Lokal anvisning för informationssäkerhet

Socialförvaltningen

Beslutad 2024-03-07
Reviderad 2024-11-06

Lokal anvisning för informationssäkerhet
Bilaga till socialnämndens verksamhetsplan 2025

Dnr. SOF 2024/667

Kontaktpersoner:
Johanna Zalyal, kanslichef, johanna.zalya@stockholm.se
Morgan Lindengren, informationssäkerhetssamordnare (ISAM), morgan.lindengren@stockholm.se

1 Bakgrund

Lokal anvisning för informationssäkerhet beskriver roller och organisation för socialförvaltningens informationssäkerhetsarbete. Dokumentet fastställdes av förvaltningschef den 2024-03-07 och revideras årligen i samband med verksamhetsplan.

Den lokala anvisningen kompletterar riktlinje för informationssäkerhet i Stockholms stad och tillhörande tillämpningsanvisningar och dokumenterar hur socialförvaltningen lokalt och praktiskt tillämpar och arbetar med informationssäkerhet och dataskyddsfrågor (GDPR). Den förtydligar hur ansvarsfördelning och roller har anpassats för socialförvaltningen – vem som ansvarar, vilka stödfunktioner och kontrollfunktioner som finns, och vilka övriga roller som i sitt uppdrag arbetar med skydd av informations-tillgångar.

Den lokala tillämpningsanvisningen beskriver också hur socialförvaltningen systematiskt arbetar med, och följer upp, informationssäkerhet och dataskyddsfrågor (GDPR).

Innehållsförteckning

2 Organisation och roller

Socialförvaltningens organisation för informationssäkerhet och dataskydd (GDPR) är indelad i tre olika nivåer.

Den **styrande** omfattar operativt beslutande roller och funktioner i verksamheten. Dessa har på olika nivåer en budget och ett personalansvar, vilket även innefattar operativt ansvar för informationshanteringen inom den delen av verksamheten.

De **stödjande** och **granskande** funktionerna är specialistfunktioner som stödjer linjeverksamheten i dess informationssäkerhetsarbete. De granskande funktionerna, utöver stadens egna revisorer, följer även upp att riktlinjer och lagstiftning följs.

2.1 Ledning (styrande)

2.1.1 Nämnd

Socialnämnden är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för socialförvaltningen. Socialnämnden ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhets- och dataskyddsarbete (GDPR) inom verksamheten samt att stadsövergripande riktlinjer och vägledande dokument för informationssäkerhet följs.

Socialnämnden ansvarar för att en ändamålsenlig organisation finns på plats och för att nödvändiga resurser tilldelas samtliga funktioner för att kunna genomföra ett effektivt informationssäkerhets- och dataskyddsarbete (GDPR). Genom detta dokument beskriver och beslutar nämnden hur denna organisation fungerar i praktiken.

Socialnämnden har ett särskilt ansvar för att utse ett data-skyddsombud (DSO) eller delegera ett sådant beslut till förvaltningschef.

Socialnämnden inhämtar årligen en så kallad GDPR-årsrapport från DSO. Syftet är att socialnämnden med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten.

I socialnämndens ansvar ligger även att delegera uppgiften att besluta om informationshantering och regler för detta. Denna uppgift beskrivs i rubrik 2.1.2 samt 2.1.3 i detta dokument.

2.1.2 Förvaltningschef

Förvaltningschefen är nämndens representant (delegat) när det gäller de övergripande lednings- och styrningsfrågorna.

Förvaltningschef ansvarar för:

- Att fastställa den lokala anvisningen och andra övergripande styrdokument för socialförvaltningen.
- Att utse en informationssäkerhetssamordnare (ISAM) och ansvara för att stödfunktioner för informationssäkerhet tilldelas de resurser som krävs.
- Att verksamheten tilldelas de resurser som behövs för att kunna upprätthålla god informationssäkerhet och möjlighet att efterleva lagstiftning på området.
- Att hålla sig underrättad om informationssäkerheten i socialförvaltningen, minst genom att inhämta de årliga rapporterna på området som exempelvis *Ledningens genomgång* från ISAM och den årliga årsrapporten från DSO.
- Att se till att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering.

2.1.3 Chef

Ansvaret för att skydda informationen som hanteras inom verksamheten följer linjeansvaret. Varje chef har inom sin verksamhet ett särskilt ansvar för att informationen hanteras på ett korrekt sätt enligt gällande lagstiftning och riktlinjer. Ansvaret för informationshanteringen ska ligga så verksamhetsnära som möjligt, och inom socialförvaltningen innebär det som lägst på enhetschefsnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom förvaltningen ansvarar för:

- Att se till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd (GDPR) årligen.

- Att följa upp och utreda de incidenter som verksamheten anmäler i IA, samt att kontakta dataskyddsansvarig (DSA) och/eller ISAM vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor. Incidenterna ska hanteras utifrån gällande rutiner.

