Ledningens genomgång år 2023

Järva stadsdelsförvaltning

Beslutad [2023-11-28]
Reviderad 2023-12-04

Ledningens genomgång

Dnr: JÄRVA 2023/710

Kontaktperson: Julia Jonsson, informationssäkerhetssamordnare

1. Sammanfattning

Ledningens genomgång är en helhetsbild för den nuvarande situationen för informationssäkerhetsarbetet på Järva stadsdelsförvaltning. Genomgången ska ge information och underlag till stadsdelsdirektören att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Sammanläggningen mellan Rinkeby-Kista och Spånga-Tensta stadsdelsförvaltningar har tagit en stor del av verksamhetens tid, samtidigt har ordinarie verksamhet pågått. Informationssäkerhetsarbetet har präglats av inventeringar från föregående stadsdelsförvaltningar, planering av hur Järva stadsdelsförvaltnings organisation kring informationssäkerhetsarbete ska se ut, vilka aktiviteter som ska prioriteras och vilka lärdomar vi tar med från föregående stadsdelsförvaltningar.

En av lärdomarna är att förvaltningen behöver arbeta fram en bättre struktur för att ta hand om de informationssäkerhetsklassningarna som förvaltningen deltar i med andra förvaltningar (normerande eller gemensamma informationssäkerhetsklassningar) och de egna informationssäkerhetsklassningarna som genomförs. Framförallt behöver förankringsarbetet med stadsdelsdirektör och avdelningschef, som i slutändan ska godkänna klassningarna, förtydligas.

Medan sammanläggningsarbetet har pågått har ordinarie verksamhet haft behov av IT-tjänster för effektivare arbetssätt som har uppstått löpande samt introducerat nya arbetssätt som behöver riskbedömas. Förvaltningen har noterat att IT-tjänster introduceras inom staden, där normerande informationssäkerhetsklassning saknas. Detta går ut över stadsdelens verksamheter då en informationssäkerhetsklassning ta lång tid att genomföra, och därmed riskerar att försena och komplicera förvaltningarnas införandearbete. Detta leder till att förvaltningar använder tjänsterna på olika sätt inom staden, vilket skickar olika signaler till medarbetare som riskerar att använda IT-tjänster på ett osäkert sätt.

Inom Järva stadsdelsförvaltning planeras följande aktiviteter 2024:

- Informationssäkerhetsklassning av lokala system
- Informationssäkerhetsklassning av nya it-tjänster som verksamheten behöver
- Delta i normerande informationssäkerhetsklassningar
- Nya obligatoriska e-utbildningar

- Ta fram en plan för införandet av pm3-modellen
- Se över rutin för registerutdrag och inventera personuppgiftsbehandlingar
- Stärka medarbetares kunskap om dataskydd på medborgarkontoren
- Uppdatera de lokala tillämpningsanvisningarna

Aktiviteter under 2025

- Implementera nytt incidentrapporteringsverktyg
- Fortsatt implementering av pm3-modellen
- Ta fram metod/arbetssätt för att följa upp informationssäkerhetsklassningar systematiskt
- Informationssäkerhetsklassa informationstillgångar
- Inventering av personuppgiftsbehandlingar
- Revidera lokala tillämpningsanvisningarna

Aktiviteter under 2026

- Genomföra övning inom verksamheter som berörs av NIS-direktivet, t.ex. nätverksbortfall eller dataförlust
- Genomföra övning för ledningsgrupp t.ex. antagonistisk cyberattack
- Slutföra implementering av pm3-modellen
- Informationssäkerhetsklassa informationstillgångar
- Inventering av personuppgiftsbehandlingar
- Revidera lokala tillämpningsanvisningarna

