2022-04-04

Diarienummer
KS 2021/1109

Dataskyddsnätverket

Dataskyddsombudets granskningsrapport 2021 – incidenthantering

Bakgrund

Av artikel 39 i EU:s dataskyddsförordning framgår det att dataskyddsombudet ska ge information och råd samt övervaka efterlevnaden av förordningen och den personuppgiftsansvariges strategi för skydd av personuppgifter. En del av detta arbete genomförs genom framåtsyftande granskning av verksamheten i syfte att kontrollera att verksamheten efterlever förordningen.

Dataskyddsombudet valde att fokusera 2021 års granskning till att omfatta Lunds kommuns hantering av personuppgiftsincidenter. Valet gjordes mot bakgrund av en omvärldsanalys samt genomgång av resultatet av 2020 års granskning, som visade att kommunen bland annat behövde utveckla sitt arbete inom incidenthantering och informationssäkerhet.

Syftet med granskningen var att granska kommunens förmåga att upptäcka, hantera, och följa upp personuppgiftsincidenter. Målet med granskningen var att ge råd och information om hur kommunen på ett bättre sätt kan säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering och identifiering av incidenter.

Granskningen genomfördes genom två intervjuer. Deltagarna var representanter från kommunkontoret, utbildningsförvaltningen, barn- och skolförvaltningen, serviceförvaltningen, socialförvaltningen samt vård- och omsorgsförvaltningen. Dessa förvaltningar intervjuades eftersom verksamheterna hanterar stora mängder personuppgifter och därmed arbetar med incidenthantering i högre grad än övriga. Övriga förvaltningar representerades av kommunkontorets deltagare och har därför inte mottagit en egen rapport, utan omfattas av kommunstyrelsens granskningsrapport.

Resultat

Dataskyddsombudet bedömer att Lunds kommun arbetar förebyggande gällande säkerhet. Granskningen har visat att

kommunen har implementerat rutiner och fastställt ansvarsfördelning vid personuppgiftsincidenter. Det finns dock behov av åtgärder, framför allt vad gäller följande:

- Kunskapsnivån i organisationen är varierande och inom vissa områden låg. Inrapporteringsgraden behöver sannolikt öka, givet kommunens storlek och omfattning. De webbaserade utbildningar som kommunen erbjuder bör användas i högre utsträckning inom hela organisationen.
- När en incident inträffar är behovet av samordning stort, i syfte att motverka negativa konsekvenser. Samordning sker emellertid informellt och processen är inte dokumenterad.
- Uppföljning och lärandeprocesser efter incidenter är huvudsakligen informell och odokumenterad.

Dataskyddsombudet rekommenderar därför att Lunds kommun ska:

- Tilldela resurser för att utbilda medarbetare och därmed öka förståelsen för personuppgiftsincidenter, vidareutveckla och implementera strukturerade och formella rutiner för rapportering och hantering av incidenter samt förtydliga och förbättra arbetssättet.
- Justera de rutiner som reglerar informationsdelning mellan verksamheter och kommunkontorets IT-avdelning, för att skapa en samordnad hantering.

Gemensamt arbete väntar

Flertalet av dataskyddsombudets rekommendationer är av kommunövergripande karaktär. Lunds kommun har redan identifierat behovet av att arbeta mer kommunövergripande med dataskyddsfrågor. För att möjliggöra ett sådant arbete har kommunkontoret fått i uppdrag att utöka och samordna de centrala resurserna som arbetar med denna typ av frågor. Detta kommer att ske under 2022.

Avsikten med kommunkontorets uppdrag är därför att, i det pågående utvecklingsarbetet, skapa ett tydligare kommunövergripande arbete där fokus bland annat kommer att vara rekommendationerna i granskningsrapporterna.

Dataskyddsnätverket

Granskningsrapport

Incidenthantering

Kommunkontoret

17 december 2021

Dataskyddsombud
Lunds kommun

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

1 Sammanfattning

Målet med granskningen är att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hanteringen och identifieringen av informationssäkerhetshändelser samt personuppgiftsincidenter.

Dataskyddsombudet noterar sedan tidigare granskning att Lunds kommun arbetar förebyggande gällande säkerhet, men det behöver även ske samordning och ett förberedande arbete för när incidenter händer för att motverka negativa konsekvenser. Bakgrunden är även att Integritetsskyddsmyndighetens (IMY) och Myndigheten för samhällsskydd och beredskap (MSB) bedömer att det sannolikt finns ett stort mörkertal i upptäckten eller incidentrapporteringen. Dataskyddsombudet beslutade därför att granska det förberedande arbetet gällande kommunens incidenthantering. Två gruppintervjuer genomfördes med representanter från förvaltningarna och IT-avdelningen baserat på ISO-standarderna 27002 och 27701.

