Ledningens genomgång år 2023

Farsta stadsdelsförvaltning

Beslutad 2023-11-21

Ledningens genomgång

Dnr: FAR 2023/834

Kontaktperson: Jenny Jonasson

1 Sammanfattning

Ledningens genomgång är ett begrepp inom informationssäkerhet 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. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschefer ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.[1]

I Anvisningar för nämndernas arbete med verksamhetsplan 2024[2] uppmanas samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplanen. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa Riktlinje för informationssäkerhet i Stockholms stad.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i nämndens verksamhetsplan under mål 3.5. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För 2024 är därför området registerförteckning och informationsklassning särskilt prioriterat i Ledningens genomgång.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

---

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet
[2] anvisningar-for-namndernas-arbete-med-verksamhetsplan-2024.pdf (stockholm.se)

Innehållsförteckning

2 Faktorer som påverkar verksamhetens LIS

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Farsta stadsdelsförvaltning 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.

2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

2.1.1 NIS 2

I slutet av 2022 beslutade EU om ett nytt direktiv som ska ersätta nuvarande NIS. Det nya direktivet har fått namnet NIS 2. De stora förändringarna i NIS 2 är följande:

- Fler sektorer av organisationer kommer att beröras
- Det kommer införas minimikrav för åtgärder
- Mer precisa rapporteringskrav kommer att implementeras

NIS 2 träder i kraft den 17 oktober 2024. Stadsdelsförvaltningen omfattas idag av NIS inom hälso- och sjukvård. I NIS 2 införs bland annat en ny sektor, offentlig förvaltning. Offentlig förvaltning kommer omfatta statliga myndigheter, men det är upp till varje medlemsstat om kommuner och regioner kommer att omfattas av detta. Regeringen har beställt en utredning om hur NIS 2 kommer att implementeras i Sverige. I februari 2024 kommer utredningen presenteras.

2.1.2 Adekvansbeslutet

I juli 2023 fattade EU-kommissionen ett nytt adekvansbeslut om tredjelandsöverföring till USA.
Den 10 juli fattade EU-kommissionen beslut om adekvat skyddsnivå för USA. EU-kommissionens beslut innebär att överföringar som sker till organisationer som omfattas av ”EU-US Data Privacy Framework” nu kan ske utan att lämpliga skyddsåtgärder, såsom standardavtalsklausuler, behöver vidtas enligt artikel 46 i dataskyddsförordningen. Mycket tyder på att

beslutet kommer att överklagas och rättsläget är därmed osäkert varför fortsatt försiktighet råder i avvaktan på detta.

2.1.3 AI

Utvecklingen av AI går fort och det finns stora möjligheter för verksamheten i och med det. Det finns också stora risker med användandet av AI och det kommer ställa höga krav på informationsklassningar och dataskyddsarbete för att hinna med i samma takt.

2.2 Vad påverkar Farsta stadsdelsnämnds informationssäkerhetsarbete?

2.2.1 Budget

I 2024 års budget framgår det att samtliga nämnder och bolagsstyrelser ska ta fram en *Ledningens genomgång* med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan.
En riskanalys ska genomföras för att identifiera vilka aktiviteter som ska prioriteras till år 2024. Dessa aktiviteter ska redovisas både i *Ledningens genomgång* samt i nämndens verksamhetsplan under mål 3.5.
För 2024 är området registerförteckning och informationsklassning särskilt prioriterat i *Ledningens genomgång*. Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

2.2.2 Vad har verksamheten identifierat i RSA-arbetet

Ett samarbete mellan säkerhetssamordnare och informationssäkerhetssamordnare kommer att inledas under våren 2024 för att få med informationssäkerhet i RSA-arbetet.

2.2.3 Resultatet från egen uppföljning (VoR och IKP)

2.2.3.1 Väsentlighet- och riskanalys

I väsentlighet- och riskanalysen finns nedanstående indikatorer från SLK samt hur stadsdelsförvaltningen har arbetat med dem under 2023.

Behörighetshantering
Identitet och åtkomst är ett av de högst prioriterade områdena i stadens informationssäkerhetsarbete. Det är därför viktigt att nämnder/styrelser har en tydlig rutin för identitet- och åtkomst. Under 2023 har stadsdelsförvaltningen arbetat med att ställa krav på att det ska finnas rutiner för hur behörigheter ska hanteras för de informationstillgångar som har klassats. Det kommer under 2024 diskuteras hur stadsdelsförvaltningen på bästa sätt kan arbeta med behörighetshantering. Under 2025 kommer rutin för behörighetshantering som rör tilldelning, ändring och borttagning samt uppföljning att tas fram.

