

Tjänsteutlåtande

Utfärdat 2024-06-10

Diarienummer 0104/23

Handläggare

Anna-Lena Björk

Telefon: 079 060 61 82

E-post: anna.björk@intraservice.goteborg.se

Återrapportering av handlingsplan utifrån dataskyddsombudets rapport samt uppdrag att etablera dataskyddsorganisation

Förslag till beslut

I nämnden för Intraservice:

Handlingsplan innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023 samt förvaltningens förslag till etablering av dataskyddsorganisation fastställs.

Sammanfattning

Dataskyddsombudets årsrapport 2023 innehåller förbättringsförslag kopplade till de brister som årsrapporten redovisar gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Förvaltningen har presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsombuds årsrapport 2022 och 2023, senast 2024-06-23, då förvaltningens handlingsplan återremitterades till förvaltningen med uppdrag att återkomma på nämndmöte i maj 2024 med förslag på en dataskyddsorganisation som uppfyller lagstiftade krav på dataskydd.

I nämndmöte 2024-04-24 beslutades om att utifrån förvaltningens pågående arbete och planering kommer handlingsplanen att redovisas för nämnden vid sammanträdet i juni 2024.

Förvaltningen har nu i juni 2024 ett förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation. Ett förslag som inkluderar att befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, vilket inkluderar aktiviteter kopplade till dataskydd. Dataskydd innefattar skydd av personuppgifter. Personuppgifter utgör en typ av information. Informationssäkerhet innefattar skydd av alla typer av information.

Bedömning ur ekonomisk dimension

Handlingsplanens aktiviteter hanteras inom ramen för förvaltningens budget 2024.

Förvaltningens förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation innefattar förslag till ett antal åtgärder. Åtgärderna inkluderar att befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, och därinom dataskydd, arkivansvar och tekniskt arkivansvar. Åtgärderna har presenterats för Intraservice ledningsgrupp och chefer, och riskanalys har genomförts med ett perspektiv på arbetsmiljö. Riskanalysen har identifierat risk för att det finns åtgärder som behöver vidtas inom förvaltningen som medför kostnader kopplade till rekryteringsbehov. Fortsatt analys och framtagande av förslag till åtgärder kommer att ske under perioden juli – december, där även hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till det systematiska informationssäkerhetsarbetet.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Handlingsplanen innehåller åtgärder som syftar till att stärka individens rättigheter vid behandling av personuppgifter enligt vad som förordas inom ramen för Dataskyddsförordningen. Dataskyddsförordningen är en lag som gäller inom hela Europeiska unionen (EU) och har bland annat till syfte att skapa en enhetlig och likvärdig nivå av skyddet av personuppgifter. Dataskyddsförordningens engelska benämning är *General Data Protection Regulation* (GDPR).

Utifrån handlingsplanens aktiviteter och dess resultat med förslag om åtgärder har riskanalys ur ett arbetsmiljömässigt perspektiv genomförts. Det arbetsmiljömässiga perspektivet kan delas in i två delar; social arbetsmiljö organisatorisk arbetsmiljö.

Social arbetsmiljö

Riskanalysen har identifierat risk för att personer som innehar roller som verksamhetschef, enhetschef och förvaltningsledare kan komma att uppleva negativ stress. Detta utifrån att dessa roller utifrån förslag om åtgärder får utökade och nya ansvar, respektive ökat antal arbetsuppgifter.

Organisatorisk arbetsmiljö

Riskanalysen har identifierat att det utifrån hur förvaltningen är organiserad idag finns risker kopplade till ledning och styrning och fördelning av arbetsuppgifter utifrån utökade och nya ansvar. Risker som ger svar om ett behov av ökat antal resurser.

Riskanalysen med perspektiv på arbetsmiljö påvisar även risker som finns idag, risker som kommer att finnas även efter att föreslagna åtgärder vidtagits. Det gäller risker tillhörande samverkan med andra myndigheter inom Göteborgs Stad. Riskerna avser otydlighet i ansvarsfördelning. Ett exempel på otydlighet i ansvarsfördelning tas även upp i dataskyddsombuds årsrapport; otydlighet kring vilka parter som är att anse som personuppgiftsansvarig, personuppgiftsbiträde, eller om det råder delat personuppgiftsansvar för de personuppgiftsbehandlingar som utförs inom Intraservices

leveranser av gemensamma tjänster och digital infrastruktur. Ett annat exempel på otydlighet rör arkivansvaret kopplat till dessa leveranser.