Resultatet från granskningen visar att kommunstyrelsen har implementerat rutiner och fastställt ansvarsfördelning vid informationssäkerhetshändelser samt personuppgiftsincidenter. En generell kunskapshöjning och högre inrapporteringsgrad behöver ske hos samtliga medarbetare då den tidvis är låg inom såväl nämnder som IT-avdelning. Flera nämnder har implementerat årliga GDPR-utbildningar för medarbetare och vid nyanställning. Uppföljning och lärandeprocesser efter incidenter eller händelser är huvudsakligen informell och odokumenterad. Det finns tekniska åtgärder för att säkra och samla bevis där en stor del av ansvarsbördan faller på IT-avdelningen, men kravställningar på omfattningen brister. Tydligt dokumenterade och formaliserade processer efterfrågas av nämnderna.

Dataskyddsombudets rekommendationer är följande:

Resurser allokeras

- Resurser allokeras för att vidareutveckla rutiner och utbilda medarbetare.

Rutiner implementeras, utvecklas och förankras

- Strukturerade och formella rutiner för rapportering implementeras.
- Förtydliga och förbättra klassificeringen, arbetssättet och förståelsen för informationssäkerhetshändelser och personuppgiftsincidenter så att medarbetare ska kunna genomföra bedömningar.
- IT-avdelningen behöver ha en strukturerad dokumentation gällande incidenthanteringen.
- Framtagning av en rutin för insamling och säkrande av bevis.

Utbildning för samtliga medarbetare

- Fortsatt utbildning för medarbetare inom både informationssäkerhetshändelser och personuppgiftsincidenter samt återkommande återkoppling efter hanteringen.

Samordning mellan kommunstyrelsen, nämnder och IT-avdelning

- Justera rutiner för informationsdelning mellan verksamheter och IT-avdelning för att skapa en samordnad hantering.

2 Bakgrund

Bakgrunden till årets granskning inom dataskydd utgick ifrån omvärldsanalys, händelser och avvikelser som rapporterats under året, samt genomgång av resultatet av 2020 års granskning, en enkätundersökning av mognadsnivå inom dataskydd.

2.1 Granskning av mognadsnivå inom dataskydd 2020

Förra året granskade Dataskyddsombudet kommunens mognadsnivå inom dataskydd. Resultatet visade att kommunen låg på en generellt lägre mognadsnivå inom incidenthantering och informationssäkerhet.

Tabell 1: Medelvärdet av mognadsnivån på skalan 1–5, där 1 innebär en ad hoc hantering och 5 innebär helt optimal hantering.

Lunds kommun	
Roller och ansvar	2,13
Styrning och efterlevnad	2,09
Utbildning och kompetens	3,15
Processer och verktyg	3,20
Risk och klassning	2,33
Incidenthantering och informationssäkerhet	1,92

2.2 Omvärldsanalys

Den 25 maj 2020 publicerade Integritetsskyddsmyndigheten (IMY) en rapport som analyserade de anmälda personuppgiftsincidenter som har orsakats av olika former av IT-angrepp. Av resultatet framgick det att av de totalt 4 800 anmälningar om personuppgiftsincidenter som anmäldes till Integritetsskyddsmyndigheten under 2019, utgjordes ca 400 (8,7 procent) av incidenter som uppges bero på IT-angrepp.

IMY gjorde bedömningen att det sannolikt finns ett mörkertal när det gäller antalet faktiskt inträffade personuppgiftsincidenter som beror på IT-angrepp och som inte upptäcks, eller som upptäcks men inte anmäls till IMY. Vidare framgick det att andelen inrapporterade incidenter från offentlig sektor var låg vilket kan tyda på ett större mörkertal inom offentlig sektor jämfört med privat sektor.

För att upptäcka IT-angrepp krävs i regel mognad inom såväl IT som informationssäkerhet. Många verksamheter kan dessutom ha relativt låg kunskap om riskerna och hoten för att utsättas för IT-angrepp, varför vidtagna skyddsåtgärder kan vara bristfälliga. Kunskapen om skyldigheten att anmäla incidenter kan också vara bristfällig.

