

Tjänsteutlåtande

Utfärdat 2023-03-08

Diarienummer 0120/22

Handläggare

Anna-Lena Björk, CISO – Enhetschef IT-säkerhet

Telefon: 079 060 61 83

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

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

Förslag till beslut

I nämnden för Intraservice

Anteckna att en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022 är påbörjad.

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 gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Den handlingsplan som ligger till grund för pågående och planerade åtgärder utifrån dataskyddsombuds årsrapport 2021 och 2022 kommer kontinuerligt att uppdateras under 2023 med information om planerade start och sluttider.

Uppdatering kommer att ske i samband med att förstudier och förvaltningsövergripande prioritering och planering genomförs. Förvaltningen återkommer under juni månad 2023 med uppdaterad handlingsplan/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 aktiviteter 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 EU och har bland annat till syfte att skapa en enhetlig och likvärdig nivå av skyddet av personuppgifter. Dataskyddsförordningens engelska benämningen är General Data Protection Regulation (GDPR).

Samverkan

Ärendet samverkans med förvaltningssamverkansgruppen 2023-03-23.

Bilagor

Tjänsteutlåtande 2023-03-08

Bilaga 1 Nämnden för Intraservice 2023-02-22 § 43

Ärendet

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.

Beskrivning av ärendet

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 gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Årsrapport för dataskyddsarbete 2021 och 2022 presenterar båda resultat av fasta kontrollpunkter för Intraservice, samt särskilda iakttagelser. Kontrollerna redovisas tillsammans med förklaring i tabell.

Kontrollpunkt	Förklaring
Kontrollpunkt 1: Dataskyddsorganisation	Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.
Kontrollpunkt 2: Personuppgiftsincidenter	Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftsincidenter.
Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.
Kontrollpunkt 4: Personuppgiftsregister	Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett

Kontrollpunkt	Förklaring
	uppdaterat och heltäckande personuppgiftsregister innefattas.
Kontrollpunkt 5: Övergripande strategi för dataskydd	Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.
Kontrollpunkt 6: Utbildning	Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.
Kontrollpunkt 7: Integritetspolicy	Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.
Kontrollpunkt 8: Mejl och dokumenthantering	Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.
Kontrollpunkt 9: Konsekvensbedömning/samråd	Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.
Kontrollpunkt 10: IT-projekt och upphandling	Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.
Kontrollpunkt 11: IT-system och digitala verktyg	Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa

Kontrollpunkt	Förklaring
	system/tjänster uppfyller kraven på dataskydd ingår.
Kontrollpunkt 12: Hantering av registrerades rättigheter	Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.
Särskilda iakttagelser 2021: Tredjelandsoverföring och användning av sociala medier	Personuppgiftsbehandlingar vid användning av sociala medier som innebär tredjelandsoverföring.
Särskilda iakttagelser 2021: Intracustomer ansvar som personuppgiftsbiträde	I samverkan med parter inom Göteborgs Stad tydliggöra ansvarsförhållande och Intracustomer del av leverantörskedjan och roll i staden.
Särskilda iakttagelser 2022: Utredning av Intracustomer personuppgiftsansvar i nya styrmodellen	I samverkan med parter inom Göteborgs Stad tydliggöra ansvarsförhållande för de personuppgiftsbehandlingar som ingår i tjänster/system som är gemensamma för flera förvaltningar/bolag inom Göteborgs Stad.

I årsrapport för dataskyddsarbete 2021 ges rekommendation att fokusera på kontrollpunkterna 1, 4, 5, 6, 7, 8 och 9. Förvaltningen rekommenderas även vidta åtgärder för att hantera de rekommendationer som lämnats med anledning av förvaltningens ansvar som personuppgiftsbiträde och tjänsteleverantör åt övriga förvaltningar och bolag inom Göteborgs Stad. I årsrapport för dataskyddsarbete 2022 ges rekommendation att fokusera på kontrollpunkterna 1, 4 och 5.

Handlingsplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2021 och 2022

I tabell nedan anges status för respektive kontrollpunkt från dataskyddsenheten årsrapport 2021 och 2022.

Status anges som initierad, delvis eller klart. Med initierad avses att förvaltningen tagit upp aktiviteter i uppdragsdirektiv, men arbete är inte påbörjat. Med delvis avses att arbete pågår. Med klart avses att samtliga aktiviteter kopplade till aktuell kontrollpunkt är klarmarkerad.

En tidplan där det framgår när aktiviteter startar och planeras att vara slutförda kommer att kunna presenteras allt eftersom förstudier blir klara och förvaltningsövergripande prioritering och planering genomförs.

Förvaltningen återkommer under juni månad 2023 med uppdaterad handlingsplan/tidplan.

