i två delar**

- Åtgärder kopplade till Stadsrevisionens rapport 2022
- Åtgärder kopplade till dataskyddsombuds årsrapport 2021 och 2022

- 2023-10-09 presenterar handlingsplanen 26 stycken huvudpaket.

- Förvaltningen återkommer i december 2023 med uppdaterad handlings- och tidplan.

- **Tidsuppskattning**

- Hittills uppskattad tidsåtgång för att åtgärda vad rapporterna tar upp uppgår till cirka 56 300 timmar.
- Av dessa timmar uppskattas cirka 35 000 timmar tillhöra rapporternas gemensamma åtgärder.
- Observera att det 2023-10-09 återstår att identifiera ytterligare åtgärder och tidsuppskattningar.
- Timmarna ska utföras av ett 100-tal olika kompetenser inom Intraservice.

Tidplan

Tidplan



Göteborgs
Stad

[illegible]

Handlingsplan

Dataskyddsbuds årsrapport 2022

Dataskyddsbuds årsrapport innehåller 12 kontrollpunkter samt särskilda iakttagelser.

På kommande sidor ges en översiktlig information om vad respektive kontrollpunkt innefattar.

Till respektive kontrollpunkt ges en kortfattad beskrivning av projektåtgärdernas omfattning.

För mer detaljerad information hänvisas till tjänsteutlåtande daterat 2023-10-09, och dess bilagor.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 1: Dataskyddsorganisation**
- Kontrollpunkt 1, Dataskyddsorganisation, 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.

Omfattning:

- Projektet kommer att inventera och föreslå justering av roller, ansvar och mandat (befogenhet) för att säkerställa att styrning, hantering och uppföljning av informationssäkerhet sker utifrån gällande krav.
- En väl fungerande dataskyddsorganisation inkluderar att alla medarbetare ges ett tydligt ansvar och mandat i frågor som rör informationssäkerhet. Det ska för varje enskild roll vara tydligt vilket ansvar och vilket mandat som följer med rollen.
- Åtgärder kommer att hanteras inom huvudpaket AnsvarRollerMandat (2023-10-26 – 2024-06-30).

Tidsuppskattning dataskyddsorganisation:

- Cirka 3 024 timmar

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-26. Åtgärder tillhörande huvudpaket AnsvarRollerMandat har prioritet 1. En tydlighet i ansvar och mandat är avgörande för att resterande arbete ska ges möjlighet att genomföras och omhändertas för fortsatt förvaltning efter att projektet avslutats.

Dataskyddsombuds årsrapport 2021 och 2022

- **Kontrollpunkt 2: Personuppgiftsincidenter**
- Kontrollpunkt 2, Personuppgiftsincidenter, avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftsincidenter.

Omfattning:

- Projektet kommer att analysera och föreslå justering av incidenthanteringsprocessen. Justeringar som inkluderar arbetssätt för att identifiera och hantera personuppgiftsincidenter.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Incident (2024-02-01 – 2025-06-30).

Tidsuppskattning personuppgiftsincidenter:

- Cirka 2 900 timmar

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Åtgärder kopplade till personuppgiftsincidenter beräknas vara genomförda i mars/april 2024. Observeras bör att vissa åtgärder är utförda under Q2/Q3 2023.

Dataskyddsombuds årsrapport 2021 och 2022

- **Kontrollpunkt 3: Biträdesavtal och andra överenskommelser**
- Kontrollpunkt 3, Biträdesavtal och andra överenskommelser, 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.

Omfattning:

- Projektet kommer att genomlysna och föreslå förbättringar i processer och arbetssätt som berör biträdesavtal och andra överenskommelser gällande dataskydd.
- Projektet kommer genomföra även analyser och ge förslag till justering av styrande dokument inom förvaltningen.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Kund (2024-02-01 – 2025-06-30).

Tidsuppskattning biträdesavtal och andra överenskommelser:

- Tidsuppskattning ännu ej genomförd.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Förslag till justering av styrande dokument beräknas vara slutfört i juni 2024. Arbetet med att genomlysna och föreslå förbättringar i processer och arbetssätt beräknas vara slutfört i sin helhet i juni 2025.

Dataskyddsombuds årsrapport 2021 och 2022

- **Kontrollpunkt 4: Personuppgiftsregister**
- Kontrollpunkt 4, Personuppgiftsregister 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 personuppgiftsregister innefattas.