Fortsatt analys och framtagande av förslag till åtgärder kommer att ske under perioden juli – december, där även hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till det systematiska informationssäkerhetsarbetet.

Samverkan

Ärendet samverkas med de fackliga representanterna i FSG 2024-05-23.

Bilagor

1. Bildspel - Återrapportering av handlingsplan utifrån dataskyddsombudets rapport
2. Bildspel – Roller och ansvar
3. Protokollsutdrag 2024-04-24 § 76
4. Protokollsutdrag 2024-03-06 § 42

Ärendet

Förvaltningen har under 2023 presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsombuds årsrapport 2022. De åtgärder som tas upp i denna handlingsplan möter även upp mot de brister som tas upp i dataskyddsombuds årsrapport 2023.

Nämnden för Intraservice har att ta ställning till godkännande av aktuell handlingsplan daterad 2024-06-10 samt förvaltningens förslag till etablering av dataskyddsorganisation.

Beskrivning av ärendet

Dataskyddsombudets årsrapport 2023 innehåller förbättringsförslag kopplade till de brister som årsrapporten redovisar gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Förvaltningen har under 2023 presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsombuds årsrapport 2022. De åtgärder som tas upp denna handlingsplan möter även upp mot de brister som tas upp i dataskyddsombuds årsrapport 2023. Förvaltningen har presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsombuds årsrapport 2022 och 2023, senast 2024-06-23, då förvaltningens handlingsplan återremitterades till förvaltningen med uppdrag att återkomma på nämndmöte i maj 2024 med förslag på en dataskyddsorganisation som uppfyller lagstiftade krav på dataskydd.

I nämndmöte 2024-04-24 beslutades om att utifrån förvaltningens pågående arbete och planering kommer handlingsplanen att redovisas för nämnden vid sammanträdet i juni 2024.

Förvaltningen har nu i juni 2024 ett förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation. Ett förslag som inkluderar att befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, vilket inkluderar aktiviteter kopplade till dataskydd. Dataskydd innefattar skydd av personuppgifter. Personuppgifter utgör en typ av information. Informationssäkerhet innefattar skydd av alla typer av information.

Kontrollpunkterna i Dataskyddsombuds årsrapport 2023 är de samma som för årsrapport 2022. Resultatet 2023 avviker dock från resultatet 2022. En anledning till dessa avvikelser är att frågorna formulerats på olika sätt. I 2022 års frågeformulär ställdes frågor om verksamheten har rutiner. I 2023 års frågeformulär ställdes motsvarande frågor, men då med frågeställningen om verksamheten har dokumenterade arbetssätt.

En annan anledning till att resultatet 2023 avviker från resultatet 2022 är att större insikt har getts i hur saker och ting fungerar när projektet Etablera systematiskt informationssäkerhetsarbete identifierade vilka åtgärder som behöver vidtas.

Den 1 juni 2023 startade projektet Etablera processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet. Projektets mål är att omhänderta brister som redovisas i dataskyddsombuds årsrapport 2021, 2022 och 2023, samt 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.

Utifrån vad som framkommit under förstudiearbetet beräknas projektet pågå fram till halvårsskiftet 2026.

Fasta kontrollpunkter

Nedan ges en redogörelse om vad respektive kontrollpunkt avser tillsammans med en beskrivning av vad som kommer att utföras inom ramen för aktuellt projekt (omfattning), statusuppdatering, samt tidsuppskattning.

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

En tydlig, förankrad och fastställd organisation kring informationssäkerhet (inkluderande dataskyddsorganisation) och arkiv tydliggör vilka arbetsuppgifter och vilket ansvar respektive tjänsteperson i organisationen har och underlättar för kunskaps- och informationsspridning. Arbetet behöver bedrivas på både strategisk, taktisk och operativ nivå i organisationen och omfattar nämnden för Intraservices roll som egen myndighet och leverantör av tjänster. Arbetet är förvaltningsövergripande och har beröringspunkter till områden som rör, informationssäkerhet (som inkluderar administrativ och teknisk säkerhet) och arkiv. Samtliga områden hänger ihop och blir sammantaget kravställare på de tjänster som levereras. Perspektiven ska genomsyra arbetet med både utveckling och förvaltning och ställer krav på förvaltningens förmåga att arbeta tillsammans och se de ingående områdena som delar i en helhet som både hänger ihop och behöver styras utifrån ett helhetsperspektiv.

