

**Tjänsteutlåtande**

Utfärdat 2024-10-23

Diarienummer 0104/23

**Handläggare**

Anna-Lena Björk

Telefon: 079 060 61 82

E-post: [anna.bjork@intraservice.goteborg.se](mailto:anna.bjork@intraservice.goteborg.se)**Slutrapportering av handlingsplan utifrån dataskyddsombudets rapport 2023 samt uppdrag att etablera dataskyddsorganisation****Förslag till beslut**

I nämnden för Intraservice:

Slutrapporteringen av förvaltningens handlingsplan innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023 antecknas till protokollet.

**Sammanfattning**

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

Förvaltningen har tidigare presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsombuds årsrapport 2022 och 2023, senast i samband med Intraservice nämndmöte 2024-06-27. Förvaltningen återkommer nu med slutrapportering av handlingsplanen.

Inom kort kommer dataskyddsombudet att redovisa granskningsrapporten för verksamhetsåret 2024. Nya brister som eventuellt identifierats, samt kvarvarande brister och rekommendationer från tidigare granskningar, kommer att omhändertas av projektet Etablera systematiskt informationssäkerhetsarbete. Förslag på ny handlingsplan med åtgärder kommer att lyftas till nämnden för fastställande under början av 2025.

**Bedömning ur ekonomisk dimension**

Handlingsplanens aktiviteter hanteras inom ramen för förvaltningens budget 2024 och 2025.

**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**

Riskanalys som genomfördes under Q2 2024 har identifierat risker för att personer som innehar roller som avdelningschef, 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.

Aktiviteter pågår och är planerade tillhörande uppföljning av de i Q2 2024 identifierade riskerna.

### **Organisatorisk arbetsmiljö**

Riskanalys som genomfördes under Q2 2024 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 inom Intraservices alla avdelningar.

Risker finns fortfarande 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. Aktiviteter ska fortsatt initieras av Göteborgs Stads stadsledningskontor och inom denna en ny enhet där jurister och dataskyddsombud har sin hemvist. Aktiviteterna ska genomföras i samarbete med inom Intraservices utsedda resurser.

Ett annat exempel på otydlighet rör arkivansvaret kopplat till Intraservices leveranser av gemensamma tjänster och digital infrastruktur. Rekrytering pågår av resurs som ska stötta i arbetet med det som benämns som det tekniska arkivansvaret.

Fortsatt analys och framtagande av förslag till åtgärder kommer att ske, där hänsyn tas till behovet av att ytterligare ansvar kopplas till roller inom förvaltningen. Ytterligare ansvar kopplade till Intraservices systematiska informationssäkerhetsarbetet.

### **Samverkan**

Ärendet samverkas med de fackliga representanterna i FSG 2024-11-21.

### **Bilagor**

1. Bildspel - Åtterrapportering november 2024 av handlingsplan utifrån dataskyddsombudets rapport

## Ärendet

Förvaltningen har under 2023 och 2024 presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsbuds årsrapport 2022. De åtgärder som tas upp i denna handlingsplan möter även upp mot de brister som tas upp i dataskyddsbuds årsrapport 2023.

Nämnden för Intraservice har att ta ställning till godkännande av aktuell handlingsplan daterad 2024-11-06.

## Beskrivning av ärendet

Dataskyddsbuds årsrapport 2023 innehöll förbättringsförslag kopplade till de brister som årsrapporten redovisade gällande förvaltningens informationssäkerhetsarbete och följsamhet mot dataskyddsförordningen.

Förvaltningen har tidigare presenterat en handlingsplan kopplat till åtgärder till brister i dataskyddsbuds årsrapport 2022 och 2023, senast i samband med nämndens sammanträde 2024-06-27 § 111.

Förvaltningen återkommer nu med slutrapportering av handlingsplan.

Handlingsplanen utgörs av en för projektet *Etablera systematiskt informationssäkerhetsarbete* övergripande projektplan. Projektet *Etablera systematiskt informationssäkerhetsarbete* startade upp under 2023. Projektet beräknas pågå till och med juni månad 2026.

## Fasta kontrollpunkter

Nedan ges en redogörelse om vad respektive kontrollpunkt avser tillsammans med en beskrivning av vad som utförts och kommer att utföras inom ramen för projektet *Etablera systematiskt informationssäkerhetsarbete*.

### 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 arbete.

#### 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, och kommer att ta fram ytterligare 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 ska 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 har och kommer att genomföras inom ramen för projektets huvudpaket AnsvarRollerMandat.