Förstudier

Förstudie 1: Ett uppdrag pågår sedan februari 2023 relaterat till *Kontrollpunkt 4: Personuppgiftsregister*. Initialt sker ett arbete inom ramen för en så kallad ”pilot”. Arbete inom ”piloten” har som mål att dokumentera personuppgiftsbehandlingar för ett urval av tjänster. Ett urval av tjänster som valts ut med tanke på önskad lansering under 2023 av det nya intranätet *Digitala Navet*. Urvalet av tjänster utgörs av tjänster som det nya intranätet *Digitala Navet* bygger på. Tidsåtgången för arbetet med att dokumentera personuppgiftsbehandlingar för dessa tjänster följs upp. Informationen om tidsåtgången kommer att ligga till grund för tidsuppskattningen för det fortsatta arbetet med att dokumentera personuppgiftsbehandlingar för samtliga tjänster som Intraservice levererar. Intraservice levererar 89 tjänster. Preliminärt slutdatum för ”piloten” är siste april 2023.

Tidsåtgången för arbetet med att dokumentera personuppgiftsbehandlingar för tjänsterna inom ramen för ”piloten” kommer också att ligga till grund för tidsuppskattningen för att dokumentera personuppgiftsbehandlingar som sker utifrån förvaltningens egen användning av tjänsterna.

Med dokumentation av personuppgiftsbehandlingar avses att nuvarande dokumentation granskas och uppdateras, eller tas fram om dokumentation saknas.

I samband med dokumentation av personuppgiftsbehandlingar sker även dokumentation av säkerhetsåtgärder.

Förstudie 2: En kartläggning har skett av vilka åtgärder som behöver hanteras relaterat till kontrollpunkterna 1 – 3, 5 – 12, samt kontrollpunkt 4 avseende process och arbetssätt för säkerställande av systematiskt och kontinuerligt underhåll av förvaltningens personuppgiftsregister. En förstudie kommer preliminärt att starta upp under Q3 2023 för att identifiera tidsåtgång och resursbehov för dessa åtgärder.

Ovan anges att förstudie preliminärt kommer att starta upp under Q3 2023. Det är preliminärt så tillvida att beroende finns till tillgång av uppdragsledare och uppdragsdeltagare.

Årsrapport för dataskyddsarbete 2021	Status oktober 2022	Status mars 2023
Fasta kontrollpunkter	<i>Initierad</i> <i>Delvis (arbete pågår)</i> <i>Klart</i>	<i>Initierad</i> <i>Delvis (arbete pågår)</i> <i>Klart</i>

Kontrollpunkt 1: Dataskyddsorganisation	Initierad	Delvis • Via chefer internt inom förvaltningen sprida och förankra att arbetet med informationsförvaltning och dataskydd är integrerat i det generella informationssäkerhetsarbetet. • Uppdragsdirektiv med aktiviteter med mål att för förvaltningen ta fram dokumenterade arbetssätt och tydliggöra roller, ansvar och mandat för att ○ reglera hur styrningen av informationssäkerhetsarbetet ska ledas och återkopplas, dvs. skapa förutsättningar för att informationssäkerhetsfrågor hanteras i rätt forum, och beslut fattas på rätt nivå ○ ange hur uppföljning av informationssäkerhetsarbetet ska ske samt hur efterlevnaden ska säkerställas, ○ motverka ”stuprörseffekten” och ○ säkerställa att ansvaret för informationssäkerhet är känt och accepterat, samt ○ att det tydligt framgår hur informationsspridning ska genomföras ○ vart frågor och synpunkter ska riktas för att omhändertas på bästa sätt. • Samtliga aktiviteter som vidtas ska utformas så att det tar hänsyn till de krav, behov och lagstiftning som gäller för förvaltningen och de tjänster som levereras.
--	------------------	--

Kontrollpunkt 2: Personuppgiftsincidenter	Initierad	Initierad
Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	Initierad	Initierad
Kontrollpunkt 4: Personuppgiftsregister	Initierad	Delvis Ett uppdrag pågår sedan februari 2023 relaterat till <i>Kontrollpunkt 4: Personuppgiftsregister</i>. Initialt sker ett arbete inom ramen för en så kallad "pilot". Arbetet inom "piloten" har som mål att dokumentera personuppgiftsbehandlingar för ett urval av tjänster. Ett urval av tjänster som valts ut med tanke på önskad lansering under 2023 av det nya intranätet <i>Digitala Navet</i>. Urvalet av tjänster utgörs av tjänster som det nya intranätet <i>Digitala Navet</i> bygger på. Preliminärt slutdatum för "piloten" är sista april 2023. Intraservice levererar 89 tjänster. Arbetet med att dokumentera personuppgiftsbehandlingar för resterande 84 tjänster ska planeras i direkt följd med genomförd pilot. Planeringen kommer att utgå från tidsåtgången för de fem tjänsterna inom piloten. I direkt följd av arbetet med piloten kommer också planering att starta upp för dokumentation av personuppgiftsbehandlingar som sker utifrån förvaltningens egen användning av tjänster. Med dokumentation av personuppgiftsbehandlingar avses att nuvarande dokumentation granskas och uppdateras, eller tas fram om dokumentation saknas. I samband med dokumentation av personuppgiftsbehandlingar sker även dokumentation av säkerhetsåtgärder. Den dokumentation som tas fram ska, förutom att ligga till grund för uppdatering av