Projektet har tagit fram förslag till en förvaltningsövergripande organisering som innebär justering av ansvar, roller och mandat (befogenhet) för att säkerställa en ändamålsenlig styrning, hantering och uppföljning av informationssäkerhetsarbetet vilket inkluderar arbetet med dataskydd och arkiv. Anvisningar, instruktioner och rutiner, samt processer och arbetssätt kommer hjälpa till med att beskriva arbetsuppgifter kopplade till informationssäkerhet/dataskydd och arkiv.

Målet är att dataskydd och arkiv blir en integrerad del i allt arbete tillhörande informationssäkerhet, och att informationssäkerhet blir en naturlig del i det dagliga arbetet för samtliga roller.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket AnsvarRollerMandat.

Status 2024-06-10

Åtgärder tillhörande huvudpaket AnsvarRollerMandat och Ledningsprocess är påbörjade och beräknas pågå fram till 2024-12-31 respektive 2025-12-31.

Aktivitets- och tidplan är framtagen.

Förvaltningen har nu i juni 2024 ett förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation. Ett förslag som inkluderar att

befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, vilket inkluderar aktiviteter kopplade till dataskydd. Dataskydd innefattar skydd av personuppgifter. Personuppgifter utgör en typ av information. Informationssäkerhet innefattar skydd av alla typer av information.

Fortsatt arbete med andra ansvar/roller/mandat kommer att ske löpande under projektets gång.

Arbete har utförts sedan en tid tillbaka när det gäller rådgivning och stöttning i dataskyddsfrågor. Rådgivning och stöttning i dataskyddsfrågor har hanterats av dataskyddskontakter inom förvaltningens kanslienhet, och sedan 2022 har även CISO och dennes medarbetare hanterat denna typ av uppdrag. Det förslag till dataskyddsorganisation som förvaltningen presenterar för nämnden i juni månad inkluderar förslag om etablering av en funktion, en dataskyddsfunktion. Dataskyddsfunktionen ska bemannas upp av informationssäkerhetssamordnare som har ansvar att agera som dataskyddskontakt.

Antar nämnden handlingsplan daterad 2024-06-10 samt förvaltningens förslag till etablering av dataskyddsorganisation kan utbildningsaktiviteter planeras utifrån aktiviteter och ansvar som är kopplade till dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Utbildningsaktiviteterna omfattar utbildning av alla medarbetare (och chefer) inom förvaltningen.

Varje medarbetare inom förvaltningen behöver förstå vad som krävs av denne utifrån alla typer av styrande regelverk (lagar, förordningar, styrande dokument, etcetera). 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.

Fortsatt arbete

Risikanalys ur ett arbetsmiljöperspektiv har identifierat risker ur ett perspektiv på social och organisatorisk arbetsmiljö.

Social arbetsmiljö

Risikanalysen har identifierat risk för att personer som innehar roller som verksamhetschef, enhetschef och förvaltningsledare kan komma att uppleva negativ stress. Detta utifrån att dessa roller utifrån förslag om åtgärder får utökade och nya ansvar, respektive ökat antal arbetsuppgifter.

Organisatorisk arbetsmiljö

Risikanalysen har identifierat att det utifrån hur förvaltningen är organiserad idag finns risker kopplade till ledning och styrning och fördelning av arbetsuppgifter utifrån utökade och nya ansvar. Risker som ger svar om ett behov av ökat antal resurser.

Risikanalysen med perspektiv på arbetsmiljö påvisar även risker som finns idag, risker som kommer att finnas även efter att föreslagna åtgärder vidtagits. Det gäller risker tillhörande samverkan med andra myndigheter inom Göteborgs Stad. Riskerna avser otydlighet i ansvarsfördelning. Ett exempel på otydlighet i ansvarsfördelning tas även upp

i dataskyddsbuds årsrapport; otydlighet kring vilka parter som är att anse som personuppgiftsansvarig, personuppgiftsbiträde, eller om det råder delat personuppgiftsansvar för de personuppgiftsbehandlingar som utförs inom Intraservices leveranser av gemensamma tjänster och digital infrastruktur. Ett annat exempel på otydlighet rör arkivansvaret kopplat till dessa leveranser.