### **Status 2024-11-06**

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

I samband med Intraservice nämndmöte juni 2024 fastställdes förvaltningens förslag till etablering av det som i dataskyddsombuds årsrapport 2023 benämns som dataskyddsorganisation. Ett förslag som inkluderar att Göteborgs Stad Intraservices befintliga roller får utökade och nya ansvar kopplade till aktiviteter tillhörande dataskydd, arkivansvar, tekniskt arkivansvar, informationsägarskap, riskägarskap, systemägarskap, informationsklassning och riskhantering.

Utbildningsaktiviteter har genomförts under perioden september – november, och kommer att fortsätta framöver.

Den typ av ansvar som ingår i det material som Intraservice nämnd fastställde juni 2024 utgör grunden till uppbyggnad av en organisationsstruktur med processer och arbetssätt som styr och stödjer arbetet med informationssäkerhet. Ett arbete som inkluderar aktiviteter kopplade till dataskydd. Dataskydd innefattar skydd av personuppgifter. Personuppgifter utgör en typ av information. Informationssäkerhet innefattar skydd av alla typer av information.

Dataskyddskontakter finns sedan 1 september placerade inom avdelningen för styrning och stöd och enheten för styrning och uppföljning av informationssäkerhet.

Dataskyddskontakter är så att säga en SPOC (Singel Point Of Contact) för alla typer av ärenden rörande dataskydd. Dataskyddskontakter är dem som kontaktar dataskyddsombud i ärenden där dataskyddsombud ska involveras.

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

## **Kontrollpunkt 2: Personuppgiftsincidenter**

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

### **Omfattning**

Projektet har och kommer även fortsättningsvis 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 2024-11-06**

Hantering kring kontaktvägar till personuppgiftsansvarig (PUA) inom 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. Lessons learned genomförs efter mer omfattande personuppgiftsincidenter.

Mallar och dokument har uppdaterats i syfte det ska bli tydligare att följa Integritetskyddsmyndighetens (IMYs) krav på dokumentation vid anmälan av personuppgiftsincident.

Utbildningar är genomförda. Detta har bland annat varit uppskattat av handläggare, vilka har erhållit kunskap om att dataskyddskontakt och koordinator av personuppgiftsincidenter (PUI-koordinator) ska kontaktas vid misstanke om personuppgiftsincident, samt att dataskyddskontakt är den som tar kontakt med dataskyddsombud.

Dokumentation kring hanteringen av personuppgiftsincidenter har uppdaterats så att den nu även omfattar brist på tillgänglighet (tillgänglighet enligt för kunden gällande Service Level Agreement (SLA)).

Fortsatt arbete med incidentprocessen och dess förgreningar till relaterade processer kommer att fortsätta. Bland annat kan nämnas att fortsatt arbete kommer att behandla det som ibland omnämns som ”säkerhetsincidenter”.

### **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 2024-11-06**

Leverans tillhörande denna kontrollpunkt är beroende av aktuell prioritering av aktiviteter inom projektet, och dels av pågående samverkan mellan Intraservice och Stadsledningskontoret i ärende rörande förslag om att Intraservice är att anse som

personuppgiftsansvarig för vissa behandlingar som utförs inom gemensamma tjänster och tjänster tillhörande digital infrastruktur.

Arbetet med att genomlysna och föreslå förbättringar i processer och arbetssätt kopplade till biträdesavtal och andra överenskommelser gällande dataskydd beräknas pågå under större delen av 2025 vara slutfört i sin helhet i december 2025.

## **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. Systemstöd är dock på gång att kunna levereras från Intraservice såsom en gemensam tjänst. Preliminär tid för produktionssättning är Q2 2025.

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 2024-11-06**

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 och arbete pågår. Det är ett omfattande arbete att ta fram dokumentation för samtliga tjänster och tjänsteerbjudande som Intraservice levererar till förvaltningar och bolag inom Göteborgs Stad. Det finns idag 85 tjänster och 182 tjänsteerbjudande.

Upphandling av ett för Göteborgs Stad gemensamt systemstöd (iFacts – även benämnt som Informationssäkerhetsdatabas (ISDB)) blev klar under juni 2024.

Implementationsarbete pågår och beräknas vara klart under Q1 2025. Därefter kan arbete med produktionssättning initieras. Produktionssättning kommer att påbörjas för några förvaltningar/bolag, för att sedan rullas ut successivt.