Innehållsförteckning

1. Sammanfattning 3

1.2 Vad är Ledningens genomgång 6

1.3 Faktorer som påverkar verksamhetens LIS 6

1.3.1 Omvärldsbevakning – hot, trender och ny lagstiftning 6

1.3.2 Vad händer inom staden – budget, inriktningar, lokala förändringar eller satsningar 9

1.3.3 Vad har verksamheten identifierat i RSA-arbetet 13

1.3.4 Resultatet från egen uppföljning (VoR och IKP) 13

1.3.5 Resultatet från revisioner 15

1.3.6 Risker som identifierats i GDPR-årsrapport 16

1.3.7 Information om avvikelser (incidenter och andra händelser) 16

1.4 Förbättringar som föreslås för verksamhetens LIS 17

1.4.1 Aktiviteter för 2024 17

1.4.2 Aktiviteter för 2025 18

1.4.3 Aktiviteter för 2026 19

1.2 Vad är Ledningens genomgång

Ledningens genomgång är en helhetsbild för den nuvarande situationen för informationssäkerhetsarbetet på Järva stadsdelsförvaltning och syftar till att informera ledningsgruppen om det arbetet som har gjorts, vilka risker som finns och åtgärder som kvarstår från det gångna året. Genomgången ska ge information och underlag till stadsdelsdirektören att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

I den här rapporten är det endast det övergripande informationssäkerhetsarbetet som beskrivs. Efterlevnad av dataskyddsförordningen följs upp i dataskyddsombudets årsrapport för dataskydd (GDPR-årsrapport) som biläggs nämndens verksamhetsberättelse för 2023. Ledningens genomgång kommer att redogöra kort vad GDPR-årsrapporten för 2022 kom fram till.

Förvaltningen arbetar utifrån Stockholms stads (stadens) riktlinjer som även utgör det övergripande ledningssystemet för informationssäkerhet (LIS). Riktlinjerna grundar sig i sin tur på standarden ISO 27000, som är ett globalt ramverk för bästa praxis om informationssäkerhetshantering[1]. I stadens riktlinjer beskrivs bland annat ansvarsfördelningen i nämndernas och styrelsernas organisationer.

1.3 Faktorer som påverkar verksamhetens LIS

1.3.1 Omvärldsbevakning – hot, trender och ny lagstiftning

1.3.1.1 Säkerhetsläget i Sverige i förhållande till omvärlden

Vi lever i en digital värld där digitaliseringen har länge varit vägen framåt för nya möjligheter och effektivitet. I vår ambition att utvecklas och vara innovativa så har mycket gott kommit ur digitaliseringen så som att tillgängliggöra information till fler människor, enklare att kommunicera och större möjlighet att koppla upp sig på nätet var man än befinner sig för att handla mat, uträtta bankärenden, arbeta eller skicka ett meddelande till sin familj.

Möjligheterna är oändliga, och med det finns det illvilliga som utnyttjar de möjligheter digitaliseringen erbjuder till sin fördel för att uppnå sina mål på bekostnad av den enskilda. Offentlig och

[1] https://www.informationssakerhet.se/stod--vagledning/standarder-for-informationssakerhet/ledningssystem-for-informationssakerhet/ 2023-02-06

privat sektor kan även de utsättas för antagonistiska attacker som kan innebära information röjs, ekonomisk skada eller förhindrar organisationerna att bedriva sina verksamheter.

Spännvidden mellan angriparna är stor när det kommer till mål, resurser och metoder men alla nätverk och enheter som är uppkopplade mot internet är potentiella vägar in i organisationen eller in i den enskildas privatliv.[2]

Rysslands invasionskrig föregicks av cyberangrepp mot statliga myndigheter och infrastruktur i Ukraina, och är fortsatt en del av deras krigsföring i kriget som pågår just nu. Även ideologiska aktörer har valt sida i kriget mellan Ryssland och Ukraina, och har angripit andra stater som inte deltar i kriget direkt så som Finska riksdagen, som utsattes för en överbelastningsattack som svar på landets natoansökan.[3] Det är därför inte helt osannolikt att även cyberattacker riktas mot Sverige som har under lång tid samarbetat med Nato, tagit ställning mot Rysslands invasion och dessutom också inväntar besked om ett inträde i Natoalliansen.

Andra internationella uppmärksammade händelser i Sverige påverkar stater och ideologiskt motiverade hotaktörer så som koranabränningarna. Därutöver gjorde Ryska och Turkiska aktörer gemensam sak för att angripa svenska intressen genom att utlösa dessinformationsattacker[4].