Fortsatt analys och framtagande av åtgärder kommer att ske under perioden juli – december, där även hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till det systematiska informationssäkerhetsarbetet.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket AnsvarRollerMandat 2023-10-26 – 2024-12-31 och Ledningsprocess 2023-10-26 – 2025-12-31.

Tidsuppskattning dataskyddsorganisation

Cirka 4 000 timmar.

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.

Status 2024-06-10

Hanteringen kring kontaktvägar till PUA på förvaltningar och bolag har förändrats så att informationen skickas till förvaltningsbrevlådor eller motsvarande för att säkra snabb hanteringen av information till PUA.

Incidenthanteringsprocessen har förstärkts gällande lessons learned som har hållits efter större personuppgiftsincidenter. Mallar och dokument har uppdaterats för att tydligare följa Integritetsskyddsmyndighetens (IMYs) krav på dokumentation vid anmälan.

För personuppgiftsincidentprocessen har utbildningssatsningarna som pågår varit bra då framför allt handläggare har erhållit ökad kunskap när det kommer till vikten av att kontakta PUI-koordinator vid misstanke om personuppgiftsincident.

Hanteringen av personuppgiftsincidenter uppdaterats så att den nu även omfattar brist på tillgänglighet (enligt SLA).

Under 2024 kommer fortsatt arbete göras med att genomlys incidentprocesser och förtydliga arbetet med säkerhetsincidenter.

Ett mål i det fortsatta arbetet utgörs av uppdatering av e-learning under hösten 2024 för nya handläggare i Servicenow med information kring PUI och säkerhetsincidenter.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Incident: 2024-02-01 – 2025-06-30.

Tidsuppskattning personuppgiftsincidenter

Cirka 3 292 timmar.

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 genomlysas och föreslå förbättringar i processer och arbetssätt som berör biträdesavtal och andra överenskommelser gällande dataskydd.

Projektet kommer genomföra analyser och ge förslag till justering av styrande dokument inom förvaltningen.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Kund.

Status 2024-06-10

Datum för start av arbete med denna kontrollpunkt var beräknad till 2024-02-01. Starten av kontrollpunkten har förskjutits framåt i tiden på grund av resursbrist. Ny beräknas start är 2024-08-19.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Kund: 2024-08-19 – 2025-12-31.

Förslag till justering av styrande dokument beräknas vara slutfört i december 2024.

Arbetet med att genomlysas och föreslå förbättringar i processer och arbetssätt beräknas vara slutfört i sin helhet i december 2025.

Observera att tidsuppskattning ännu inte genomförts, vilket innebär att datum för när åtgärder beräknas vara slutförda kan komma att ändras.

Tidsuppskattning biträdesavtal och andra överenskommelser

Tidsuppskattning ej ännu genomförd.

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.

Dokumentation av personuppgiftsbehandlingar tillhörande tjänsteleveranser inkluderar framtagande av tjänstespecifikationer och funktionsbeskrivningar. Tjänstespecifikationer och funktionsbeskrivningar är dokument som respektive kund enkelt ska ha möjlighet att ta del av. I dagsläget finns inte systemstöd för säker lagring och säker delning av denna typ av dokumentation. Framtagning av kravspecifikation för denna typ av systemstöd kommer att ske inom projektet.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Systemstöd (inkl. PU-reg). PU-reg är en förkortning för Personuppgiftsregister.

Arbetet kommer att ske i samarbete med avdelningen för Gemensamma tjänster.

Status 2024-06-10

Dokumentation av personuppgiftsbehandlingar och säkerhetsåtgärder tillhörande tjänsteleveranser påbörjades under februari 2023 med fokus på att dokumentera de behandlingar och säkerhetsåtgärder som rör tjänsten Digitala navet.

Arbete med fortsatt dokumentation för resterande tjänsteleveranser återupptogs under oktober 2023.

Preliminär plan för upphandling av ett för Göteborgs Stad gemensamt systemstöd ger svar om att upphandling beräknas vara slutförd juli 2024 och att implementationsarbetet kan påbörjas under Q3 2024. Separat planering kommer att ske av produktionssättning. Produktionssättning kommer att påbörjas för några förvaltningar/bolag, för att sedan rullas ut successivt.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Systemstöd (inkl. PU-reg.): 2023-10-01 – 2025-06-30.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Tjänstespecifikationer och Funktionsbeskrivningar: 2023-10-01 – 2025-06-30.