Intraservice kommer att vara en av de första förvaltningarna som kommer att starta upp sitt införandeprojekt, innebärande bland annat att förvaltningens personuppgiftsregister upprättas i systemstödet.

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. Denna tidsperiod är dock mycket preliminär. Beroenden finns till det för medarbetare dagliga operativa arbetet inom respektive tjänsteleverans.

## **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 2024-11-06**

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

Nämnden för Intraservices anvisning för informationssäkerhet, informationsklassning, riskhantering och autentisering och åtkomst fastställdes i juni 2024.

Arbete med framtagande av anvisningar pågår. Planerat är att ärende med förslag till fastställande av några ytterligare anvisningar ska lyftas till Intraservice nämnd i februari 2025. Därefter kommer arbete att fortsätta med framtagande av flera anvisningar.

Hittills har det uppskattats att behov finns av att projektet tar fram 31 anvisningar. Detta kan förändras om det upptäcks att ytterligare behov finns av anvisningar för specifika områden.

Anvisningarna samlas inom ramen för det som benämns som Intraservices InformationssäkerhetsFörfattningsSamling (IIFS).

<b>Anvisning</b>	<b>Status</b>
<b>IIFS 01 Anvisning för Informationssäkerhet</b>	Fastställd
<b>IIFS 02 Anvisning för Informationsklassning</b>	Fastställd
<b>IIFS 03 Anvisning för Riskhantering</b>	Fastställd
<b>IIFS 04 Anvisning för Autentisering och åtkomst</b>	Fastställd
IIFS 05 Anvisning för Hantering av tillgångar	
IIFS 06 Anvisning för Medvetenhet och utbildning inom informationssäkerhet	
IIFS 07 Anvisning för IT-användande	
IIFS 08 Anvisning för Rent Skrivbord och tom skärm	
IIFS 09 Anvisning för Hantering av mobila enheter	
IIFS 10 Anvisning för Kontinuitetshantering	Pågående
IIFS 11 Anvisning för Datalagring och Säkerhetskopiering	
IIFS 12 Anvisning för Skadlig kod och Antivirus	
IIFS 13 Anvisning för Ändringshantering	
IIFS 14 Anvisning för Hantering av Tredjepartsleverantörer	
IIFS 15 Anvisning för Ständig förbättring	
IIFS 16 Anvisning för Loggning och Övervakning	
IIFS 17 Anvisning för Nätverkssäkerhet	Pågående
IIFS 18 Anvisning för Dataöverföring	
IIFS 19 Anvisning för Säker Utveckling	
IIFS 20 Anvisning för Fysisk och miljömässig säkerhet	
IIFS 21 Anvisning för Hantering av Kryptografiska Nycklar	
IIFS 22 Anvisning för Kryptering	
IIFS 23 Anvisning för Dokumentation	
IIFS 24 Anvisning för Incidenthantering, Forensik och Insamling av Bevis	Pågående
IIFS 25 Anvisning för Patchhantering, sårbarhetshandling och konfigurering	
IIFS 26 Anvisning för Molntjänster	
IIFS 27 Anvisning för Immateriella rättigheter	
IIFS 28 Anvisning för Drift och Underhåll	
IIFS 29 Anvisning för HR och hantering av oegentligheter	
IIFS 30 Anvisning för Informationssäkerhet inom projektledning	Pågående
IIFS 31 Anvisning för Hotunderrättelser	



## Kontrollpunkt 6: Utbildning

Kontrollpunkt 6, Utbildning avser 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 för att säkerställa att personal är medveten om sitt ansvar tillhörande informationssäkerhet (inkl. dataskydd) och hur detta ansvar kan fullgöras.

Projektet arbetar med framtagande av lärarledda och online-utbildningar. 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 genom att höja medvetenheten och kompetensen samt etablera en säkerhetskultur genom att öka förståelsen för Intraservices behov.

Målet är att säkerställa att alla intressenter i identifierade målgrupper är utbildade och kompetenta utifrån vad roller och ansvar anger.