Desinformationskampanjen som handlade om LVU blev särskilt påtagligt för förvaltningens verksamhet i dåvarande Rinkeby-Kista och Spånga-Tensta stadsdelsförvaltningars socialtjänst. I Försvarshögskolans rapport LVU-kampanjen beskrivs det att desinformation om socialtjänstens arbete har spridits under flera år i sociala medier och andra plattformar på nätet, men att det var under 2022 som kampanjen fick ett internationellt genomslag.

Den 8 februari 2023 gick Säkerhetspolisen ut med ett pressmeddelande där de bedömde att hotbilden mot Sverige hade blivit sämre i samband med koranabränningarna, LVU-kampanjen samt det försämrade säkerhetsläget i omvärlden.[5]

---

[2] Nationellt cybersäkerhetscenter (ncsc.se) 2023-11-30
[3] Nationellt cybersäkerhetscenter (ncsc.se) 2023-11-30
[4] https://www.aftonbladet.se/nyheter/a/EQzrm2/ryska-och-turkiska-hackare-samverkade-efter-koranbranningen 2023-11-30
[5] https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2023-02-08-sverige-i-fokus-for-allvarliga-hot.html 2023-11-30

1.3.1.2 Nationellt cybersäkerhetscenter (NCSC)

I Nationellt cybersäkerhetscenters (NCSC) årliga rapport för 2022[6] beskriver de att de vanligaste hotaktörerna är statliga aktörer, kriminella och i viss omfattning även av ideologiskt motiverade aktörer, såsom hacktivister.

Avsaknaden av ett strukturerat säkerhetsarbete kan få stora konsekvenser för en verksamhet så som skadat förtroende, verksamheten kan behöva ligga nere tillfälligt, ekonomisk skada och enskilda kan drabbas.

Vanliga sårbarheter som tas upp i rapporten är bland annat

- Brister i behörighetshantering
- Ej administrerad och hanterad utrustning ansluts till nätverket
- Ingen organisation eller kunskap för incidentupptäckt och hantering

NCSC beskriver även de brister som är vanligt förekommande hos myndigheter i Sverige bland annat:

- lågt engagemang i säkerhetsfrågor
- otydligt ansvar och ägarskap för säkerhetsfrågor
- bristfällig hot- och riskanalys
- information är inte korrekt inventerad och klassificerad
- brister i avtal med leverantörer och deras underleverantörer om sekretess, kontrollmöjligheter och andra hanteringsregler

En brist som särskilt lyfts i rapporten är anställdas kompetens inom cybersäkerhet. NCSC uppmanar arbetsgivare att öka sina insatser för att rekrytera, utveckla och behålla personal med denna kompetens. Att utveckla egna utbildningsprogram eller köpa utbildningar, samt att kontinuerligt vidmakthålla kompetensen för att följa teknikutvecklingen är kostsamt men nödvändigt. En femtedel av de allvarliga IT-incidenter som rapporterats under 2019 till myndigheten för samhällsskydd och beredskap (MSB) av statliga myndigheter bedöms ha sin grund i handhavandefel. Anledningen till kompetensbristen menar de är bland annat att verksamheten inte arbetar systematiskt med att identifiera sina skyddsvärden eller att säkerhetsskyddsklassificera sin information.

1.3.1.3 NIS 2-direktivet

NIS-direktivet som antogs den 6 juli 2016 syftade till att förbättra den inre marknadens funktion[7] för att uppnå en hög gemensam nivå

[6] Nationellt cybersäkerhetscenter (ncsc.se) 2023-11-30

[7] Den inre marknaden innebär fri rörlighet för tjänster, varor, personer och kapital inom den europeiska unionen. För att säkerställa att den inre marknadens funktion

för säkerhet i nätverk och informationssystem inom unionen. NIS-direktivet omfattar leverantörer av samhällsviktiga tjänster inom privat och offentlig sektor. Dessa områden anses vara samhällsviktiga enligt NIS-direktivet:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Leverans och distribution av dricksvatten
- Digital infrastruktur

Direktivet ställer krav på leverantörerna att vidta säkerhetsåtgärder för att hantera risker och incidenter i nätverk och informationssystem som de är beroende av för att kunna erbjuda tjänsterna.[8] Järva stadsdelsförvaltning är en leverantör av samhällsviktiga tjänster inom området hälso- och sjukvård.