Implementering av lokal anvisning
Förvaltningschef ska för nämndens/styrelsens räkning fastställa en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten.
Den lokala anvisningen är beslutad av stadsdelsdirektör och har implementerats genom att den har skickats ut till chefer och den har tagits upp i de obligatoriska utbildningarna i informationssäkerhet och dataskydd för chefer som genomfördes våren 2023.

Incidenthantering
Nämnder och styrelser ska etablera en lokal rutin för hur incidenter ska hanteras i den egna verksamheten. Det är förvaltningschef som är ansvarig för att verksamheten antagit en lokal incidentrutin. I rutinen ska framgå vilka roller som har vilket ansvar sett till incidenthanteringen, exempelvis ansvar för att registrera en incident eller för att följa upp vidtagna åtgärder.
Under 2023 har rutinen för personuppgiftsincidenter uppdaterats och en rutin för NIS-incidenter har tagits fram. Implementering av rutinen har skett genom utbildningar i informationssäkerhet och dataskydd för chefer och för informationssäkerhets- och dataskyddshandläggare. Rutinerna har publicerats i förvaltningens gemensamma dokumentbibliotek och finns tillgängliga för alla anställda i organisationen.

Informationsklassning
När verksamhetens information kartlagts ska en informationsklassning genomföras för att bestämma informationens värde. Det är informationsägaren som ansvarar för att verksamhetens krav på informationssäkerhet fastställs genom en informationsklassning samt att resultatet från klassningen tas om hand och efterlevs. Det ska ske regelbunden uppföljning av att klassningens krav efterlevs samt att de implementerade kraven fortfarande är tillräckliga.
Under 2023 har förvaltningen arbetat fram ett fungerande samarbete för informationsklassning, som bland annat består av funktionerna informationssäkerhetssamordnare, dataskyddsombud, IT-strateg och IT-samordnare. Verksamheterna har också deltagit i klassningarna. Det har under 2023 genomförts 12 klassningar och 3 tidigare genomförda klassningar har följts upp.

Informationssäkerhet inom upphandlingsförfarande
Informationssäkerhetsarbete är en viktig förutsättning för att stadens verksamheter ska lyckas väl med anskaffning eller utveckling av varor och tjänster. Det är därför viktigt att se över och implementera informationssäkerhetsarbete i verksamhetens processer för anskaffning och utveckling av varor och tjänster som ska användas för informationshantering i Stockholms stad. Varje nämnd/styrelse behöver säkerställa att informationssäkerhet kommer in i ett tidigt skede i förarbetet inför anskaffning eller utveckling av varor och tjänster för att säkerställa att rätt krav uppfylls.
Under 2023 har det anställts en upphandlings- och inköpssamordnare som är väl insatt i att vid upphandlingar av varor och tjänster behöver informationssäkerhet tas i beaktande. Under 2026 planeras det göras en översyn av detta arbete och en rutin kommer tas fram.

2.2.3.2 Interkontrollplan

I internkontrollplanen för 2023 fanns nedanstående kontroller med som rör informationssäkerhet.

Kontroll av enheternas genomförande av e-utbildningar
Under 2023 har de obligatoriska e-utbildningarna för informationssäkerhet och dataskydd certifierats. Det gör att alla har registrerats som att de har gått utbildningarna under året. Under 2024 kommer det kunna följas upp vilka som har gått respektive inte har gått dem.

Kontroll av enheternas rutiner för informations- och personuppgiftshantering
Under 2023 har stickprovskontroller genomförts på enheternas rutiner för informations- och personuppgiftshantering. Det har konstaterats att enheterna har kännedom om, och tillämpar, förvaltningens centrala rutiner vad gäller dessa delar. Däremot finns det ett behov av att integrera dem i verksamhetens övriga rutiner.

Kontroll av GDPR-följsamhet
Under 2023 har det genomförts stickprovskontroller på enheternas kännedom om registrerades rätt till information genomförts. Kontrollen visar att det finns god kännedom om informationskravet och efterlevnad av detsamma.