Tidsuppskattning personuppgiftsregister

Nuvarande tidsuppskattning för kvarstående arbete ger svar om cirka 7 400 timmar. Det finns dock identifierade aktiviteter som inte är tidsuppskattade, vilket gör att det tillkommer timmar. Utöver dessa 7 400 timmar tillkommer cirka 3 600 till fortsatt arbetet med dokumentation av personuppgiftsbehandlingar och säkerhetsåtgärder i tjänstespecifikationer och funktionsbeskrivningar tillhörande tjänsteleveranser. Ca. 25 % av tjänsterna är påbörjade vad gäller tjänstespecifikationer och funktionsbeskrivningar där 350 timmar har lagts ner i arbete vilket ger att 3 250 timmar återstår.

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.

Projektet kommer inte enbart fokusera på strategi, utan även anvisningar, rutiner och instruktioner i avsikt att få till de förbättringar som bland annat hör till kontrollpunkt 1 Dataskyddsorganisation.

Som tidigare omnämnts är målet att dataskydd ska bli en integrerad och naturlig del av allt arbete tillhörande informationssäkerhet.

Åtgärder kommer att genomföras inom ramen för flera av projektets huvudpaket. Exempelvis Ledningsprocess, Informationsklassning, Riskhantering, Kontinuitetshantering, med flera.

Status 2024-06-10

Arbetet med denna kontrollpunkt startade upp 2023-10-01.

De åtgärder som ingår i huvudpaketen Ledningsprocess, Informationsklassning, Riskhantering och Kontinuitetshantering är prioriterade, och har startats upp parallellt med arbetet inom huvudpaket AnsvarRollerMandat samt Identitet och åtkomst.

Tidsuppskattning övergripande strategi för dataskydd

Den totala tiden för samtliga aktiviteter som omnämns ovan uppskattas till cirka 3 600 timmar. Av dessa uppskattas 1 000 timmar till framtagande och beslut om anvisningar som inkluderar dataskydd. Exempelvis anvisning tillhörande Informationssäkerhet, IT-säkerhet, fysisk säkerhet, ”moln”, Autentisering och åtkomst, etcetera.

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. Utbildningsinsatser ska genomföras kontinuerligt för att säkerställa att personal är medveten om sitt ansvar tillhörande informationssäkerhet (inkl. dataskydd) och hur detta ansvar kan fullgöras.

Projektet arbetar med framtagande, genomförda och kontinuerliga utbildningar. kopplade till processer och arbetssätt, samt styrande dokument, som justeras respektive implementeras av projektet. Utbildningarna kommer att utgå från resultat från projektets översyn av roller, ansvar och mandat och den/de roller som medarbetare har. Arbetet omfattar planering, identifiering av målgrupper, framtagning av utbildningsmaterial, genomförande av utbildningar, samt uppföljning och kontinuerlig förbättring.

Utbildningsinsatserna syftar till att minska risker och förbättra säkerheten enligt bästa praxis genom att höja medvetenheten och kompetensen samt etablera en säkerhetskultur genom att öka förståelsen för Intraservice säkerhetsbehov.

Målet är att säkerställa att alla intressenter i identifierade målgrupper är utbildade och kompetenta för att uppfylla sina säkerhetsrelaterade roller och ansvar.

Detta innefattar att all personal ska ha kunskap och kompetens kring de krav som gäller för den eller de roller som denne har. Så oavsett om det gäller administrativa eller tekniska arbetsuppgifter.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Utbildning.

Status 2024-06-10

I samband med arbetet tillhörande dokumentation av personuppgiftsbehandlingar, framtagande av tjänstespecifikationer och funktionsbeskrivningar med fokus på de underliggande tjänsterna till Digitala navet genomfördes utbildning med inriktning på detta arbete. Motsvarande utbildningar kommer att genomföras i samband med att arbete med fortsatt dokumentation tillhörande resterande tjänster.

Övriga utbildningsinsatser genomförs inom projektet allteftersom implementation sker av uppdaterade och nya styrande dokument, processer och arbetssätt. Dessa utbildningar publiceras i utbildningsportalen.