NIS 2-direktivet är ett nytt direktiv som kommer omfatta fler områden än dessa sju som räknades upp här ovan, alltså offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. Direktivet håller på och utreds, där utredaren bland annat tittar på om kommuner (offentlig förvaltning) ska omfattas av det nya direktivet och där med fler verksamhetsområden inom kommunerna.

Vad utredningen kommer fram till redovisas senast den 23 februari 2024[9].

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

1.3.2.1 Sammanläggningen av Rinkeby-Kista och Spånga-Tensta stadsdelsnämnder

I budgeten för 2023 beslutades det att stadsdelsnämnderna Rinkeby-Kista och Spånga-Tensta ska läggas samman till en nämnd och bilda Järva stadsdelsnämnd.

---

inte sätts ur spel antas regler som ska harmonisera staternas arbetssätt och främja den fria rörligheten.

[8] Dir. 2023:30, https://regeringen.se/contentassets/77a6664e7064451c8616caef98fd6961/genomforande-av-eus-direktiv-om-atgarder-for-en-hog-gemensam-cybersakerhetsniva-i-hela-unionen-och-eus-direktiv-om-kritiska-entiteters-motstandskraft.pdf 2023-11-13

[9] https://regeringen.se/rattsliga-dokument/kommittedirektiv/2023/03/dir.-202330 2023-11-13

Sammanläggningen är en process som kommer att pågå flera år framöver för att arbeta ihop organisationerna till en organisation. I ett informationssäkerhetsperspektiv så har följande fokusområden identifierats under 2023 års arbete med sammanläggningen:

- Inventering av informationssäkerhetsklassningarna.
- Sammanfoga de två registren över personuppgiftsbehandlingarna till ett register.
- Anta lokala tillämpningsanvisningar för informationssäkerhetsarbetet.
- Starta upp lokalt nätverk för informationssäkerhet och dataskydd.
- Lägga samman digital och analog information från föregångarna på ett kontrollerat sätt samt säkerställa att informationen är tillgänglig för medarbetare efter sammanläggningen den 1 juli.

Inventering av informationssäkerhetsklassningar

En inventering över informationssäkerhetsklassningar som har genomförts i de tidigare nämnderna gjordes i samband med sammanläggningen. Föregående stadsdelsförvaltningar har deltagit vid så kallade normerande informationssäkerhetsklassningar eller gemensamma informationssäkerhetsklassningar med andra förvaltningar i staden.

Tanken med underlaget från de gemensamma klassningarna är att varje förvaltning ska göra en egen bedömning utifrån sina behov och hur förutsättningar.

Många underlag som har framkommit i inventeringen saknar godkännande från stadsdelsdirektör eller avdelningschef. Det är därför svårt att säga om informationssäkerhetsklassningarna har förankrats hos stadsdelsdirektör eller avdelningschef.

En tydligare process för hur en informationssäkerhetsklassning ska gå till behöver tas fram, så att det säkerställs att de personer som ska godkänna informationssäkerhetsklassningar vet vad de godkänner och att klassningen förankras i verksamheten på ett strukturerat sätt.

Ta fram ett register över personuppgiftsbehandlingar för Järva stadsdelsförvaltning

Registerna av personuppgiftsbehandlingar från föregångarna har tagits om hand, bearbetats och sammanfogats till ett sammanhållet register. Idag består registret av ungefär 160 personuppgiftsbehandlingar. Sammanställningen är ett underlag

som ska granskas djupare under 2024 för att säkerställa att uppgifterna om registreringarna är korrekta och aktuella.

Anta lokala tillämpningsanvisningar
Den tilltänka ledningsgruppen för Järva stadsdelsförvaltning var redan tillsatt i februari 2023, och kunde anta de lokala tillämpningsanvisningarna för Järvas arbete med informationssäkerhet i juni.

En kommunikationsplan för att göra de lokala tillämpningsanvisningarna kända i organisationen har inte tagits fram på grund av tidsbrist. En plan ska tas fram för uppdateringen av anvisningarna under 2024.