2.2.4 Resultatet från revisioner

Nämnden rekommenderas att säkerställa ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med bestämmelserna i NIS och stadens riktlinjer. Nämnden rekommenderas att säkerställa att incidentrapporter för verksamhet som omfattas av NIS delges stadsledningskontorets informationssäkerhetsfunktion. Revisionskontoret har även följt upp den granskning av nämndens arbete med att implementera dataskyddsförordningen som genomfördes år 2019. Uppföljningen visar att nämnden behöver fortsätta arbeta för att säkerställa att förordningen och stadens riktlinjer efterlevs. Sammantaget visar de båda granskningarna att nämnden behöver fortsätta att utveckla sitt arbete inom informationssäkerhetsområdet.

Nämnden rekommenderas att utveckla styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen. Rekommendation kvarstår. Nämnden rekommenderas att informationsklassa sina informationstillgångar samt regelbundet och systematiskt inventera sina personuppgiftsbehandlingar. Nämnden rekommenderas att genomföra en kartläggning av behovet av personuppgiftsbiträdesavtal.

Granskningen visar att nämnden har identifierat de verksamheter, funktioner och system som står under NIS-direktivets krav, men att organisation och arbetssätt för informationssäkerhetsarbetet fortfarande befinner sig i en etableringsfas. Arbetet kan i dagsläget således inte anses systematiskt och riskbaserat i en sådan utsträckning som NIS och stadens riktlinjer kräver.

Hösten 2022 gjordes en revision om hur staden följer NIS-direktivet. Farsta stadsdelsförvaltning var en av tre stadsdelsförvaltningar som valdes ut i granskningen. Stadsledningskontoret har sekretessbelagt resultatet av revisionen, vilket gör att vi inte kan få ta del av resultatet.

2.2.5 Risker som identifierats i GDPR-årsrapport

Stadsdelsförvaltningens registerförteckning är ofullständig, dels att flertalet behandlingar saknas, dels att de behandlingar som finns registrerade är bristfälliga.
Interna rutinerna är bristfälliga, framför allt inom säkerställandet av individens rättigheter.
Få informationsklassningar och konsekvensbedömningar är gjorda.

2.2.6 Information om avvikelser (incidenter och andra händelser)

Under 2023, till och med 2023-10-31, har det inkommit 3 anmälningar om NIS-incidenter. Antalet personuppgiftsincidenter är 15 stycken.

3 Förbättringar som föreslås för verksamhetens LIS

3.1 Under 2024 ska Farsta stadsdelsförvaltning

Genomföra informationsklassning
Under 2024 ska Farsta stadsdelsförvaltning informationsklassa verksamhetsprocesser som omfattas av NIS. Stadsdelsförvaltningen kommer att delta i de normerande klassningarna i samarbete med objektförvaltningen.

I och med övergången från det nuvarande GSIT-avtalet till stadens nya systemtjänsteavtal för Lokala system behöver all data i de system som berörs vara informationsklassad. För Farsta stadsdelsförvaltning gäller det endast ett system.

Följa upp gjorda klassningar
Uppföljning av klassningar som är gjorda sedan tidigare kommer att ske årligen.

Fortsatt inventering av informationstillgångar
En inventering av stadsdelsförvaltningens informationstillgångar har gjorts under 2023. Under 2024 kommer den ses över ifall det behöver kompletteras med fler informationstillgångar.

Registerförteckning
Ny struktur ska genomföras under 2024. Syftet är att förenkla och tydliggöra för de registrerade och verksamheten hur vi behandlar personuppgifter. Genom att ha fler nämndgemensamma registreringar minskar vi också administrationen på enhetsnivå. Utbildning för de som registrerar behandlingar kommer att genomföras och praktiskt stöd kommer finnas tillgängliga. Genom övergången kommer det också bli tydligare att identifiera eventuella luckor som finns i registreringen idag.

Under 2023 har en ny rutin för årlig inventering av registerförteckningen tagits fram. Syftet är att tydliggöra ansvar och behovet av årlig inventering. Rutinen kommer att implementeras under 2024.