Verksamheter bör därför säkerställa sin förmåga att upptäcka och anmäla IT-angrepp som rör personuppgifter. Tydliga interna instruktioner och rutiner för när ett IT-angrepp som berör personuppgifter ska anmälas till IMY är angeläget.

Inför årets granskning inom dataskydd beslutade dataskyddsombudet att fokusera på hantering av incidenter.

3 Ansvar och roller

3.1 Personuppgiftsansvarig

Respektive nämnd är personuppgiftsansvarig för sin verksamhets personuppgiftsbehandlingar. Den personuppgiftsansvarige är skyldig att enligt Artikel 32 GDPR vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till de personuppgiftsbehandlingar man utför.

Vidare ska den personuppgiftsansvarige enligt Artikel 33 GDPR dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

3.2 Dataskyddsombud

Av Artikel 39 dataskyddsförordningen framgår att dataskyddsombudet ska övervaka efterlevnaden av förordningen, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges strategi för skydd av personuppgifter. En del av detta arbete innebär att granska verksamheten i syfte att kontrollera att den efterlever förordningen.

4 Terminologi

Personuppgiftsansvarig (PUA)	Den organisation som bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till, organisationen bestämmer mål och medel för behandlingen.
Personuppgiftsbiträde (PUB)	Den organisation som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvarigas organisation.
Dataskyddsombud (DSO)	Dataskyddsombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.
Informationssäkerhetshändelse	En händelse som äventyrar informationens säkerhet utifrån konfidentialitet, riktighet eller tillgänglighet.
Personuppgiftsincident	En händelse som orsakar att personuppgifter röjs, går förlorade, ändras, eller förstörs.
Intrång	En händelse som innebär otillåten insyn i eller påverkan på ett informationssystem.
Dataskydd	Skyddet för den personliga integriteten vid behandling av personuppgifter.
IT-angrepp	En attack som använder IT-teknik för att orsaka skada

5 Syfte

Syftet var att granska kommunens förmåga att upptäcka, hantera, och följa upp personuppgiftsincidenter och informationssäkerhetshändelser.

6 Mål med granskningen

Målsättningen är att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation kring säkerhetshändelser och svagheter samt identifiering av personuppgiftsincidenter.

7 Granskningsmetod och målområden

Granskningen genomfördes i form av två gruppintervjuer den 27 oktober 2021 med representanter från nämnderna och IT-avdelningen. Nämnderna som deltog vid intervjuerna gjorde det genom representanter från förvaltningarna. Deltagande var Kommunkontoret, Utbildningsförvaltningen och Barn och skolförvaltningen, Serviceförvaltningen, Socialförvaltningen samt Vård och omsorgsförvaltningen. Ett urval gjordes av kommunstyrelsens representant nämnder där de som deltog vid granskningstillfället var de nämnder som hanterar mycket personuppgifter och därmed arbetar med incidenthantering i högre grad. De nämnder som inte deltog representerades av kommunstyrelsens representant.

Underlaget för intervjuerna bestod av utvalda kontrollfrågor från standarderna ISO 27002 (kapitel 16), och ISO 27701 (kapitel 6.13), totalt 22 kontrollfrågor. Dessa frågor tar sikte på att få förståelse för hur kommunen går till väga i sin hantering av informationssäkerhetshändelser.

Gruppintervjuerna faciliterades av Dataskyddsombudet som gick igenom kontrollfrågorna med gruppen. Representanterna från nämnderna och IT-avdelningen fick presentera sina svar och det gavs möjlighet att ställa följdfrågor samt ha en diskussion kring frågorna. Gruppintervjuerna syftade även att vara ett lärandetillfälle för deltagarna, genom att dela med sig och ta del av varandras erfarenheter och arbetssätt.

Efter granskningstillfället sammanställde Dataskyddsombudet en granskningsrapport med en sammanställning av resultatet samt rekommendationer på förbättringsområden. Resultatet presenteras i sex övergripande målområden. Områdena utgår från ISO standarden 27002, specifikt kapitel 16 med målet att säkerställa att konsekvent och verkningsfullt tillvägagångssätt för hantering av informationssäkerhetshändelser och personuppgiftsincidenter.

