

Tjänsteutlåtande

Utfärdat 2024-02-16

Diarienummer 0104/23

Handläggare

Anna-Lena Björk

Telefon: 079 060 61 82

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

Handlingsplan kopplat till brister i kontrollområde som framkommer i dataskyddsenhetens årsrapport 2023

Förslag till beslut

I nämnden för Intraservice

Anta handlingsplan innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023.

Sammanfattning

Dataskyddsombuds 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.

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, 2022 och 2023, samt Stadsrevisionens rapport 2022.

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 2024-02-28.

Bilagor

Bildspel 2024-02-16

Ärendet

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

Nämnden för Intraservice har att ställning till godkännande av aktuell handlingsplan daterad 2024-02-16.

Beskrivning av ärendet

Dataskyddsbuds 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 dataskyddsbuds årsrapport 2022. De åtgärder som tas upp denna handlingsplan möter även upp mot de brister som tas upp i dataskyddsbuds årsrapport 2023.

Kontrollpunkterna i Dataskyddsbuds 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 dataskyddsbuds 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 2024-02-16

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. Arbete med framtagande av material är påbörjat kopplat till arbete med informationsklassning och riskanalyser. Praktiskt test/utvärdering kommer att ske internt Intraservice med start i februari 2024. 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.

Kommande 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)

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 – 2024-12-31.

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 2024-02-16

Datum för start av arbete med denna kontrollpunkt är 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 Q3 2024.

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 genomlysa 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 2024-02-16

Datum för start av arbete med denna kontrollpunkt är 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 genomlysa 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 2024-02-16

Dokumentation av personuppgiftsbehandlings- 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. Arbete med att ta fram kravspecifikation tillhörande systemstöd pågår. Business Case planeras vara klara under mars/april 2024.

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.

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 personuppgiftsbehandlings- 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 2024-02-16

Arbetet med denna kontrollpunkt startade upp 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 har startats upp parallellt med arbetet inom huvudpaket AnsvarRollerMandat. Plan är framtagen för vilka leveranser som kommer att ske. Det finns beroenden till andra huvudpaket inom projektet vilket medför att leveranser kommer genomföras löpande under projektets gång.

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”, 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 2024-02-16

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. 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: 2023-10-01 – 2026-06-30.

Tidsuppskattning utbildning

Hittills uppskattad tid: cirka 5 200 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 2024-02-16

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 2024-02-16

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 sker 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 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 genomlys 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 2024-02-16

Arbetet med denna kontrollpunkt startade 2023-10-01. Arbete uppstartat med initiala dialoger med bland andra ansvarig för inköpsprocessen och representanter för Intraservice kvalitets- och processutveckling.

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 genomlysas 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 2024-02-16

Arbete med denna kontrollpunkt startade upp 2023-10-01. Förslag till innehåll i process för informationsklassning och riskanalys, med tillhörande anvisningar, är framtagna och kommer att testas internt Intraservice med start under februari 2024. Fortsatt arbete är planerat.

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.

Status 2024-02-16

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 2024-02-16

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

Dataskyddsombud 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.

Arbete tillhörande Dataskyddsorganisation pågår, liksom arbete med register över personuppgiftsbehandlingar och förvaltningens informationsplikt.

Förvaltningens/bolagets bedömning

Förvaltningen föreslår nämnden att anta handlingsplan med datum 2024-02-16 innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023.

Stina Hall Hellqvist

Peter Söderström

Avdelningschef för styrning och stöd

Förvaltningsdirektör