Stockholms stad

Bilaga 7
Dnr KS 2023/1237

Ledningens genomgång 2024

– informationssäkerhetsplan

Stadsledningskontoret

Ledningens genomgång är ett begrepp inom ledningssystemet för informationssäkerhet enligt standarden ISO 27001 som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad Ledningens genomgång, från informationssäkerhetssamordnaren.

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024* uppmanas samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhets-arbetet under de kommande tre åren. Denna ska biläggas verksamhetsplanen.

Innehållsförteckning

1 Ledningssystem för informationssäkerhet

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS.

Stockholms stads informationssäkerhetsarbete regleras i en riktlinje för informationssäkerhet som är en bilaga till stadens kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För stadsledningskontorets räkning har stadsdirektören fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas vid stadsledningskontoret.

För att kunna leda och styra arbetet med informationssäkerhet inom den egna verksamheten ska förvaltningschef minst årligen informera sig om hur arbetet går. Det sker genom att förvaltningschef inhämtar en rapportering som kallas *Ledningens genomgång* från informationssäkerhetssamordnaren. Ledningens genomgång innebär en genomlysning av informationssäkerhets-arbetet inom verksamheten och ska resultera i beslut om förbättringar inför nästkommande verksamhetsår. Rapporteringen ska även innefatta dataskydd utifrån vad som exempelvis framkommer i GDPR årsrapport, som årligen sammanställs av dataskyddsombudet för nämndens räkning.

2 Vad påverkar stadsledningskontorets informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska stadsledningskontoret ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering. Integritetsrisker behöver hanteras i enlighet med dataskyddslagstiftningen.

2.1 Vad händer inom staden – budget, inriktningar, lokala förändringar eller satsningar

Följande aktiviteter i förslag till budget 2024 kan komma att ge positiv påverkan för informationssäkerheten vid stadsledningskontoret:

- Kommunstyrelsen ska inleda arbetet med framtidssäkring av stadens löneadministrativa system LISA (3.4)
- Kommunstyrelsen ska se över och revidera stadens försörjningsstrategi för it-området med fokus på säkerhetsaspekter vid outsourcing och behov av intern kompetens (3.5)
- Kommunstyrelsen ska utreda behov och förutsättningar för en starkare uppföljning och kontroll över delar av gemensam service IT (3.5)

2.2 Risker som identifierats i GDPR årsrapport 2022 (med kommentar angående 2023)

Summeringen nedan utgår ifrån dataskyddsombudets GDPR årsrapport 2022.

Registerförteckning

En riktad insats utförs för att alla personuppgiftsbehandlingar inom kommunstyrelsens ansvarsområde ska bli registerförtecknade utifrån ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde.

Arbetsprocessen behöver sammanlänkas med arbetsprocessen för arkivredovisning, informationsklassning, riskanalys och konsekvensbedömning avseende dataskydd.

Styrdokument avseende dataskydd

En förstärkning av dataskyddsperspektivet i tillämpningsanvisning till stadens riktlinje för informationssäkerhet planeras för 2023. En lokal anvisning av informationssäkerhet har tagit fram under 2023. Under 2023 har tillämpningsanvisningarna uppdaterats och dataskyddsperspektivet förstärkts.

Implementering av tekniska och organisatoriska skyddsåtgärder och hantering av personuppgiftsincidenter

Ett viktigt område för integritetsskyddet är att tekniska och organisatoriska säkerhetsåtgärder är implementerade och att åtgärderna motsvarar gällande lagkrav. Tillhandahållande av stadsövergripande system och stadsgemensam it-infrastruktur medför att kommunstyrelsen har ett ansvar, både som personuppgiftsansvarig och personuppgiftsbiträde, för att korrekta tekniska och organisatoriska åtgärder är implementerade.

Rekommendationen i GDPR årsrapport 2021 om informationsklassningens prioritet har fått genomslag.

Tillhandahållandet av stadsövergripande system och stadsgemensam it-infrastruktur innebär att kommunstyrelsen har i uppgift att identifiera, dokumentera, hantera och skyndsamt informera övriga nämnder och bolagsstyrelser om personuppgiftsincidenter.

Positivt är att flertalet system eller tjänster där stadsledningskontoret är personuppgiftsansvarig och/eller personuppgiftbiträde har aktuella informationsklassningar.

Uppföljning ska ske avseende att personuppgiftsbehandlingar som enligt tillsynspraxis kräver kryptering har implementerad kryptering.