Starta upp lokalt nätverk för informationssäkerhet och dataskydd
Ett lokalt nätverk för informationssäkerhet och dataskydd har under hösten startats upp. Informationssäkerhets- och dataskyddsambassadörerna (IDA) har fått en introduktion om området och om de aktiviteter som nätverket kommer att arbeta med löpande enligt det årshjul som har tagits fram för förvaltningens informationssäkerhetsarbete i tillämpningsanvisningarna.

Projektgrupper för att säkerställa föregångarnas informationstillgångar
Det fanns flera delprojekt som ansvarade för att genomföra sammanläggningen. De delar som handlar om stadsdelsförvaltningarnas information omhändertogs i tre olika projekt; Arkiv och juridik, IT samt Sociala system. Samtliga delprojekt är avslutade och har gått över till ordinarie verksamhet.

Många gemensamma mappar samt samarbetsytor finns kvar som användes i de föregående stadsdelsförvaltningarna. En särskild aktivitet för att säkerställa att informationstillgångarna omhändertas på rätt sätt ska genomföras i nätverket för informationssäkerhet och dataskydd.

1.3.2.2 Pågående informationssäkerhetsklassningar
Medan sammanläggningsarbetet har pågått har ordinarie verksamheten haft behov av IT-tjänster för effektivare arbetssätt som har uppstått löpande eller nya arbetssätt som behöver riskbedömas. En tendens som har varit är att IT-tjänster introduceras inom staden, där normerande informationssäkerhetsklassning saknas. Vilket ställer krav på de förvaltningar som vill använda tjänsterna att själva genomföra en grundlig informationssäkerhetsklassning utan något underlag från

leverantör som beskriver hur de skyddar informationen eller hur ansvarsförhållandena mellan staden och it-leverantörerna TietoEvry och/eller Fujitsu ser ut. Detta går ut över stadsdelens verksamheter då en informationssäkerhetsklassning ta lång tid att genomföra, och riskerar att förlänga och komplicera införandearbetet. Detta leder i sin tur till att förvaltningar inom staden gör olika bedömningar i klassningarna, och vissa förvaltningar använder IT-tjänsterna utan någon informationssäkerhetsklassning. Detta skickar olika signaler till medarbetare som riskerar att använda IT-tjänster på ett osäkert sätt.

1.3.2.3 Reviderat inriktningsbeslut avseende tredjelandsöverföringar till USA

Under 2021 fattade SLK ett inriktningsbeslut gällande tredjelandsöverföring och användning av amerikanska molntjänster i staden (KS 2021/581). I korthet så handlar beslutet om att inga nya tjänster som innebär tredjelandsöverföringar av personuppgifter införs i den stadsgemensamma digitala arbetsplatsen. Pågående avtal där tredjelandsöverföring förekommer och där personuppgiftsansvarig inte kan införa kompletterande skyddsåtgärder som innebär att personuppgiftsbiträdet kan ge tillräckliga garantier för en lagenlig personuppgiftshantering rekommenderas att senast inför nästa licensperiod finna alternativ som uppfyller lagstadgade krav.

Den 10 juli 2023 fattade EU-kommissionen beslut om adekvat skyddsnivå för USA. Beslutet innebär att överföringar som sker till organisationer som omfattas av ”EU-US Data Privacy Framework” nu kan ske utan att lämpliga skyddsåtgärder behöver vidtas enligt artikel 46 i dataskyddsförordningen.

I det reviderade inriktningsbeslutet (KS 2023/241) så uppmanas stadens förvaltningar och bolag att vidta generell försiktighet gällande införanden av några amerikanska molntjänster då beslutet inte bygger på amerikanska lagändringar utan en presidentorder. En presentorder kan upphävas av en ny eller sittande president med omedelbar verkan. Ramverket som beslutades om har inte heller prövats i domstol. Ramverket är inte heller obligatoriskt utan frivilligt för amerikanska leverantörer att ansluta sig till. En sista faktor som lyfts i SLK:s inriktningsbeslut är att staden i så stor utsträckning som möjligt bör se till att verksamhetskritisk

information ligger inom organisationens egen kontroll och inte under främmande makt.[10]

De molntjänster som används idag där viss tredjelandsöverföring förekommer är i den pedagogiska verksamheten i Järva stadsdelsförvaltning, där Microsofts tjänster och Teams används. Utbildningsförvaltningen som ansvarar för den pedagogiska verksamhetens it-leverans, har sedan tidigare beslutat om att fortsätta att använda dessa tjänster för att de är så viktiga för att verksamheten ska fungera.[11]

1.3.3 Vad har verksamheten identifierat i RSA-arbetet

En risk och sårbarhetsanalys har genomförts i de föregående stadsdelsförvaltningarna för samtliga verksamheter där man har tagit hänsyn till bortfall av el, telefoni och nätverk, men inte särskilt för den nya organisationen. En ny analys kommer att genomföras för Järva stadsdelsförvaltnings samtliga verksamheter under 2024.

