

Tjänsteutlåtande

Utfärdat 2023-10-12

Diarienummer 0120/22

Handläggare

Anna Björk

Telefon: 031-368 29 86

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

Återrapportering av uppdrag - Handlingsplan för att åtgärda brister utifrån dataskyddsenhetens årsrapport 2022

Förslag till beslut

I nämnden för Intraservice:

Uppdaterad handlingsplan med tidplan innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022 godkänns

Sammanfattning

2023-02-22 § 43 uppdrog nämnden för Intraservice förvaltningen att ta fram en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022.

Dataskyddsombuds årsrapport 2022 innehåller förbättringsförslag kopplade till de brister som årsrapporten redovisar gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Förvaltningen har tidigare presenterat en översiktlig handlingsplan, senast under augusti månad 2023 inför möte med nämnden för Intraservice.

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 påbörjats inom förstudien finns 2023-10-09 en uppdaterad version av handlingsplan med tillhörande tidplan. Utifrån vad som framkommit hittills under förstudiearbetet beräknas projektet pågå fram till halvårsskiftet 2026.

Handlingsplanen redovisar pågående och planerade åtgärder utifrån dataskyddsombuds årsrapport 2022 och Stadsrevisionens rapport 2022 kopplat till informationssäkerhet.

Förvaltningen återkommer i december 2023 med uppdatering av handlings- och tidplan.

Bedömning ur ekonomisk dimension

Handlingsplanen hanteras inom ramen för förvaltningens budget 2023.

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).

Samverkan

Ärendet samverkas med de fackliga representanterna i FSG 2023-10-19.

Bilagor

1. Tidplan Etablera processer och arbetssätt för informationssäkerhet
2. Nämnden för Intraservice 2023-08-31 § 158
3. Nämnden för Intraservice 2023-06-21 § 126
4. Nämnden för Intraservice 2023-02-22 § 43
5. Bildspel 2023-10-26

Ärendet

Nämnden för Intraservice beslutade 2023-02-22 § 43 att ge förvaltningen i uppdrag att ta fram en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022. Nämnden för Intraservice har att ställning till godkännande av denna handlingsplan.

Beskrivning av ärendet

Dataskyddsombudets årsrapport 2022 innehåller förbättringsförslag kopplade till de brister som årsrapporten redovisar gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Förvaltningen har tidigare presenterat en översiktlig handlingsplan, senast under augusti månad 2023 inför möte med nämnden för Intraservice.

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 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 påbörjats inom förstudien finns 2023-10-09 en uppdaterad version av handlingsplan med tillhörande tidplan (se bilaga 1). Utifrån vad som framkommit hittills under förstudiearbetet beräknas projektet pågå fram till halvårsskiftet 2026. Handlingsplanen redovisar pågående och planerade åtgärder utifrån dataskyddsombuds årsrapport 2021 och 2022 och Stadsrevisionens rapport 2022.

Projektet har idag identifierat 26 antal arbetspaket och uppskattat tids- och resursåtgång för åtgärder inom de arbetspaket som startat och beräknas starta under 2023. Arbete med att arbeta med att ta fram tids- och resursuppskattningar för övriga arbetspaket kommer att fortsätta och förvaltningen återkommer i december med uppdaterad handlings- och tidplan. Utifrån vad som framkommit hittills 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 kommer att ta 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. Riktlinjer och rutiner, samt processer och arbetssätt kommer hjälpa till med att beskriva arbetsuppgifter kopplade till informationssäkerhet/dataskydd.

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

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket AnsvarRollerMandat.

Status 2023-10-01

Datum för start av arbete med denna kontrollpunkt är i projektplanen satt till 2023-10-26. 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.

Nästkommande steg är att tydliggöra roller, ansvar och mandat kopplade till informationssäkerhet (inkl. dataskydd) och utbilda alla medarbetare inom förvaltningen i vilket ansvar och mandat som följer med den roll som medarbetaren har. Varje medarbetare inom förvaltningen behöver förstå vad som krävs av denne utifrån alla typer av styrande regelverk (lagar, förordningar, styrande dokument, etcetera)

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.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket AnsvarRollerMandat: 2023-10-26 – 2024-06-30.

Tidsuppskattning dataskyddsorganisation

Cirka 3 024 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 2023-10-09

Datum för start av arbete med denna kontrollpunkt är planerat till 2024-02-01. Resultat från tidigare efterfarenhetsgenomgångar efter incidenter kommer att utgöra material in till arbetet med att förbättra incidenthanteringsprocessen.

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

Åtgärder kopplade till personuppgiftsincidenter beräknas vara genomförda i mars/april 2024.

Tidsuppskattning personuppgiftsincidenter

Cirka 2 900 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 genomlys 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.

Status 2023-10-09

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

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

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

Arbetet med att genomlys och föreslå förbättringar i processer och arbetssätt beräknas vara slutfört i sin helhet i juni 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 och Stadsledningskontoret.

Status 2023-10-09

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 kommer att återupptas efter semesterperioden.

Arbete med att ta fram kravspecifikation tillhörande systemstöd är påbörjat.

Under projektet kommer flera processer och arbetssätt att genomlysas och det kommer att föreslås förändringar som även inkluderar uppdatering av personuppgiftsregister.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Systemstöd (inkl. PU-reg):
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.

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 projektets huvudpaket Ledningsprocess.

Arbetet kommer att utföras i dialog med Stadsledningskontoret med mål att anvisningar, rutiner och instruktioner ska användas av förvaltningar och bolag inom Göteborgs stad.

Status 2023-10-09

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.