Omfattning:

- Projektet kommer att införa kontrollpunkter i relevanta processer för verifiering av att personuppgiftsregistret är uppdaterat, inklusive att relevanta riskanalyser utförts.
- Projektet kommer därtill att komplettera process för efterlevnadskontroller med kontrollpunkt av att personuppgiftsregister är uppdaterade.
- Utöver detta kommer projektet att se över hantering av personuppgiftsregister och processer och arbetssätt tillhörande dokumentation av personuppgiftsbehandlingar, riskanalyser och tröskelanalyser/konsekvensbedömningar.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Systemstöd (inkl. PU-reg) (2023-02-01 – 2025-06-30). *PU-reg är en förkortning för Personuppgiftsregister.*

Tidsuppskattning personuppgiftsregister:

- Cirka 7 400 timmar. Arbete pågår med att identifiera tillkommande timmar. Se även särskilda iakttagelser 2021.

Status 2023-08-09: Åtgärder påbörjades i februari 2023. Efter ett uppehåll juni – augusti återupptogs arbetet i september 2023. Arbetet beräknas vara klart 2025-06-30. Arbetet sker i samarbete med avdelningen för Gemensamma tjänster och Stadsledningskontoret.

Dataskyddsombuds årsrapport 2021 och 2022

- **Kontrollpunkt 5: Övergripande strategi för dataskydd**
- Kontrollpunkt 5, Övergripande strategi för dataskydd, avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Omfattning:

- Projektet kommer att se över/ge förslag på justering av/ta fram processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhetsarbetet inom förvaltningen och organisationen som ansvarar för leverans av tjänster.
- Inom detta deluppdrag kommer strategier, anvisningar, rutiner och instruktioner kopplade till informationssäkerhet att tas fram med mål att medarbetare inom Intraservice enkelt och lätt ska få handledning i det dagliga arbetet.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Ledningsprocess (2023-10-01 – 2025-12-31).

Tidsuppskattning övergripande strategi för dataskydd:

- Cirka 1 000 timmar

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Ledningsprocess: 2023-10-01 – 2025-12-31.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 6: Utbildning**
- Kontrollpunkt 6, Utbildning, verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Omfattning:

- Inom ramen för projektet kommer processer och arbetssätt tas fram avseende kontinuerlig utbildning av personal med fokus på styrning, hantering och uppföljning av informationssäkerhet.
- Utifrån de förändringar som kommer att genomföras inom projektet kommer utbildningsinsatser att genomföras.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Utbildning (2023-10-01 – 2026-06-30).

Tidsuppskattning utbildning:

- Cirka 4 100 timmar. Ej medräknat är den insats som utbildningsdeltagare behöver bidra med.

Status 2023-08-09: Utbildningsinsatser är genomförda under perioden februari – april utifrån arbetet inför lansering av Digitala navet. Utbildningar kommer att genomföras under hela projektperioden, from 2023-09-01 tom 2026-06-30..

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 7: Integritetspolicy**
- Kontrollpunkt 7, Integritetspolicy, avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Omfattning:

- Inom projektet kommer processer att granskas/justeras/tas fram för att säkerställa att styrande dokument som ägs av Intraservice årligen granskas och verifieras. Integritetspolicy med inriktning på de registrerade (både internt och externt) ska följa processen för livscykelhantering av styrande dokument inom Intraservice.
- Projektet kommer att genomlysas och föreslå förändringar av existerande Integritetspolicy till registrerade (både internt och externt).
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Registrerades rättigheter (2024-02-01 – 2024-06-30).

Tidsuppskattning integritetspolicy:

- Cirka 120 timmar

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Registrerades rättigheter: 2024-02-01 – 2024-06-30.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 8: Mejl och dokumenthantering**
- Kontrollpunkt 8, Biträdesavtal och andra överenskommelser, avser verksamhetens rutiner för e-post och dokumenthantering. För detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Omfattning:

- Projektet kommer att genomföra en inventering och föreslå förbättringar till nuvarande rutin och arbetssätt tillhörande förvaltning av dokumenthanteringsplan. Projektet kommer att ställa krav på att Intraservice ska ha en uppdaterad dokumenthanteringsplan.
- Inom projektet kommer hänsyn tas till kravställningar utifrån tekniskt arkivansvar avseende skydd av information så att den kan bevaras för framtida bruk.
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Tekniskt arkivansvar (2024-02-01 – 2026-06-30).