Sammanfattning av pågående utbildningar

Utbildning	Lansering	Deltagare (av målgrupp)
Digital informationssäkerhetsutbildning för alla (DISA) för Intraservice	2024-03-29	151 (av 743) 20%
Change management	2024-05-20	15 (av 743) 2 % (Ej kommunicerad)

Två utbildningar har lanserats under våren i utbildningsportalen:

Vidare är fyra utbildningar planerade för lansering i juni - augusti gällande informationsklassning samt riskhantering. Senare under hösten 2024 planeras lansering av sammanlagt 15 utbildningar inom områdena Informationssäkerhet, AI-säkerhet, Kontinuitetshantering IT inom Intraservice och uppdatering av utbildningen Dataskyddsförordningen (DSF) på jobbet samt NIS-2.

Tidsuppskattning utbildning

Uppskattad tid: cirka 4030 timmar. Ej medräknat är den insats som utbildningsdeltagare behöver bidra med.

Kontrollpunkt 7: Informationsplikt

Kontrollpunkt 7, Informationsplikt, avser bland annat 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 Ledningsprocess.

Status 2024-06-10

Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Ledningsprocess: 2023-10-01 – 2025-12-31.

Tidsuppskattning informationsplikt

Tidsuppskattning för delaktivitet Registrerades Rättigheter påbörjad men ej slutförd.

Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkt 8, Mejl och dokumenthantering, 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 arbeta tillsammans med övriga funktioner inom Intraservice som arbetar med styrning av förvaltningens hantering av allmänna handlingar. Arbetet genomförs utifrån de rekommendationer som givits av Stadsrevisionen och Arkivnämnden i tidigare granskningar och inspektioner. Ett omfattande arbete pågår utifrån att förvaltningen med början under hösten 2024 ska införa stadens nya ärendehanteringssystem Ciceron. Detta arbete kommer att innebära en total inventering av samtliga handlingstyper i organisationen vilket kommer gå hand i hand med utvecklingen av nämndens dokumenthanteringsplan.

Inom projektet kommer hänsyn tas till kravställningar utifrån Nämnden för Intraservices tekniska arkivansvar avseende skydd av information så att den kan bevaras för framtida bruk.

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Tekniskt arkivansvar.

Status 2024-06-10

Arbete med nämndens dokumenthanteringsplan och klassificeringsstruktur pågår enligt plan inom ramen för Stadsrevisionens och Arkivnämndens granskningar och inspektioner. Anvisningar för hantering av allmänna handlingar har fastställts och en omfattande utbildningsinsats har initierats. Mall för "Plan för bevarande av digital

information" har tagits fram liksom "Rutin för arkivkrav och informationssäkerhet utifrån ett arkivperspektiv" samt "Anvisning för bevarande av digitala handlingar". Dessa styrande dokument är ännu inte fastställda utan är föremål för samråd med Arkivnämnden.

Införande av funktionalitet för gallring av chattmeddelanden i Teams genomfördes den 1 december 2023 i syfte att bland annat säkerställa gallring av information som inte ska bevaras i enlighet med Arkivnämndens beslut. Detta innebär även att uppgiftsminimering utifrån dataskyddsperspektivet beaktas.

Datum för start av arbete med denna kontrollpunkt är inte beslutad om på grund av att resurser med nödvändig kompetens saknas inom projektet. Rekryteringsaktiviteter har genomförts under 2024 med ambition att anställa medarbetare med kompetens tillhörande arkivfrågor. Resultatet från rekryteringen gav svar om att det inte fanns någon sökande med tillräcklig grundläggande kompetens. Rekryteringsaktiviteter kommer att starta upp på nytt under juni 2024.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Tekniskt arkivansvar: Ej beräknad.

Tidsuppskattning mejl och dokumenthantering

Tidsuppskattning ej ännu genomförd.

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.

Anvisningar, rutiner och instruktioner kommer att uppdateras med mål att ta fram tydliga kriterier kring när en konsekvensbedömning ska genomföras och hur.

Process och arbetssätt tillhörande efterlevnadskontroller kommer att kompletteras med kontrollpunkter för uppföljning av att konsekvensbedömning/samråd genomförs.

Dessa kontrollpunkter definieras av en huvudprocess kopplat till samtliga huvudpaket och kommer att utvecklas under hela projektets gång.

Två exempel på processer där konsekvensbedömning/samråd ska genomföras är processen för Inköp och Förändringsprocessen (Change Management).