De åtgärder som ingår i huvudpaketet Ledningsprocess är prioriterade, och rekommenderas startas upp parallellt med arbetet inom huvudpaket AnsvarRollerMandat.

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 strategier som inkluderar dataskydd. Exempelvis Informationssäkerhetsstrategi, IT-säkerhetsstrategi, Strategi tillhörande fysisk säkerhet, Molnstrategi, 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 kommer därtill arrangera 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.

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

Åtgärder kommer att genomföras inom ramen för projektets huvudpaket Utbildning.

Status 2023-10-09

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 startar upp efter semesterperioden 2023. I övrigt kommer utbildningsinsatser att genomföras inom projektet allteftersom implementation sker av uppdaterade/nya styrande dokument, processer och arbetssätt.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Utbildning: 2023-09-01 – 2026-06-30.

Tidsuppskattning utbildning

Hittills uppskattad tid: cirka 4 100 timmar. Ej medräknat är den insats som utbildningsdeltagare behöver bidra med.

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.

Status 2023-10-09

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.

Tidsuppskattning integritetspolicy

Tidsuppskattning 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 2023-10-09

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 där svar ännu inte har erhållits.

Införande av funktionalitet för gallring av chattmeddelanden i Teams införs 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 planerat till 2024-02-01.

Beräknad tidsperiod för åtgärder kopplade till huvudpaket Tekniskt arkivansvar: 2024-02-01 – 2026-06-30.

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).

Arbetet kommer att utföras i dialog med Stadsledningskontoret med mål att anvisningar, rutiner och instruktioner ska användas av förvaltningar och bolag inom Göteborgs stad.

Status 2023-10-09

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.

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 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 2023-10-09

Datum för start av arbete med denna kontrollpunkt är planerat till 2023-10-01.

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, Projekt, Systemstöd, Riskhantering och Omvärldsbevakning.

Arbetet kommer att utföras i dialog med Stadsledningskontoret med mål att anvisningar, rutiner och instruktioner ska användas av förvaltningar och bolag inom Göteborgs stad.

Status 2023-10-09

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 Registrerades rättigheter.

Status 2023-10-09

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.

Tidsuppskattning hantering av registrerades rättigheter

Tidsuppskattning påbörjad dock ej slutförd.

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.

Status 2023-10-09

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 har återupptagits under oktober 2023 och beräknas pågå fram till 2025-06-30.

Tidsuppskattning särskilda iakttagelser 2021

Fortsatt arbetet med dokumentation av personuppgiftsbehandlingar och säkerhetsåtgärder i tjänstespecifikationer och funktionsbeskrivningar uppskattas till cirka 3 600 timmar.

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.

Status 2023-10-09

Initiala samverkansmöten med Stadsledningskontoret är genomförda.

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

Tidsuppskattning ej ännu genomförd. Arbete med denna kontrollpunkt kommer inte att hanteras inom projektet.

Förändring

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 tillhörande genomförandet av projektet

Projektet har genomfört riskanalys och bland annat identifierat risker utifrån den ekonomiska situationen som råder inför verksamhetsåren 2024 och 2025. Det är risker som kan komma att påverka projektets möjligheter att genomföra identifierade åtgärder kopplade till dataskyddsombuds rapport 2021 och 2022, och Stadsrevisionens rapport 2022.

Det kan röra sig om risk för att resurser i form av expertstöd (konsulter) inte finns att tillgå, eller att rekrytering av egen personal inte är möjlig, utifrån tillgång till ekonomiska medel.

Expertstöd i form av sex konsulter kommer att bemanna upp projektet från och med 2023-09-01. Behov finns av att rekrytera egen personal till både projektaktiviteter (konsultväxling) och kommande förvaltning av det som projektet ska producera i form av processer, arbetssätt och styrande dokument.

Det är av stor vikt att det som projektet producerar kan lämnas över för förvaltning och vidareutveckling. Om inte så sker, kommer Intraservice att åter igen stå inför det faktum att genomförda åtgärder inte får den effekt som var planerad. Projektet refererar till konsultinsatser och andra typer av utvecklingsinsatser som genomförts under några års

tid. Ett arbete som genomförts, men som inte är slutfört eller som inte förvaltats eller vidareutvecklats och som nu är oanvändbart till stora delar.

I övrigt ses risker i att projektaktiviteterna är omfattande i både tidsåtgång och komplexitet, vilket påverkar Intraservice förmåga att leva upp till gällande krav (de granskningskriterier som ligger bakom Stadsrevisionens rapport 2022, dataskyddsombuds rapport 2022 samt nya styrande dokument, nya lagar och förordningar) och Intraservice förmåga att förhindra och hantera incidenter, nu och en tid framöver.

Framgångar

Det arbete som utförts sedan senaste återrapporteringen i augusti har gett tydligare bild över åtgärder, omfattning, tids- och resursåtgång. Handlingsplanen och tidsplanen har uppdaterats. Dialoger med resursägare är påbörjade. Prioritering av åtgärder i handlingsplanen genomförs utifrån 1) behov och 2) efterfrågan

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 bland annat för arbete med informationsklassning, riskanalyser, konsekvensbedömningar, med mera). Ett sådant arbetssätt ses som kostnadseffektivt och kvalitetshöjande för alla parter.

Förvaltningens bedömning

Förvaltningen föreslår nämnden att anta handlingsplan med datum 2023-10-09 innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022.

Förvaltningen återkommer i december månad 2023 med ytterligare uppdatering av handlings- och tidsplanen.

Stina Hall Hellqvist
Avdelningschef för styrning och stöd

Peter Söderström
Förvaltningsdirektör