De sex övergripande målområdena presenteras nedan:

7.1 Ansvarsfördelning och fastställda rutiner

Ledningsansvar och rutiner bör fastställas inom verksamheten för att säkerställa effektiv, verkningsfull och korrekt hantering av informationssäkerhetshändelser och personuppgiftsincidenter. Rutinen bör inkludera planering och förberedelser, tillvägagångssätt för upptäckt, analys, rapportering, bedömning och hantering av incidenter och händelser, rutiner för loggning. Rutinen bör även innehålla processer för hanteringen av kriminaltekniska bevis. Ledningsansvaret ska tydligt framgå med eskaleringskedjor samt kompetent och rätt personal som hanterar incidenter och händelser inom verksamheten.

7.2 Rapportering

Personal och leverantörer bör informeras om sitt ansvar att rapportera informationssäkerhetshändelser och personuppgiftsincidenter. Rutinerna för rapportering samt kontaktperson bör tydligt förmedlas till medarbetare. Rutinen bör inkludera varierande typer av incidenter och händelser för att säkerställa att

allt rapporteras korrekt. Störningar eller andra avvikande händelser i system kan indikera ett angrepp och bör där med rapporteras som en informationssäkerhetshändelse.

7.3 Bedömning och beslut

Bedömning och beslutsrutiner om informationssäkerhetshändelser och personuppgiftsincidenter bör inbegripas i de övergripande rutinerna för informationssäkerhetshändelser och personuppgiftsincidenter. Ansvarig för hanteringen av incidenter och händelser ska alltid bedöma inkomna incidenter och göra det utifrån en sedan tidigare etablerad bedömningsskala. Klassning och prioriteringar av incidenter och händelser kan vara till hjälp för att tydliggöra bedömningen. Resultaten av bedömningarna ska alltid dokumenteras för att kunna verifieras och hänvisas till.

7.4 Hantering av informationssäkerhetshändelser och personuppgiftsincidenter

Hantering av informationssäkerhetshändelser och personuppgiftsincidenter ska göras i enlighet med fastställda rutiner och ska genomföras av en relevant person eller grupp. Hanteringen bör inkludera insamling av bevis, eskalering vid behov, säkerställande av loggar, information om incidenten kommuniceras internt och externt vid behov, fastställande av eventuella brister som orsakat incidenten eller händelsen samt adekvat och korrekt dokumentering av resultatet.

7.5 Lärandeprocesser

Informationssäkerhetshändelser och personuppgiftsincidenter bör betraktas som kunskapsgivande händelser som kan minska sannolikheten för att liknade situationer uppstår. Utvärdering efter inträffad incident eller händelse kan visa på förbättringsområden inom verksamheten gällande dataskyddsarbetet och informationssäkerheten. Lärandeprocessen bör utgå från utvärderingar av tidigare incidenter och händelser för att kunna identifiera återkommande incidenter och händelser med stor påverkan.

7.6 Insamling och säkrande av bevis

Rutiner bör fastställas för identifiering, insamling, kopiering och bevarande av information som kan komma att utgöra bevismaterial. Rutinen bör ta hänsyn till spårbarhet, säkerhet för bevis och personal, roller och ansvar, dokumenterad information, personalens kompetens samt delgivning. Rutinen bör även inkludera möjligheter till disciplinära och rättsliga åtgärder. Rutinen bör även beakta organisatoriska och myndighetsgränser för att säkerställa att insamlingen sker korrekt.

8 Resultat

Nedan presenteras resultatet för granskningen där såväl kommunstyrelsens, IT-avdelningens samt kommunövergripande resultat presenteras. I anslutning till varje rubrik ger dataskyddsombudet ett antal rekommendationer i enlighet med analysen av nämndens incidenthantering.

8.1 Ansvarsfördelning och fastställda rutiner

Det finns kommunövergripande rutiner för personuppgiftsincidenter där roller är fastställda och beslutsfattande är delegerat. Kommunkontoret har även ett tydligt ansvar för att driva processen. Utöver de övergripande rutinerna har vissa nämnder implementerat nämndspecifika rutiner med nämndspecifika kontaktpersoner vid incidenter. Rutinen för att hantera personuppgiftsincidenter finns dokumenterad och är tillgänglig för kommunens medarbetare. Dataskyddssamordnare på nämnderna har ledningsansvar vad gäller informationssäkerhetshändelser och personuppgiftsincidenter. I de flesta nämnder finns fastsatta rutiner kring tillvägagångssätt samt kontaktpersoner för incidenthantering, men det finns vissa svårigheter för medarbetare att hitta informationen på intranätet.