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 2024-11-06

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

Hittills har projektet lanserat sex (6) utbildningar:

- DISA för Intraservice
- Change Management
- Tjänstespecifikationer och funktionsbeskrivningar
- Informationsklassning (orientering)
- Informationsklassning (lärarledd)
- Riskhantering (lärarledd)

Arbete pågår med att ta fram utbildningar tillhörande

- Riskhantering (orientering)
- Kontinuitetshandling
- Informationssäkerhet för chefer
- Introduktion till AI-förordning

Utbildningarna är integrerade i ESI-projektet och anpassas efter implementationen av uppdaterade och nya styrande dokument, processer och arbetssätt. Förutom de

utbildningar som behandlar dokumentation av tjänsterna har utbildningar i informationsklassning och riskhantering lanserats i september i samband med att *Nämnden för Intraservices anvisning för informationsklassning* samt *Nämnden för Intraservice anvisning för riskbaserat informationssäkerhetsarbete* trädde i kraft. Utbildningar i informationsklassning visar hur vi tillämpar stadens klassningsmodell på Intraservice. Utbildningen i riskhantering syftar till att säkerställa att risker för informationssäkerhet identifieras och hanteras på ett strukturerat sätt och hur man genomför riskanalyser.

Utbildningar publiceras löpande i utbildningsportalen.

Följande utbildningar är planerade att färdigställas under Q1 – Q2 2025

- lärarledd utbildning om kontinuitetshantering för IT
- uppdaterad onlinekurs tillhörande dataskyddsförordningen på jobbet
- grundläggande säkerhetsutbildning online som ett alternativ till DISA
- lärarledd kurs om AI och säkerhet
- hantering av säkerhetsincidenter
- introduktion till NIS2-direktivet

### Hittills framtagna pågående utbildningar

Utbildning	Lansering	Deltagande (av 738 medarbetare)	Utbildningen riktar sig mot
Digital informationssäkerhetsutbildning för alla (DISA) för Intraservice - online	2024-03-29	210 (20%)	Alla medarbetare
Change management - online	2024-05-20	35 (4 %)	Alla medarbetare
Informationsklassning orienteringskurs - online	2024-09-02	41 (6 %)	Alla medarbetare
Informationsklassning för genomförare - lärarledd	2024-09-02	37 (5 %)	Samtliga chefer, Projektledare, Förvaltningsledare, Systemförvaltare och andra medarbetare som arbetar med ex. förändrings-/utvecklingsuppdrag och inköp.
Riskhantering för genomförare - lärarledd	2024-09-02	28 (2 %)	Samtliga chefer, Projektledare, Förvaltningsledare, Systemförvaltare och andra medarbetare som arbetar med ex. förändrings-/utvecklingsuppdrag och inköp.
Tjänstespecifikation - lärarledd	2024-03-02	100 (14%)	Förvaltningsledare, Systemförvaltare, Service Delivery Managers

## 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 2024-11-06

Några aktiviteter är påbörjade i samarbete med Stadsledningskontoret. Projektplanen anger att några aktiviteter tillhörande existerande Integritetspolicy väntar på att prioriteras och planeras in för omhändertagande under perioden december 2024 – januari 2025.

### Sammanfattning av pågående aktiviteter

Aktivitet	Status 2024-11-06	Förväntat utfall
Förändring av stadens anställningsavtal för att korrekt informera om de registrerades rättigheter (interna), hur deras personuppgifter används och hanteras inom Intraservice/Staden. Stadens nuvarande anställningsavtal saknar vitala delar om hur registrerades uppgifter hanteras.	Dialog med Göteborg Stads CISO, som ansvarar för att ärende lyfts till Göteborgs Stads HR	Förändring av stadens anställningsavtal utifrån hur hantering av personuppgifter sker inom Göteborgs Stad och de tjänster som förvaltningar och bolag använder sig av. Tidsplan till införande är svår att bedöma.
Införande av aktiviteter och åtgärder tillhörande existerande integritetspolicy samt dess nuvarande rutiner.  Detta sker via kartläggning av nuvarande rutiner samt dokumentera vilka åtgärder som behöver förändras/läggas till.	Analys pågår under införandefasen av systemstödet iFacts (ISDB) om hur registrerades rättigheter ska kommuniceras samt dokumenteras på ett korrekt sätt. Analysen inkluderar översyn av vilka aktiviteter och åtgärder som saknas idag utifrån målet att efterleva gällande integritetspolicy.	Efter kartläggning av existerande integritetspolicy ska identifikation ske av vilka aktiviteter och åtgärder som saknas utifrån målet att efterleva gällande integritetspolicy.
Analys av hur registrerade externa parter rättigheter kommuniceras och förvaltas	Analys pågår under införandet av systemstödet iFacts (ISDB) av hur nuvarande processer och rutiner fungerar för att tillvarata de externa registrerades rättigheter. Vilka processer och rutiner finns på plats, vilka åtgärder behöver vidtas för att på ett korrekt sätt informera	Efter kartläggning av existerande processer och rutiner ska kompletterande åtgärder och aktiviteter utföras med mål att efterleva GDPR och att de registrerades rättigheter kan kontrolleras ur ett efterlevnadsperspektiv (ELK). Detta kommer att ske under

	externa registrerade om deras rättigheter	införandefasen av systemstödet iFacts (ISDB).
--	---	---

## 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 ska genomföras 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 2024-11-06

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 har åter startats upp under oktober 2024.