1.3.4 Resultatet från egen uppföljning (VoR och IKP)

1.3.4.1 Uppföljning av de obligatoriska e-utbildningarna

Informationssäkerhet
1125 av 2457 medarbetare har genomför utbildningen (2023-11-21)
Dataskydd: 1096 av 2457 medarbetare har genomfört utbildningen (2023-11-21)

1.3.4.2 Tydliggöra hur vi använder sociala medier

I sociala medier rör sig stockholmarna därför behöver även förvaltningen finnas där för att kommunicera och nå ut med vår verksamhet. De stora plattformarna domineras av amerikanska företag så som Facebook som även äger Instagram. Med stadens inriktningsbeslut i åtanke, där återhållsamhet av överföring av information till USA framhålls, så behöver förvaltningen ta fram en strategi för hur verksamheterna ska använda sociala medier. Förvaltningen har ännu inte tagit fram en strategi, men planeras att påbörja detta arbete under 2024.

---

[10] https://intranat.stockholm.se/globalassets/nyheter/stadsledningskontoret/dokument/pm-reviderat-inriktningsbeslut-tredjelandsoverforingar-beslutad.docx 2023-11-14

[11] https://intranat.stockholm.se/nyheter/utbildningsforvaltningen/kommentar-till-inriktningsbeslut-for-molntjanster/ 2023-11-21

1.3.4.3 Incidenthantering – Kompetenshöjande insatser gällande NIS inom hälso- och sjukvård

Som en del av incidenthanteringen har förvaltningen under hösten haft en utbildning gällande NIS-direktivet. Hälften av de inbjuda cheferna och biträdande cheferna deltagit. Ännu ett utbildningstillfälle planeras under januari 2024.

1.3.4.4 Tydliggöra rutinen för upphandling/inköp av digitala tjänster/system

När nya IT-tjänster ska köpas in behöver förvaltningen tydliggöra i upphandlings- och inköpsprocesserna att en kravställning gällande informationssäkerhet ska göras, och att rätt kompetens behöver involveras så som dataskyddsombud, IT-funktion och informationssäkerhetsamordnare. Detta ska göras oavsett vilken beloppsgräns upphandlingen/inköpet av IT-tjänsten når upp till. Detta har inte genomförts under 2023, men en uppdatering av upphandling- och inköpsprocesserna planeras under 2024.

1.3.4.5 Genomföra informationssäkerhetsklassning av de mest skyddsvärda verksamhetsprocesserna

En plan för informationssäkerhetsklassningar har tagits fram för 2024, se nedan under 1.4.1.1 informationssäkerhetsklassningar.

Under 2023 har två informationssäkerhetsklassningar för Järva stadsdelsförvaltning genomförts. Dessa har påbörjats i föregångarna Rinkeby-Kista och Spånga-Tensta stadsdelsförvaltningar. Det är Zoom X och Mellanlagring e-arkiv Stockholm, som har klassats.

1.3.4.6 Upprätta lokala tillämpningsanvisningar

Lokala tillämpningsanvisningar har upprättats för Järva stadsdelsförvaltning som beskriver hur det systematiska informationssäkerhetsarbetet ska utföras. I dåvarande Rinkeby-Kista och Spånga-Tensta stadsdelsförvaltningar beslutades det att en tillämpningsanvisning för Järva stadsdelsförvaltning skulle upprättas för att minimera dubbelarbete. Tillämpningsanvisningarna fastställdes i juni 2023.