- Att säkerställa att registervård genomförs inom chefens verksamhet och att uppdatera och följa upp förvaltningens register över hantering av personuppgifter (det vill säga registerförteckningen i Draftit).
- Att de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och förvaltningens styrdokument.
- Att informationsinventering görs av den egna verksamheten med stöd från ISAM och arkivfunktioner. Att se till att viktigare informationstillgångar är klassade och att verksamhetens it-tillgångar har en utsedd objektledare.
- Att ta fram lokala rutiner för den egna verksamheten vid behov.

2.1.4 Processägare

All informationshantering i förvaltningen har en ansvarig chef. En ansvarig chef har utsetts för respektive process med särskilt uppdrag att se till att rutiner och instruktioner finns på plats för informationshanteringen inom processområdet. Dessa ska även följa förvaltningens klassificeringsstruktur. Den chef som ansvarar för en specifik process har benämningen processägare. Processägaren beslutar vilka digitala verktyg som får användas i processen och hur information ska hanteras inom processen.

2.1.5 Objektledare

En objektägare för verksamheten ansvarar för att utse roller i objektsverksamheten, i enlighet med modellen PM3[1]. En nyckelroll är objektledare, vilken ansvarar för drift och förvaltning av en IT-tjänst.

Vilka som tilldelats rollen objektledare inom förvaltningen framgår i den förteckning över verksamhetens informationstillgångar som förs i Draftit och som upprättas på uppdrag av objektägarna.

När det gäller de it-tjänster där drift sköts på entreprenad eller på annan förvaltning, är verksamhetens (personuppgiftsansvarig) objektledare ansvarig för tjänsten i relation till den beställda (personuppgiftsbiträde) tjänsten och fungerar då som lokalt ansvarig för hur systemet används i verksamheten. I de fall både drift och verksamhet finns inom förvaltningen förekommer ibland rollen objektledare specifikt för tjänstens drift.

Objektledarens ansvar är:

[1] För information om PM3, se stadens metodstöd samt samarbetsyta för PM3

- Att tillse att informationstillgången är klassad och att handlingsplaner från klassning tas om hand för systemet.
- Att se till att förvaltningsplan och andra nödvändiga rutiner finns på plats och följs upp.
- Att tillse att stadens riktlinjer och tillämpningsanvisningar följs vad gäller informationssäkerhet för it-tjänster.
- Att besluta om regler för tillgång till systemet och se till att dessa är kända av medarbetarna.
- Att utse övriga nödvändiga funktioner inom it (t.ex. objektspecialist).

2.2 Stödjande och uppföljande

2.2.1 Informationssäkerhetssamordnare (ISAM)

Socialförvaltningens ISAM är utsedd av förvaltningschefen.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela förvaltningens verksamhet. ISAM ska arbeta utifrån förvaltningschefens styrning av vilka verksamhetsrisker och åtgärder som ska prioriteras.

ISAM ansvarar för:

- Att vara kontaktpunkt för stadens centralt informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna.
- Att fungera rådgivande gentemot förvaltningens objektledare, i projekt samt till ansvariga för upphandling.
- Att samverka med andra närliggande ansvarsområden och roller.
- Att stödja linjeverksamheten när det gäller det strategiska arbetet, kartlägga information, informationssäkerhetsklassificera den, hantera incidenter samt att utbilda medarbetare och sprida kunskap om lokala rutiner.
- Att bevaka förändringar i lagstiftningen och händelser i omvärlden.
- Att genomföra uppföljning/revision av det lokala informationssäkerhetsarbetet.

2.2.2 Dataskyddsombud (DSO)

Verksamhetens DSO utses formellt av nämnden.

Dataskyddsombudets övergripande och viktigaste uppgift är att kontrollera att dataskyddsförordningen (GDPR) följs av

verksamheten. Uppföljningen består bland annat i att utföra kontroller och informationsinsatser. Dataskyddsombudets granskningar sker genom att utföra enskilda kontroller av personuppgiftsbehandlingar och att upprätta en DSO-årsrapport till nämnden.

DSO ska kunna agera självständigt och oberoende i sitt uppdrag och ska därför inte utföra det operativa arbetet. DSO har ett nära samarbete och kontakt med ISAM, vilket är nödvändigt för att arbetet ska bedrivas effektivt och leda till största möjliga nytta.

DSO har dessutom i uppgift att:

- Vägleda, informera och ge råd till verksamheten om hur relevanta skyddsåtgärder ska väljas och implementeras för att person- och integritetsskyddet ska upprätthållas. DSO ska fokusera på de risker som finns med olika behandlingar, och då särskilt risker kopplat till behandlingens art, omfattning, sammanhang och syften.
- Ge råd vid personuppgiftsincidenter, i enlighet med verksamhetens incidentrutin.
- DSO ska alltid involveras i samband med konsekvensbedömningar och ges möjlighet granska genomförandet av dem.
- Lämna rekommendationer och medverka vid analys av personuppgiftsincidenter samt lämna sin bedömning om anmälan till Integritetsmyndigheten (IMY) är aktuell.

2.2.3 Dataskyddsansvarig (DSA)

Förvaltningens DSA samordnar det operativa dataskyddsarbetet och är kontaktlänk mellan DSO och dataskyddssamordnarna (DSS). Nätverket och roller beskrivs ytterligare i bilaga 1, Dataskydd (GDPR) uppdrag och organisation.