Det finns incidenthanteringsrutiner på IT-avdelningen men de är fokuserade på IT-relaterad verksamhet i stort. Gällande informationssäkerhetshändelser och personuppgiftsincidenter är det en outtalad och icke-formaliserad process. Rutinerna för händelser och incidenter är riktade mot tekniska lösningar där dokumentation och rapportering för personuppgiftsincidenter inte är fastställda i rutinen. Skulle en incident ske kan den eskaleras enligt en prioritetsmodell där IT:s digitaliseringschef kan tillkalla krisorganisationen. IT-avdelningen arbetar även med att förebygga incidenter med systemförvaltare, leverantörer och centralt på kommunen med syftet för att bygga upp säkerhet utöver nätverkssäkerhet. I den tekniska delen av upphandlingsavtalen kravställs patchning och tidsramar för leverantörer. IT-avdelningen menar att incidenter eller händelser som sker inom ramen för nämnders verksamhet ska rapporteras av berörd verksamhet och inte till IT.

8.1.1 Analys och bedömning:

Lunds kommuns nämnder samt har implementerat rutiner och fastställt ansvarsfördelning samt arbetssätt vid en informationssäkerhetshändelse och personuppgiftsincident. IT-avdelningen har etablerade rutiner för hanteringen av IT-relaterad verksamhet. IT-avdelningen har tydlig ansvarsfördelning inom verksamheten och med nyckelpersoner på nämnder och kommunkontoret. Det är av stor vikt att rutinerna och ansvarsfördelningen är välkänd för medarbetare.

Dataskyddsombudet rekommenderar att:

- Kommunstyrelsen justerar rutiner för informationsdelning mellan styrelsen och IT-avdelning för att skapa en samordnad hantering.
- Resurser allokeras för att vidareutveckla rutiner och utbilda medarbetare.

8.2 Rapportering

Tillgängligheten av information angående informationssäkerhetshändelser och personuppgiftsincidenter skiljer sig mellan nämnderna samt hur lättillgänglig eller etablerad rapporteringsrutinerna för händelser och incidenter är. Informationssäkerhet är inte välkänt inom nämnderna. Rutinerna för rapportering av informationssäkerhetshändelser är därmed inte allmänt

kända av medarbetare. Nämnderna lyfter även vikten av att skapa en positiv kultur av rapportering där medarbetare har ett genomgående incidenttänk i verksamheten. Leverantörer skickar ut rapporter direkt till nämnden som därefter får göra en bedömning kring personuppgiftsincidenter. Rapporteringen sker i enlighet med PUB-avtal och leverantören skickar incidentrapporter inom den angiva tidsramen.

IT-avdelningen lyfter utmaningen med att säkerställa att alla medarbetare är informerade och bekanta med rutinerna för rapportering av informationssäkerhetshändelser och personuppgiftsincidenter. Medarbetarna arbetar med att hantera IT-relaterad verksamhet i allmänhet, och rapporterar eller diskuterar det med de relevanta personerna inom IT-avdelningen. Rutiner för rapportering av personuppgiftsincidenter eller informationssäkerhetshändelser är inte etablerade utan det sker indirekt via dialog med nyckelpersoner.

8.2.1 Analys och bedömning:

Kunskapen kring informationssäkerhetshändelser och personuppgiftsincidenter är generellt låg hos medarbetare vilket leder till att händelser och incidenter inte rapporteras. Såväl kunskapsnivån som rapporteringsgraden måste höjas hos medarbetare för både informationssäkerhetshändelser samt personuppgiftsincidenter.

Dataskyddsombudet rekommenderar att:

- Kommunstyrelsen implementerar strukturerade och formella rutiner för rapportering.
- Rutinerna för rapportering diskuteras med tydliga exempel från nämnden eller IT-avdelningens verksamhet för att visa vad som kan och ska rapporteras.

8.3 Bedömning och beslut

Inom nämnderna görs bedömningen om det är en personuppgiftsincident eller informationssäkerhetshändelse av medarbetaren som rapporterar incidenten. Bedömningen och beslutet kan även göras tillsammans med medarbetarens chef och i samråd med dataskyddssamordnare. Genom vidaredelegationen av uppgiftshanteringen hamnar mycket av beslut och hantering hos dataskyddssamordnaren. Då informationssäkerhetshändelser och personuppgiftsincidenter inte är förankrade hos nämndernas medarbetare blir det svårt för enskilda medarbetare att göra bedömningar avseende dessa frågor. De tillgängliga GDPR-utbildningarna fokuserar på att förhindra incidenter utan att ge likvärdig utbildning i bedömningen av händelser och incidenter vilket försvårar en korrekt hantering.