1.3.4.7 Behörighetshantering

Behörighetshantering har tagits upp i nätverket för informationssäkerhet och dataskydd. Ambassadörerna uppmanades att informera sina avdelningar om att se över sina behörigheter i de IT-tjänster som avdelningarna använder, men särskilt för gemensamma mappar och samarbetsytor. I och med sammanläggningen finns många gemensamma mappar och samarbetsytor kvar från föregångarna som behöver rensas och eller tas om hand för arkivering. Information om detta kommer även att

gå ut i ett chefsbrev som regelbundet skickas ut till förvaltningens chefer.

1.3.5 Resultatet från revisioner

1.3.5.1 Resultat från Spånga-Tensta stadsdelsnämnds revison 2022

Revisorernas rekommendationer för Spånga-Tensta stadsdelsnämnd gällande Implementering av dataskyddsförordningen löd så här:

Nämnden rekommenderas att utveckla styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen. Rekommendationen kvarstår.

Nämnden rekommenderas att informationsklassificera sina informationstillgångar samt regelbundet och systematiskt inventerar sina personupp-giftsbehandlingar. Rekommendationen kvarstår. – Rapporten indikerar att informationsklassificering av informationstillgångar inte har gjorts fullt. Arbete pågår för att uppdatera informationsklassning. Rapporten visar att inventering av personuppgiftsbehandlingar är ett utvecklingsområde. Uppdatering har skett under 2022 men det saknas rutiner.

Nämnden rekommenderas genomföra en kartläggning av behovet av personuppgiftsbiträdesavtal. Rekommendationen är åtgärdad. – En översyn av behovet av personuppgiftsbiträdesavtal har genomförts.

Nämnden har enligt anvisningarna upprättat en årsrapport för GDPR vilken har identifierat och synliggjort de utvecklingsområden som finns. Den samlade bedömningen är att nämnden har vidtagit åtgärder delvis.

1.3.5.2 Rinkeby-Kista stadsdelsnämnds revision 2022

Revisorernas rekommendationer för Rinkeby-Kista stadsdelsnämnd gällande Implementering av dataskyddsförordningen löd så här:

Utveckla styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen. – Nämnden har vidtagit åtgärder för att utveckla styrning och uppföljning av dataskyddsarbetet.

Informationsklassa sina informationstillgångar samt regelbundet och systematiskt inventera sina personuppgiftsbehandlingar. – Nämnden har ett systematiskt och strukturerat arbete för att löpande se över, inventera och klassa sina informationstillgångar.

Kartlägga behovet av personuppgiftsbiträdesavtal samt teckna sådana avtal där behov föreligger. – Personuppgiftsbiträdesavtal har tecknats där behov finns.

Nämnden identifierar själv vissa utvecklingsområden och har en planering för hur dessa ska åtgärdas. Rekommendationerna bedöms åtgärdade.

1.3.6 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudets årsrapport för 2023 kommer att redovisas i samband med Järva stadsdelsförvaltnings verksamhetsberättelse för 2023. De risker som kommer att lyftas där är:

- Osäker e-posthantering med personuppgifter
- Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor

Dessutom kommer följande områden att granska särskilt under 2024:

- Sociala system
- Operativt arbete med dataskyddsförordningen – medarbetare missförstår dataskydd och exempelvis använder inte vissa godkända verktyg/tjänster.

1.3.7 Information om avvikelser (incidenter och andra händelser)

Nedan finns de informationssäkerhetsincidenter som har anmälts i stadens incidentrapporteringssystem IA för Rinkeby-Kista, Spånga-Tensta och Järva stadsdelsförvaltningar under 2023.

Typ av incident	**Antal**
Borttappad/stulen mobil, dator, surfplatta, handling, USB eller liknande	6
Dörr som lämnats öppen/inbrott	4
Installerat otillåten programvara på dator	1
Mejlat/kommunicerat sekretess till extern mottagare (ej krypterat) eller fel mottagare	8
Skickat/tagit emot post på ett felaktigt sätt	6
Phishing	4
Felaktig information/registrering	6

Incidenter rörande fel behörigheter	1
Ej omhändertagna handlingar	2
Övriga personuppgiftsincidenter	3

1.4 Förbättringar som föreslås för verksamhetens LIS

1.4.1 Aktiviteter för 2024

1.4.1.1 Informationssäkerhetsklassningar

Lokala system
En del av förberedelsen inför att överföra lokala system till systemtjänsteavtalet är att informationen i systemen behöver informationssäkerhetsklassas. Klassningarna behöver genomföras under 2024 för att systemet ska kunna överföras under 2025. Exempelvis är det Vård och prognos (VORP) och Yong-UAH (journalföringssystem) som omfattas.