## **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 2024-11-06**

Sedan hösten 2023 har arbete utförts tillsammans med bland andra ansvarig för inköpsprocessen, representanter för Intraservice kvalitets- och processutveckling samt processledare för förändringsprocessen (Change Management). Vissa justeringar och kompletteringar av berörda processer är utförda. Fortsatt arbete är och ska planeras. Fokus ligger nu under perioden Q4 2024 – Q2 2025 på arbetspaketet Projekt.

Inom arbetspaketet Projekt kommer flera typer av projekt att analyseras, exempelvis ”inköps- och utvecklings-projekt”. Processer och arbetssätt kommer att justeras och kompletteras med perspektiv på informationssäkerhet (inklusive dataskydd).

## **Kontrollpunkt 10: IT-projekt och upphandling**

Kontrollpunkt 10, IT-projekt och upphandling, avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

### **Omfattning**

Projektet kommer att genomlysas, föreslå och genomföra förändringar i relevanta processer med avsikt att säkerställa att arbetet inte går vidare förrän det är verifierat att relevanta informationssäkerhets-/dataskyddsfrågor är hanterade. Målet är att denna typ av

frågor hanteras i samband med nyutveckling, inköp/upphandling, förvaltning, förändring och avveckling av system och tjänster.

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 säkerhetskändelser 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.

I juni 2024 fastslog nämnden för Intraservice anvisning för informationssäkerhet, informationsklassning, riskhantering samt autentisering och åtkomst.

Inom projektets regi har utbildningar genomförts, och kommer att genomföras, tillhörande informationsklassning och riskhantering i syfte att öka medarbetares kunskap kring detta inför det att de kommer att delta i olika typer av aktiviteter såsom exempelvis IT-projekt och upphandlingar.

Aktiviteter som ska stärka upp processer och arbetssätt kopplade till hur projekt bedrivs pågår inom arbetspaketet Projekt. Preliminär tidsperiod för detta arbete är Q4 2024 – Q2 2025.

Inom arbetspaketet Teknisk säkerhet pågår arbete med framtagande av anvisningar som ska ge medarbetare stöd gällande kravställningar som behöver uppnås i samband med IT-projekt och upphandlingar.

Utifrån förändrade och kommande nya regelverk som påverkar inköps- och förändringsprojekt sker dialoger med förvaltningens egna jurister, men även med jurister stationerade inom Stadsledningskontoret.

Åtgärder kopplade till kontrollpunkten IT-projekt och upphandling beräknas på fram till 2026-06-30.

## **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 arbetet 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 2024-11-06**

Arbete med framtagande av tjänstespecifikationer och funktionsbeskrivningar för samtliga tjänster som Intraservice levererar till förvaltningar och bolag inom Göteborgs Stad pågår och beräknas preliminärt pågå fram till och med Q2 2025. Denna planering är preliminär och påverkas av det ordinarie arbetet som medarbetare behöver hantera.

Prioriterat är för närvarande arbete med arbetspaketet Projekt (Q4 2024 – Q2 2025) och Systemstöd (Q2 2024 – Q1 2025).

Aktiviteter som rör det som ryms inom arbetspaketet Säkerhetskontroller pågår likaså.

### **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 2024-11-06**

Projektplanen anger att aktiviteter tillhörande kontrollpunkt 12, hantering av registrerades rättigheter, inkl. översyn av existerande Integritetspolicy, väntar på att prioriteras och planeras in för omhändertagande.

## **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 2024-11-06**

Aktiviteter har genomförts kopplade till kontrollpunkt 1, Dataskyddsorganisation.

Nämnden för Intraservices fastslog i juni 2024 det förslag till dataskyddsorganisation som förvaltningen presenterade.

Gällande kontrollpunkt 4, Register över personuppgiftsbehandlingar, pågår ett flertal aktiviteter. Aktiviteter ska också planeras in under 2025, bland annat för att registrera in uppgifter i ett för förvaltningen nytt register över personuppgiftsbehandlingar.