Metodik för riskanalys är beslutad och tillgänglig, ett viktigt komplement till informationsklassningen. Riskanalysmetodiken omfattar även personuppgiftsbehandling, där kan krypteringsfrågan med fördel adresseras.

Stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter har nyttjats och rutinen fyller sin funktion.

Stadens arbete med att etablera CERT är ännu i en inledande fas och än finns ingen lägesbild, varken statisk eller kontinuerligt uppdaterad, eller förmåga att upptäcka och identifiera personuppgiftsincidenter.

Konsekvensbedömning avseende dataskydd

Konsekvensbedömning avseende dataskydd är en lagreglerad bedömning och ska utföras när hög risk för individs integritet, rättigheter och friheter föreligger. Syftet med bedömningen är att förebygga risker för individ och personuppgiftsincidenter innan de uppkommer.

Uppdaterat metodstöd och mall för konsekvensbedömning avseende dataskydd har tagits fram under 2022. Dataskyddsombudet rekommenderade i GDPR årsrapport en behovskartläggning för kommunstyrelsen och att ett behov föreligger att ta fram en stadsövergripande process för referenskonsekvensbedömning avseende dataskydd för att förenkla och effektivisera efterlevnaden inom staden.

Konsekvensbedömningar avseende dataskydd har genomförts enligt befintligt metodstöd och då i konsultation med dataskyddsombudet enligt gängse rutin.

Då flera personuppgiftsansvariga nämnder och bolagsstyrelser inom staden använder stadsgemensamma och stadsövergripande it-tjänster behöver arbetet förenklas och samordnas. Dataskydds-vägledning pekar tydligt ut att flera personuppgiftsansvariga tillsammans med sitt personuppgiftsbiträde kan genomföra en gemensam konsekvensbedömning, referenskonsekvensbedömning, istället för flera enskilda bedömningar.

Individens rättigheter

EU-domstolen har kommit med flera domstolsavgöranden och Europeiska dataskyddsstyrelsen har tagit fram ny vägledning 2023 gällande rätten till tillgång. Med anledning detta behöver metodstöd uppdateras.

2.3 Informationssäkerhetssamordnares uppföljning av informationssäkerheten

Uppföljning av informationssäkerhet i samtliga objekt (t ex it-system)

Informationssäkerhetssamordnare följer upp samtliga objekt där stadsledningskontoret är personuppgiftsansvarig och/eller personuppgiftsbiträde. Objektägaren kan och behöver oftast ta stöd av objektledare it samt objektledare. Svaren sammanställs, analyseras och blir del av Ledningens genomgång inför kommande verksamhetsplaner.

Övriga reflektioner från ISAM kring informationssäkerheten vid stadsledningskontoret

De personuppgiftsbehandlingar som registerförtecknas i verktyget Wisma Draftit Records är väl dokumenterade. Information från registerförteckning kan nyttjas direkt i protokoll för informationsklassning och till PuB-avtalsinstruktionen. Registerförteckningen förenklar att uppfylla kraven om den obligatoriska informationsplikten gentemot individen vars personuppgifter behandlas. Genom registerförteckningen kan kartläggas vilka tredjelandsöverföringar som finns och vilka som kan behöva ses över om EU-kommissionens adekvansbeslut för Data Privacy Framework för USA förkastas av EU-domstolen. Samma resurseffektivitet kan uppnås gällande AI och IoT.

Stadsledningskontoret är PuA och/eller PuB för cirka 240 system varav cirka 117 av karaktär ”verksamhetssystem eller lagrar verksamhetsdata”. Det är särskilt viktigt att IoT och AI registerförtecknas utifrån personuppgiftsbehandlingen, då dessa verktyg behöver konsekvensbedömmas avseende dataskydd.

Informationsklassning

Av totalt cirka 240 system där SLK är PuA och/eller PuB har cirka 200 av dessa en informationsklassning från år 2020 eller senare.

Ett större arbete med informationsklassning genomfördes 2022 kring gemensam it, där cirka 130 system klassades. Klassnings-nivåerna skulle sannolikt bli högre när verksamhetssystemens kravbild inkluderas, men detta kan hanteras genom steget ”Riskanalys” där man kan väga in nytta gentemot kostnad. Konceptet kommer att utvecklas och implementeras under 2024.

Integritetsskyddet kräver att tekniska och organisatoriska åtgärder ska vara införda. Åtgärderna ska även testas, utvärderas och ha förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna.