Status 2024-06-10

Arbetet med denna kontrollpunkt startade 2023-10-01. Arbeta uppstartat med initiala dialoger med bland andra ansvarig för inköpsprocessen och representanter för Intraservice kvalitets- och processutveckling. På grund av behov av att prioritera ordinarie arbetsuppgifter har aktiviteter kopplade till inköpsprocessen legat vilande sedan december 2023, men kommer återupptas inom kort.

Arbete är också uppstartat tillhörande Förändringsprocessen (Change Management) och pågår sedan april 2024.

Beräknad tidsperiod för åtgärder kopplade till huvudprocessen: 2023-10-01 – 2026-06-30.

Arbete med andra huvudpaket som har inriktning på processer och arbetssätt sträcker sig över perioden 2023-10-01 – 2026-06-30.

Observera att tidsuppskattning ännu inte genomförts i sin helhet, vilket innebär att datum för när åtgärder beräknas vara slutförda kan komma att ändras.

Tidsuppskattning konsekvensbedömning/samråd

Tidsuppskattning ej ännu genomförd i sin helhet. Tidsuppskattning för genomlysning av, beroenden till och eventuell förändring av inköpsprocess ligger på cirka 1 500 timmar.

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 genomlysna, 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.

Interna och externa faktorer påverkar informationssäkerhets-/dataskyddsarbetet, och det är viktigt att arbeta proaktivt med exempelvis omvärldsbevakning för att tidigt identifiera potentiella risker som kan uppstå i samband med förändringar av system och/eller tjänster. Det gäller att förekomma eventuell negativ påverkan genom att ta fram åtgärder. Kontinuerlig och kvalitativ omvärldsbevakning leder till effektiv riskhantering.

Projektet kommer att genomlysna och föreslå förändringar i processer för att säkerställa att omvärldsbevakning genomförs, och att riskhantering sker återkommande och i samband med alla typer av förändringar i samband med projekt; IT-projekt, inköps-/upphandlingsprojekt eller annan typ av projekt. Varje tjänst ska äga och kontinuerligt uppdatera ett riskregister där risker är dokumenterade tillsammans med information om hur de ska/kan hanteras.

Förändringar av system och tjänster sker inte enbart i samband med projektarbete. Förändringar sker kontinuerligt i det dagliga arbetet, vilket gör att informationssäkerhets-/dataskyddsfrågor behöver hanteras som en naturlig del i det dagliga arbetet i syfte att förhindra eller upptäcka intrång och andra säkerhetshändelser som skulle kunna orsaka ett driftstopp eller informationsläckage. Projektet kommer att ta fram strategier, anvisningar, rutiner och instruktioner som stöd till respektive medarbetare utifrån den roll och det ansvar denna har.

Kopplat till informationssäkerhet/dataskydd finns det idag en problematik kring avsaknad av systemstöd för säker hantering av dokumentation. Exempel på dokumentation som det idag saknas säker hantering av är: system med register över tjänster, tjänstebeskrivningar, tjänstespecifikationer, tjänstetyper, funktionsbeskrivningar, riskanalyser, riskregister, konsekvensbedömningar, säkerhetsåtgärder, pub-avtal, leverantörer, systemdokumentation, driftsdokumentation, system etcetera.

Process och arbetssätt tillhörande efterlevnadskontroller ska inom projektet uppdateras för uppföljning av att omvärldsbevakning och riskanalyser genomförs (inom projekt och i det dagliga arbetet), och att varje tjänst äger och kontinuerligt uppdaterar ett riskregister.

Åtgärder tillhörande denna kontrollpunkt kommer att genomföras inom flera av projektets huvudpaket. Främst kommer arbete att ske inom huvudpaket Teknisk säkerhet, Informationsklassning, Projekt, Riskhantering och Omvärldsbevakning.

Status 2024-06-10

Arbete med denna kontrollpunkt startade upp 2023-10-01. Förslag till innehåll i process för informationsklassning och process för riskanalys, med tillhörande anvisningar, är framtagna och har testats internt Intraservice sedan under februari 2024. Förvaltningen inväntar nu nämndens svar om förslag att fastställa dessa.

Beräknad tidsperiod för åtgärder kopplade till kontrollpunkten: 2023-10-01 – 2026-06-30.

Arbete med andra huvudpaket som har inriktning på processer och arbetssätt sträcker sig över perioden 2023-10-01 – 2026-06-30.