Utbildningsinsatser för chefer och medarbetare
I januari 2024 kommer två nya e-utbildningar att lanseras. Båda består av 8 avsnitt som kommer att släppas under året. Varje avsnitt tar ca 5-10 minuter att genomföra. Dessa kommer att vara obligatoriska. Chefen gör utbildningen själv medan medarbetarnas utbildning ska göras tillsammans på t ex ett enhetsmöte eller APT. En handledning kommer finnas tillgänglig då syftet är att medarbetare ska reflektera tillsammans. Dessa utbildningar kompletterar befintliga och ambitionen är att dessa ska ge ett stöd i hur medarbetare och chefer ska jobba, hur man omsätter vad som befintliga e-utbildningar redovisar.
En gång per år kommer även en fysisk obligatorisk utbildning för nyanställda chefer att hållas.

Uppföljning av rapportering av NIS-incidenter och personuppgiftsincidenter
Under hösten 2023 utbildade informationssäkerhetssamordnare och dataskyddsombud sjuksköterskor och chefer på två vård- och omsorgsboenden om hur rapportering av NIS-incidenter och

personuppgiftsincidenter ska ske. Under 2024 kommer stadsdelsförvaltningen följa upp hur rapporteringen fungerar.

Rutin för uppföljning av informationssäkerhetsincidenter
Under 2023 har rutin för personuppgiftsincidenter uppdaterats samt rutin för NIS-incidenter har tagits fram. 2024 kommer stadsdelsförvaltningen att ta fram en rutin för hur förvaltningen ska följa upp informationssäkerhetsincidenter.

Uppdatera Lokal anvisning
Lokal anvisning kommer att ses över årligen och uppdateras vid behov.

Implementering av PM3
Under 2023 har en kartläggning av samtliga system och tjänster samt objektindelning och tillsättning av roller enligt PM3 genomförts. Detta är ett pågående arbete. Under 2024 kommer arbetet att fortgå med vidare arbete med ytterligare kartläggning av objektens komponenter, samt utveckling av styrstrukturen samt implementering av process för anskaffning av nya tjänster och system.

Årshjul för informationssäkerhet och dataskydd
Under 2024 kommer ett årshjul för informationssäkerhet och dataskydd att tas fram. Syftet är att det ska underlätta för berörda chefer och medarbetare när under året de behöver lägga resurser på området.

3.2 Under 2025 ska Farsta stadsdelsförvaltning

Genomföra informationsklassning
Under 2025 ska informationsklassning ske rörande verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter. Stadsdelsförvaltningen kommer att delta i de normerande klassningarna i samarbete med objektförvaltningen.

Följa upp gjorda informationsklassningar
Uppföljning av klassningar som är gjorda sedan tidigare kommer att ske årligen.

Utbildningsinsatser för chefer och medarbetare
Utöver de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd som finns på Utbildningsportalen kommer det en gång per år hållas en fysisk obligatorisk utbildning för nyanställda chefer.

Uppdatera Lokal anvisning
Lokal anvisning kommer att ses över årligen och uppdateras vid behov.

Översyn av behörighetshantering
Förvaltningsövergripande rutin för behörighetshantering som rör tilldelning, ändring och borttagning samt uppföljning kommer att tas fram under 2025.

Översyn av hantering av skyddade personuppgifter
En översyn kommer att göras över hur skyddade personuppgifter hanteras på stadsdelsförvaltningen. Översynen kommer att resultera i en rutin.

3.3 Under 2026 ska Farsta stadsdelsförvaltning

Genomföra informationsklassning
Under 2026 ska informationsklassning ske rörande verksamhetsprocesser som är prioriterade enligt RSA. Stadsdelsförvaltningen kommer att delta i de normerande klassningarna i samarbete med objektförvaltningen.

Följa upp gjorda informationsklassningar
Uppföljning av klassningar som är gjorda sedan tidigare kommer att ske årligen.

Uppdatera Lokal anvisning
Lokal anvisning kommer att ses över årligen och uppdateras vid behov.

Utbildningsinsatser för chefer och medarbetare
Utöver de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd som finns på Utbildningsportalen kommer det en gång per år hållas en fysisk obligatorisk utbildning för nyanställda chefer.

Översyn av informationssäkerhet vid upphandling
En översyn av informationssäkerhet vid upphandling kommer att göras 2026. Implementering av informationssäkerhetsarbetet i verksamhetens processer för anskaffning och utveckling av varor och tjänster kommer att införas, så att det blir enkelt för verksamheterna att få med informationssäkerhet vid upphandling.

Dokumentet är fastställt av stadsdelsdirektör Gunilla Ekstrand, 2023-11-21