Nya system som verksamheten efterfrågar
För att säkerställa att Järva stadsdelsförvaltning har ett bra skydd för den informationen som hanteras i verksamheterna kommer förvaltningen att prioritera nya system/tjänster som verksamheterna behöver som stöd i sitt arbete. Exempel på system/tjänster är

- FIT outcomes – Arbetet påbörjas redan under 2023 och kommer att pågå under 2024
- MCSS Appva – Arbetet påbörjas redan under 2023 och kommer att pågå under 2024
- Rondplattformen
- Hypergene
- Löpande förfrågningar

Normerande klassningar
Satsningen Normerande klassning som samordnas av SLK kommer att prioritera information som omfattas av NIS enligt hälso- och sjukvårdslagen. Järva stadsdelsförvaltning kommer att delta i klassningarna i samarbete med objektförvaltningen för Vodok.

1.4.1.2 Nya obligatoriska e-utbildningar

I januari 2024 kommer två nya e-utbildningar att lanseras. Båda består av åtta avsnitt som kommer att släppas under januari-oktober månadsvis med undantag för juli. Utbildningarna ska utföras

gruppvis inom varje enhet med syftet att gruppen ska reflektera tillsammans för att konkretisera hur vi kan arbeta för en säkrare informationshantering.

Cheferna ansvarar för att planera in tillfällena för sina enheter.

1.4.1.3 Ta fram en plan för införande av pm3-modellen

Inventera och identifiera objekt samt genomföra nulägesanalyser för hur styrningen av objekten ser ut. Sedan ska en plan för utvalda objekt tas fram och stegvis införa pm3 under kommande åren.

1.4.1.4 Se över rutin för registerutdrag och inventera personuppgiftsbehandlingar

Rätten till tillgång (registerutdrag) har av Europiska dataskyddsstyrelsen (EDPB) valts ut som ett fokusområde för år 2024 och det är därmed ett område som kommer att prioriterats av dataskyddsmyndigheterna under det kommande året. I och med detta ska Järva stadsdelsförvaltning se över sin rutin för begäran om registerutdrag.

Förvaltningen kommer även att inventera och följa upp vilka personuppgiftsbehandlingar som finns och uppdatera registerförteckning.

1.4.1.5 Stärka medarbetares kunskap om dataskydd på medborgarkontoren

Medarbetare på medborgarkontoren kommer att få utbildning gällande dataskydd för att bättre kunna informera medborgare om deras rättigheter gällande dataskydd ur ett konsumentperspektiv.

1.4.1.6 Uppdatera de lokala tillämpningsanvisningarna

Årlig revidering av Järva stadsdelsförvaltnings lokala tillämpningsanvisningar för informationssäkerhetsarbetet.

1.4.2 Aktiviteter för 2025

- Implementera nytt incidentrapporteringsverktyg[12]
- Fortsatt implementering av pm3-modellen
- Ta fram metod/arbetssätt för att följa upp informationssäkerhetsklassningar systematiskt
- Informationssäkerhetsklassa informationstillgångar
- Inventering av personuppgiftsbehandlingar
- Revidera lokala tillämpningsanvisningarna

[12] SLK utreder för tillfället vilket incidentrapporteringsverktyg för informationssäkerhetsincidenter ska köpas in. Om förarbetet är klart till 2025 så kommer förvaltningen att ha detta som en aktivitet.

1.4.3 Aktiviteter för 2026

- Genomföra övning inom verksamheter som berörs av NIS-direktivet, t.ex. nätverksbortfall eller dataförlust
- Genomföra övning för ledningsgrupp till exempel antagonistisk cyberattack
- Slutföra implementering av pm3-modellen
- Informationssäkerhetsklassa informationstillgångar
- Inventering av personuppgiftsbehandlingar
- Revidera lokala tillämpningsanvisningarna

Beslutad 2023-11-28