2.2.4 Dataskyddssamordnare (DSS)

DSS utgör dataskyddsansvarigs länk till chefer och medarbetare i verksamheterna. DSS stödjer chefer att säkerställer att verksamhetens personuppgiftsbehandlingar är registrerade i Draftit och stödjer verksamheten i frågeställningar kopplat till GDPR. Rollen beskrivs mer i bilaga 1, Dataskydd (GDPR) uppdrag och organisation.

2.2.5 ILS-samordnare (Integrerat ledningssystem)

Förvaltningens ILS-samordnare samordnar uppföljningen och beredningen av nämndens ILS-arbete.

ILS-samordnaren ska aktivt arbeta för att informationssäkerhet är med och följs upp i förvaltningens väsentlighets- och riskanalys samt införliva informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren.

ILS-samordnaren ansvarar även för användarnas behörighet i ILS.

2.2.6 Arkivfunktionen

Övergripande arkivfunktioner har en viktig funktion i stadens informationssäkerhetsarbete. Arkivfunktionen deltar aktivt i socialförvaltningens informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.

Arkivfunktionen hanterar framtagandet av de dokument där hantering och arkivering av socialförvaltningens samtliga informationstillgångar beskrivs, d.v.s. förvaltningens klassificeringsstruktur, hanteringsanvisningar, dokumenthanteringsplan och övrig arkivdokumentation.

Arkivfunktionernas roller beskrivs i förvaltningens arkivinstruktion.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom förvaltningen ska följa stadens riktlinjer och regelverk (både centrala och lokala), ta del av den information som finns om informationssäkerhet och genomföra de obligatoriska utbildningarna inom informationssäkerhet och dataskydd. Vidare ska medarbetare uppmärksamma brister och eventuella incidenter till närmsta chef för vidare hantering. Nyanställda medarbetare godkänner stadens generella användarkontrakt i samband med sin första inloggning i stadens it-miljö.

2.3.2 It-funktioner

Roller med denna expertfunktion deltar aktivt i det operativa arbetet genom att t.ex. delge sin expertkunskap vid upphandlingar, införande av system/produkt, informationsklassningar och drift.

2.3.3 Särskild systemspecialist/objektspecialist

Inom förvaltningen finns även de som genom administratörsbehörigheter på olika sätt förvaltar it-objekt i verksamheten. Strukturen/hanteringen för varje it-objekt sätts för

varje enskilt objekt, men det finns alltid minst en kontaktperson. Objektledaren ansvarar för att utse den organisationen.

3 Nätverk och grupper

Intern och extern samverkan inom informationssäkerhet och dataskydd sker utifrån behov i linjearbetet. Utöver det sker samverkan även inom olika nätverk och grupperingar. Nätverken arbetar för informationsdelning, kunskapsutbyte och metodutveckling för driva ett ändamålsenligt arbete enligt gällande lagstiftning på området.

4 Årshjul

Informationssäkerhetsarbetet finns med i nämndens verksamhetsplan i form av särskild redovisning samt med obligatoriska arbetssätt i väsentlighet- och riskanalys (VoR). Arbetet följs upp årligen i samband med nämndens tertialrapporter och verksamhetsberättelse.

Informationssäkerheten i förvaltningens verksamhetssystem hanteras genom informationsklassningar. Arbetet med informationsklassningar revideras årligen.

Förvaltningens registerförteckning över personuppgiftsbehandlingar återfinns i verktyget Draftit Privacy Records och följs upp årligen. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund inom ramen för all personuppgiftsbehandling.

Dataskyddsarbetet undersöks, kontrolleras och följs upp genom ett årshjul. De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter. Resultaten inom ramen för personuppgiftsbehandling presenteras särskilt i DSO-årsrapport.

5 Styrande dokument

Informationssäkerhetsarbetet för förvaltningen samordnas av ISAM som till sin hjälp har en informationssäkerhetsgrupp bestående av

medarbetare med kompetens inom informationssäkerhet, som it-strateger och systemansvariga vid Enheten för digitalt verksamhetsstöd (EDV). Ansvarig för informationssäkerhetsarbetets samordning är närmaste chef, till vilken frågeställningar och beslut eskaleras vid behov.

Verksamheter inom förvaltningen kan vända sig till ISAM för rådgivning och stöd vid exempelvis incidenter, inköp av nya digitala verktyg för stöd i bedömning av informationssäkerhetskraven, för hjälp med informationsklassningar och tillhörande processer samt för allmän rådgivning om informationssäkerhet. Uppgifter kopplade till detta kan fördelas inom informationssäkerhetsgruppen.

Likaså är ISAM och/eller representanter från informationssäkerhetsgruppen kontaktpersoner till Stadsledningskontoret (SLK) i olika frågor kopplade till informationssäkerhet, såsom säker kommunikation och centrala system.

Inom förvaltningen finns rutiner för incidentrapportering av informationssäkerhetsincidenter, NIS-incidenter samt för personuppgiftsincidenter. Det finns även rutiner för behörighetshantering.