Observera att tidsuppskattning ännu inte genomförts i sin helhet, vilket innebär att datum för när åtgärder beräknas vara slutförda kan komma att ändras.

Tidsuppskattning IT-projekt och upphandling

Tidsuppskattning ej ännu genomförd i sin helhet.

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.

I det arbete som ska utföras ingår att dokumentera personuppgiftsbehandlingar och säkerhetsåtgärder i tjänstespecifikationer och funktionsbeskrivningar, samt att uppdatera personuppgiftsregister.

Inkluderat är även arbetet kopplat till samverkan i avsikt att tydliggöra ansvarsförhållande inom Göteborgs Stad och Intraservice del av leverantörskedjan och roll i staden.

Anvisningar, rutiner och instruktioner ska tas fram med mål att underlätta för medarbetare att hantera informationssäkerhet-/dataskyddsfrågor.

Åtgärder tillhörande denna kontrollpunkt kommer att genomföras inom flera av projektets huvudpaket. Främst kommer arbete att ske inom huvudpaket Ledningsprocess (2023-10-01 – 2025-12-31), Projekt (2024-04-01 – 2025-06-30), Systemstöd (2023-10-01 – 2025-06-30), Riskhantering (2023-11-01 – 2024-12-31) och Omvärldsbevakning (2023-12-01 – 2025-06-30), samt ett nytt huvudpaket Säkerhetskontroller (2024-04-01 – 2025-06-30).

Status 2024-06-10

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Ledningsprocess: 2023-10-01 – 2025-12-31.

Tidsuppskattning IT-system och digitala verktyg

Den totala tiden för samtliga aktiviteter som omnämns ovan uppskattas till cirka 3 600 timmar.

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 Ledningsprocess.

Status 2024-06-10

Datum för start av arbete med denna kontrollpunkt är 2024-02-01.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Ledningsprocess: 2023-10-01 – 2025-12-31.

Tidsuppskattning hantering av registrerades rättigheter

Tidsuppskattning för delaktivitet Registrerades Rättigheter påbörjad men ej slutförd.

Rekommenderade fokusområden 2024

Dataskyddsombudet rekommenderar förvaltningen att under 2024 fokusera på:

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkt 7: Informationsplikt

Projektet *Etablera systematiskt informationssäkerhetsarbete* har planerade aktiviteter för 2024 fram till 2026 som berör dessa kontrollpunkter. Delresultat kommer att redovisas under 2024.

Status 2024-06-10

Förvaltningen har i juni 2024 ett förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation. Ett förslag som inkluderar att befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering. Denna typ av ansvar utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet, vilket inkluderar aktiviteter kopplade till dataskydd. Dataskydd innefattar skydd av personuppgifter. Personuppgifter utgör en typ av information. Informationssäkerhet innefattar skydd av alla typer av information.

Förvaltningen har sedan oktober 2023 ett kontinuerligt pågående arbete med framtagande av tjänstespecifikationer och funktionsbeskrivningar tillhörande de gemensamma tjänster och den digitala infrastrukturen som levereras till Göteborgs Stads förvaltningar och bolag. Den dokumentation som tas fram innehåller bland annat information om vilka personuppgiftsbehandlingar som utförs inom leveranserna och vilka säkerhetsåtgärder som finns implementerade. Arbetet beräknas pågå fram till och med 2025-06-30.

Inom ramen för de gemensamma tjänster som förvaltningen levererar till Göteborgs Stads förvaltningar och bolag pågår ett arbete med upphandling av ett systemstöd. Ett systemstöd som bland annat ska innehålla modul utgörande register över personuppgiftsbehandlingar. Preliminär plan för upphandling av ett för Göteborgs Stad gemensamt systemstöd ger svar om att upphandling beräknas vara slutförd juli 2024 och att implementationsarbetet kan påbörjas under Q3 2024. Separat planering kommer att ske av produktionssättning. Produktionssättning kommer att påbörjas för några förvaltningar/bolag, för att sedan rullas ut successivt.

Förvaltningens bedömning

Förvaltningen föreslår nämnden att anta handlingsplan med datum 2024-06-10 innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023, samt förvaltningens förslag till etablering av dataskyddsorganisation.

Stina Hall Hellqvist
Avdelningschef Styrning och stöd

Peter Söderström
Förvaltningsdirektör