Tidsuppskattning mejl och dokumenthantering:

- Tidsuppskattning ännu ej genomförd.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Tekniskt arkivansvar: 2024-02-01 – 2026-06-30.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 9:
Konsekvensbedömning/samråd**
- Kontrollpunkt 9, Konsekvensbedömning/samråd, avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Omfattning:

- Projektet kommer att genomlysas och föreslå förändringar i relevanta processer i avsikt att säkerställa att beslutspunkter införs. Beslutspunkter som kräver någon form av dokumentation. Avsikten med detta är att det ska vara tydligt att relevanta riskanalyser samt tröskelanalyser/konsekvensbedömningar ska genomföras, samt att det ska vara möjligt att följa upp att så skett.
- Alla processer där behov av att konsekvensbedömning/samråd genomförs kommer att hanteras. Två exempel på processer som kommer att hanteras inom projektet är inköpsprocessen, förändringsprocessen (Change Management).
- Dessa kontrollpunkter definieras av en huvudprocess kopplat till samtliga huvudpaket och kommer att utvecklas under hela projektets gång. 2023-10-01 – 2026-06-30).

Tidsuppskattning konsekvensbedömning/samråd:

- Tidsuppskattning ännu ej genomförd i sin helhet.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-01. Beräknad tidsperiod för åtgärder kopplade till huvudprocessen 2023-10-01 – 2026-06-30.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 10: IT-projekt och upphandling**
- Kontrollpunkt 10, IT-projekt och upphandling, 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.

Omfattning:

- Projektet kommer att genomlysas, föreslå och genomföra förändringar i relevanta processer med avsikt att säkerställa att arbetet inte går vidare förrän det är verifierat att relevanta informationssäkerhets-/dataskyddsfrågor är hanterade. Målet är att denna typ av frågor hanteras i samband med nyutveckling, inköp/upphandling, förvaltning, förändring och avveckling av system och tjänster.
- Åtgärder tillhörande denna kontrollpunkt kommer att genomföras inom flera av projektets huvudpaket. Främst kommer arbete att ske inom huvudpaket Teknisk säkerhet, Informationsklassning, ~~Ledningsprocess~~, Projekt, Riskhantering och Omvärldsbevakning (2023-10-01 – 2026-06-30).

Tidsuppskattning IT-projekt och upphandling:

- Tidsuppskattning ännu ej genomförd i sin helhet.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket-där förändringar av processer och arbetssätt kommer att hanteras: 2023-10-01 – 2026-06-30.

Dataskyddsombuds årsrapport 2021 och 2022

- **Kontrollpunkt 11: IT-system och digitala verktyg**
- Kontrollpunkt 11, IT-system och digitala verktyg, avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår.

Omfattning:

- I samband med genomlysning och justering av processer och arbetssätt för att säkerställa att informationssäkerhet-/dataskyddsfrågor hanterats i samband med nyutveckling, inköp/upphandling, förvaltning, förändring och avveckling av system och tjänster ingår att analysera verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg.
- Åtgärder tillhörande denna kontrollpunkt kommer att genomföras inom flera av projektets huvudpaket. Främst kommer arbete att ske inom huvudpaket Ledningsprocess, Projekt, Systemstöd, Riskhantering och Omvärldsbevakning (2023-10-01 – 2025-12-31).

Tidsuppskattning IT-system och digitala verktyg:

- Cirka 3 600 timmar.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Ledningsprocess och huvudpaket där förändringar av processer och arbetssätt kommer att hanteras: 2023-10-01 – 2025-12-31.

Dataskyddsbuds årsrapport 2021 och 2022

- **Kontrollpunkt 12: Hantering av registrerades rättigheter**
- Kontrollpunkt 12, Hantering av registrerades rättigheter, avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering

Omfattning:

- Projektet kommer att genomlysas och ta fram förslag till justering av processer och rutiner för hanteringen av de registrerades rättigheter.
- Projektet kommer även att genomlysas och föreslå förändringar av existerande Integritetspolicy till registrerade (både internt och externt).
- Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Registrerades rättigheter (2024-02-01 – 2024-06-30).