Dagens lagstiftning kräver att incidenter ska kunna upptäckas, identifieras, hanteras och förebyggas. Vid incidenter ska även kort tidsram beaktas och anmälningsskyldighet till respektive tillsynsmyndighet. Tillämpningsanvisningen har 2023 förtydligats inom detta område.

Kontinuitetsplaner

- Tätare intern avstämning behöver ske kring var det saknas kontinuitetsplaner. Kontinuitetsplaner behöver övas och dess kvalitet behöver utvärderas och även följas upp.

Kravställning krävs från respektive objekt avseende systemtjänsteavtalet

- Nödvändig kravställning krävs kring vad som ska loggas avseende respektive objekt (it-tjänster) och hur länge dessa loggar sparas. Denna kravställning kan med fördel samordnas då lagkrav behöver beaktas, likaså hanteringsanvisningarna för arkivredovisningen.

Behörighetshantering

- Styrning och uppföljning av behörigheter behöver stärkas. Ansvarsrollerna Personuppgiftsansvarig och Personuppgiftsbiträde styr hur behörigheter utformas idag.
- Behörighetshanteringen sker på många olika sätt i staden och enhetliga rutiner kan med fördel tas fram.

AI

Erfarenheter och kompetens behöver byggas upp kring nyttjande av AI, avseende informationssäkerhet inklusive dataskydd. Erfarenheter behöver dras och samlas från realiserade lösningar inom och utanför staden.

IoT

Erfarenheter och kompetens behöver byggas upp kring nyttjande av IoT, avseende informationssäkerhet inklusive dataskydd. Erfarenheter behöver dras och samlas från realiserade lösningar inom och utanför staden.

2.4 Risk- och sårbarhetsanalys, RSA

Stadsledningskontoret har arbetat vidare med att stärka kontinuitetshanteringen med utgångspunkt i behov av åtgärder som identifierats i RSA-processen 2022-2023. En ny RSA-cykel inleds under 2024. Stadsledningskontoret följer stadens risk- och sårbarhetscykel och instruktioner.

2.5 Väsentlighets- och riskanalys (VOR) och internkontrollplan

Det interna kontrollarbetet utifrån kommunstyrelsens internkontrollplan 2023 har fortgått under året. Kontroll-aktiviteter respektive åtgärder utifrån väsentlighets- och riskanalys har följts upp. Inga väsentliga avvikelser har identifierats för perioden januari–augusti.

Processen Systematiskt informationssäkerhetsarbete var obligatorisk för samtliga nämnder att väsentlighet- och riskanalysera 2023, detsamma gäller inför 2024. Till processen hör fem obligatoriska arbetssätt: behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning och informationssäkerhet inom upphandlingsförfarandet.

3 Förbättringar för verksamhetens LIS

Den 31 oktober 2023 fastställde stadsdirektören stadsledningskontorets lokala anvisning för informationssäkerhet.

Den lokala anvisningen finns tillgänglig för alla medarbetare på intranätsidan Informationssäkerhet, på den ”lokala” delen av intranätsidan som gäller specifikt för stadsledningskontoret.

4 Prioritering av åtgärder

Lagstiftningen på digitaliseringsområdet och identifierade risker avseende informationssäkerhet och integritetsskyddet kan medföra att nedan kan komma att behöva revideras till viss del.

2024
Förvaltningen ska under 2024 följa upp att den lokala anvisningen följs, främst med fokus på att:

- Tillse att informationstillgångar är klassade och att handlingsplaner tas fram och implementeras.
- Uppdatera genomförda klassningar och att tekniska och organisatoriska åtgärder är genomförda.
- Genomföra fler sårbarhetsgranskningar av it-system.
- Kravställa för respektive it-system inom systemtjänsteavtalet. Kravställningen ska främja inbyggt dataskydd och dataskydd som standard.
- Se över metodstöd för registrerades rättigheter.

2025
Under 2025 ska stadsledningskontoret prioritera:

- Utifrån RSA säkerställa att kontinuitetsplaner finns. Förbättra förmåga att övervaka stadsledningskontorets it-infrastruktur (kontinuerligt kunna upprätthålla och agera på en lägesbild).
- Genomföra fler normerande informationsklassningar och referenskonsekvensbedömningar avseende dataskydd.
- Granska hur väl kravställda skyddsåtgärder från informationsklassningar och riskanalyser är implementerade.

2026
Under 2026 ska stadsledningskontoret prioritera:

- Revidering av lokal anvisning.
- Öva utifrån kontinuitetsplaner.