		förvaltningens personuppgiftsregister, vara tillgänglig för kund att tillgå i syfte ligga till grund för dennes egen riskanalys/konsekvensbedömning när det rör sig om förvaltnings/bolags användning av för Göteborgs Stad gemensamma tjänster/system. Dokumentation sker därav i Word/Excel-dokument i och med att det inte finns ett för Göteborgs Stad gemensamt systemstöd för denna typ av gemensamt informationsutbyte. Att dokumentation sker i Word/Excel-dokument ger utmaningar kring åtkomst av information, gallring, och förmåga att på ett enkelt sätt söka fram och hålla informationen uppdaterad och aktuell. Dialoger har inletts med representanter inom Stadsledningskontoret kring dessa utmaningar. Representanter inom förvaltningar/bolag är av informationssäkerhetschef informerade om pågående aktiviteter och de utmaningar som är knutna till förmedling och underhåll av information (2023-03-08 <i>Informationssäkerhetsdagen hos Stadsledningskontoret</i>).
Kontrollpunkt 5: Övergripande strategi för dataskydd	Initierad	Initierad
Kontrollpunkt 6: Utbildning	Initierad	Delvis Inom ramen för det arbete som utförs kopplat till kontrollpunkt 4 Personuppgiftsregister har medarbetare tagit del av utbildning. Utbildning har haft fokus på att ge information om vad en personuppgiftsbehandling är och hur dessa behandlingar kan identifieras och dokumenteras enligt en för Intraservice framtagna metodik. De medarbetare som deltagit i utbildningen har varit medarbetare som arbetar med de tjänster som ingår i ”piloten”.

		I direkt följd till arbetet med ”piloten” kommer flera och fler medarbetare att utbildas allt eftersom arbetet fortsätter med övriga tjänster. För ytterligare information se anteckningar tillhörande kontrollpunkt 4 Personuppgiftsregister. Andra typer av utbildningar (<i>med inriktning på informationssäkerhet/dataskydd/arkivansvar</i>) kommer att planeras in utifrån aktiviteter i övriga uppdrag inom förvaltningen under 2023 (<i>Etablera processer och arbetssätt tillhörande kontinuitetshantering, Etablera processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet, Omhändertagande av åtgärder utifrån interna analyser</i>).
Kontrollpunkt 7: Integritetspolicy	Initierad	Initierad
Kontrollpunkt 8: Mejl och dokumenthantering	Initierad	Initierad
Kontrollpunkt 9: Konsekvensbedömning/s amråd	Initierad	Initierad
Kontrollpunkt 10: IT-projekt och upphandling	Initierad	Initierad
Kontrollpunkt 11: IT-system och digitala verktyg	Initierad	Initierad
Kontrollpunkt 12: Hantering av registrerade rättigheter	Initierad	Initierad
Särskilda iakttagelser 2021: Tredjelandsoverföring och användning av sociala medier	Initierad	Initierad

Särskilda iakttagelser 2021: Intraservice ansvar som personuppgiftsbiträde	Initierad	Delvis Förvaltningens informationssäkerhetschef har under februari 2023 haft inledande dialoger med representanter inom Stadsledningskontoret. Utifrån dessa dialoger har ett arbete startats upp tillsammans med representanter från Stadsledningskontoret med syfte att samverka kring ansvar för de olika personuppgiftsbehandlingar som utförs inom de tjänster/system som är gemensamma för förvaltningar och bolag inom Göteborgs Stad. Samverkan kommer att behöva ske med flera parter såsom Demokrati och medborgarservice och Inköp och upphandling.
Särskilda iakttagelser 2022: Utredning av Intraservice personuppgiftsansvar i nya styrmodellen		Delvis Förvaltningens informationssäkerhetschef har under februari 2023 haft inledande dialoger med representanter inom Stadsledningskontoret. Utifrån dessa dialoger har ett arbete startats upp tillsammans med representanter från Stadsledningskontoret med syfte att samverka kring ansvar för de olika personuppgiftsbehandlingar som utförs inom de tjänster/system som är gemensamma för förvaltningar och bolag inom Göteborgs Stad. Samverkan kommer att behöva ske med flera parter såsom förvaltningen för Demokrati och medborgarservice och förvaltningen för Inköp och upphandling.

Förvaltningens bedömning

Förvaltningen föreslår nämnden att anteckna att en handlingsplan med tidplan för att omhänderta brister i kontrollområden som framkommer i dataskyddsenhetens årsrapport 2022 är påbörjad.

Förvaltningen återkommer under juni månad 2023 med uppdaterad handlingsplan/tidplan.

Anna-Lena Björk

CISO – Enhetschef IT-säkerhet IT

Malin Lundqvist

Verksamhetsområdeschef IT