Projektplanen anger att aktiviteter tillhörande kontrollpunkt 7, Informationsplikt, väntar på att prioriteras och planeras in för omhändertagande under perioden december 2024 – januari 2025.



**Uppskattad tidsåtgång och utförd tid tillhörande kontrollområden i dataskyddsbuds årsrapport 2023**

Kontrollpunkt	Status	Planerad tid (timmar)	Upparbetad tid (timmar)
01 Dataskyddsorganisation	Pågående	5 000	1 250
02 Personuppgiftsincidenter	Pågående	3 000	170
03 Biträdesavtal och andra överenskommelser	Ej påbörjad	-	-
04 Register över personuppgiftsbehandlingar	Pågående	2 000	1 200
05 Övergripande styrning av dataskyddsarbetet	Pågående	15 000	4 500
06 Utbildning	Pågående	5 000	500
07 Informationsplikt	Pågående	1 000	150
08 E-post och dokumenthantering	Ej påbörjad	-	-
09 Konsekvensbedömning/samråd	Pågående	2 000	250
10 IT-projekt och upphandling	Pågående	1 750	350
11 IT-system och digitala verktyg	Pågående	10 000	300
12 Hantering av registrerade rättigheter	Pågående	500	100
<b>Summa timmar</b>		45 250	8 770

**Uppskattad tidsåtgång och utförd tid inom projektet Etablera systematiskt informationssäkerhetsarbete (inkluderar timmar i tabell - Uppskattad tidsåtgång och utförd tid tillhörande kontrollområden i dataskyddsbuds årsrapport 2023)**

Huvudpaket	Status	Planerad tid (timmar)	Upparbetad tid (timmar)
01 Ansvar/Roller/Mandat	Pågående	3 000	750
02 Incident	Pågående	3 000	170
03 Informationsklassning	Klar	1 000	550
04 Inköp	Pågående	1 500	150
05 Kontinuitetshandling	Pågående	14 000	2 800
06 Identitet & Åtkomst	Pågående	1 500	120
07 Ledningsprocess	Pågående	3 500	500
08 Projekt	Pågående	2 500	200
09 Riskhantering	Pågående	2 500	680
11 Systemstöd (inkl. PU-register)	Pågående	2 000	1 200
12 Teknisk säkerhet (IT-säkerhet)	Pågående	5 500	700
13 Utbildning	Pågående	5 000	500
16 Personrelaterade Säkerhetsåtgärder	Pågående	100	20

17 Kund	Ej påbörjad	-	-
18 Tekniskt arkivansvar	Ej påbörjad	-	-
19 Drift och Förvaltning	Ej påbörjad	-	-
20 Efterlevnadskontroll	Pausad	5 000	300
21 Fysisk Säkerhet	Pågående	1 000	175
22 Change	Pausad	-	-
23 Request	Pausad	-	-
24 Utlämning	Ej påbörjad	-	-
25 Omvärldsbevakning	Pågående	1 750	50
27 Identifiera Tillgångar	Pågående	8 000	130
28 Asset Management	Pågående	-	150
29 Tjänstespecifikationer & Funktionsbeskrivningar	Pågående	3 600	2 300
30 Säkerhetskontroller	Pågående	1 000	130
<b>Summa timmar</b>		64 450	11 575

## Förvaltningens bedömning

Förvaltningen föreslår nämnden att anta slutrapportering av handlingsplan med datum 2024-11-06 innehållande åtgärder utifrån brister i kontrollområden som framkommer i dataskyddsombuds årsrapport 2023.

Handlingsplanen utgörs av en för projektet *Etablera systematiskt informationssäkerhetsarbete* övergripande projektplan. Arbete med aktiviteter inom ramen för projektet *Etablera systematiskt informationssäkerhetsarbete* startade upp under 2023. Projektet beräknas pågå till och med juni månad 2026.

Inom kort kommer dataskyddsombudet att redovisa granskningsrapporten för verksamhetsåret 2024. Nya brister som eventuellt identifierats, samt kvarvarande brister och rekommendationer från tidigare granskningar, kommer att omhändertas av projektet *Etablera systematiskt informationssäkerhetsarbete*. Förslag på ny handlingsplan med åtgärder kommer att lyftas till nämnden för fastställande under början av 2025.

Stina Hall Hellqvist  
Avdelningschef Styrning och stöd

Peter Söderström  
Förvaltningsdirektör