Tidsuppskattning Registrerades rättigheter:

- Cirka 120 timmar.

Status 2023-08-09: Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Beräknad tidsperiod för åtgärder kopplade till huvudpaket Registrerades rättigheter: 2024-02-01 – 2024-06-30.

Dataskyddsbuds årsrapport 2021 och 2022

- **Särskilda iakttagelser 2021**

- Tredjelandsoverföring och användning av sociala medier. Personuppgiftsbehandlingar vid användning av sociala medier som innebär tredjelandsoverföring.

Omfattning:

- Inom ramen för projektet kommer kartläggning och dokumentation ske av personuppgiftsbehandlingar inom ramen för tjänsteleveranser. Detta inkluderar dokumentation av personuppgiftsbehandlingar vid användning av sociala medier.

Tidsuppskattning särskilda iakttagelser 2021:

- Cirka 4 500 timmar för fortsatt arbete from september 2023. Observera att dessa timmar är inkluderade i timmar som anges tillhörande kontrollpunkt 4.

Status 2023-08-09: Arbete med dokumentation av personuppgiftsbehandlingar inom ramen för tjänsteleveranser påbörjades i februari 2023 och beräknas fortsätt fram till 2025-06-30.

Dataskyddsbuds årsrapport 2021 och 2022

• Särskilda iakttagelser 2022

- Intraservices ansvar som personuppgiftsbiträde. I samverkan med parter inom Göteborgs Stad tydliggöra ansvarsförhållande och Intraservice del av leverantörskedjan och roll i staden.

Omfattning:

- Samverkan med parter inom Göteborgs Stad för att tydliggöra ansvarsförhållande och Intraservice del av leverantörskedjan och roll i staden kommer att ske utanför projektet.
- Juni 2023 tog nämnden för Intraservice beslut om att ärende om ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur hemställs till kommunstyrelsen.

Tidsuppskattning särskilda iakttagelser 2022:

- Arbete med denna kontrollpunkt kommer inte att utföras inom projektet.

Status 2023-08-09: Initiala samverkansmöten med Stadsledningskontoret genomförda april – juni 2023. Juni 2023 tog nämnden för Intraservice beslut om att ärende om ansvarsfördelning av personuppgiftsbehandlingar i gemensamma tjänster och tjänster tillhörande digital infrastruktur hemställs till kommunstyrelsen.

Förändringar

Förändringar

- Tidigare angivna avgränsningar i form av att projektet endast tar fram kravspecifikation för systemstöd gäller inte längre.
- Projektet tar över planerade förstudie tillhörande systemstöd. En förstudie som skulle ha genomförts av avdelningen för Gemensamma tjänster. Ekonomiska medel kommer att föras över till projektet från Gemensamma tjänster.

Risker

Risker tillhörande genomförandet av projektet

- Ekonomiska förutsättningar verksamhetsåren 2024, 2025.
- Tillgång till expertstöd i form av konsulter.
- Tillgång till interna resurser inom förvaltningen.
- Utvecklings- och förvaltningsaktiviteter får högre prioritet än projektaktiviteter.
- Projektaktivitet är omfattande och komplexa, vilket påverkar Intraservice förmåga att leva upp till gällande krav, samt att förhindra och hantera incidenter, nu och framöver.

Framgångar

- Sedan föregående åiterrapportering i augusti 2023 ses specifikt nedan framgångar
 - Arbete med handlingsplan och tidplan har gett tydligare bild över åtgärder, omfattning, tids- och resursåtgång. Dialoger med resursägare är påbörjade, och det är ett positivt bemötande.
 - Arbetet tillhörande framtagande och implementation av anvisningar, rutiner, instruktioner samt systemstöd kommer att utföras i dialog med Stadsledningskontoret med mål att förvaltningar och bolag inom Göteborgs stad ska erhålla gemensamma processer och arbetssätt (inkl. systemstöd) (detta gäller bl.a. för arbete med informationsklassning, riskanalyser, konsekvensbedömningar, med mera).
 - Ekonomiska medel för förstudie tillhörande systemstöd förs över från Gemensamma tjänster till projektet.

Förvaltningen återkommer i december 2023 med uppdaterad handlings- och tidplan

Kontakt

Anna-Lena Björk

anna.bjork@intraservice.goteborg.se

Intraservice, Göteborgs Stad