En preliminär bedömning görs av Service Desk där de hanterar alla inkomna händelser och incidenter. Medarbetarna bedömer hur man ska hantera händelsen och tar vid behov kontakt med nyckelpersoner inom nämnderna eller IT-avdelning för att bedömning och beslutet kring händelsen ska göras. För att incidenten eller händelsen ska kategoriseras som en informationssäkerhetshändelse eller personuppgiftsincident ska det klassas som sådant under incidentprocessen, där det idag inte inbegrips i den ordinarie modellen. IT-avdelningen efterfrågar ett gemensamt system för både incidenter, händelser och IT-relaterade ärenden.

8.3.1 Analys och bedömning:

För att följa rådande lagar så ska alla personuppgiftsincidenter och informationssäkerhetshändelser rapporteras.

Dataskyddsombudet rekommenderar att:

- Kommunstyrelsen förtydligar och förbättrar klassificeringen, arbetssättet och förståelsen för händelser och incidenter så att medarbetare ska kunna genomföra bedömningen.
- Kommunstyrelsens medarbetare utbildas i rapporteringsrutinerna för att säkerställa att rapportering sker.

8.4 Hantering av informationssäkerhetshändelser och personuppgiftsincidenter

Inom nämnder följs de rutiner som är fastställda för hur medarbetare och ansvarig ska hantera informationssäkerhetshändelser och personuppgiftsincidenter. Det finns skillnader mellan nämnderna i implementeringen av eskaleringstrappan vid händelser och incidenter. Inom nämnderna finns även skillnader i möjligheten för loggning i systemen som används där det saknas möjlighet i vissa system och det finns automatiserade loggkontroller i andra. Där loggkontroller görs kan man vid incidenter kontrollera vem som gått in i systemen. För leverantörer hanteras incidenter och händelser i enlighet med personuppgiftsbiträdesavtalet med tillit till leverantörernas rapportering.

Inom IT-avdelningen arbetar man utifrån Information Technology Infrastructure Library (ITIL)-ramverket och dess problem-process, men ramverket är inte implementerad till fullo inom kommunen. Hanteringen av händelser och incidenter utgår ifrån att riskminimera och lösa problem. Rapporteringen av incidenter kommer sekundärt och hanteras då genom kommunikation med nyckelpersoner eller medarbetare inom IT-avdelningen. Fokus ligger på den operativa hanteringen av incidenterna och på att få upp systemen igen eller göra nödlösningar för att få systemen användningsbara. Loggning används på systemen och är automatiserat vilket innebär att patchning görs ofta. Systemförvaltaren har ansvar för att hantera serversystemens loggning och patchning.

8.4.1 Analys och bedömning:

Kommunstyrelsen arbetar utefter fastställda rutiner och riktlinjer med eskaleringstrappor och tydligt utsatta steg för hantering. Kommunstyrelsen har bra och tydlig rapporteringsrutin kring informationssäkerhetshändelser och personuppgiftsincidenter. Hanteringen på systemnivå koncentreras kring att få systemen användbara och fungerande.

Dataskyddsombudet rekommenderar att:

- IT-avdelningen behöver ha en strukturerad dokumentation gällande incidenthanteringen.
- Kommunstyrelsen fortsätter utbilda alla medarbetare inom verksamheten i informationssäkerhetshändelser och personuppgiftsincidenter.
- Kommunstyrelsen utvärderar och granskar rutinerna för hantering av incidenter och händelser.

8.5 Lärandeprocesser

Fokus inom nämnderna ligger på utbildning kring informationssäkerhetshändelser och personuppgiftsincidenter i stort och hur de ska förhindras. Medarbetare genomgår utbildningarna vid nyanställning och därefter en gång per år. Det efterfrågas tydligare diskussioner kring vad medarbetare ska göra vid incidenter samt efter hanteringen. Utvärdering efter

informationssäkerhetshändelser eller personuppgiftsincidenter sker i liten skala inom nämnderna. I rapporteringssystemet finns rutinerna fastställda kring hur en rapportering ska gå till men lärandeprocesser hos enskilda nämnder sker sparsamt utanför enskilda diskussioner med medarbetare kring mindre händelser.

IT-avdelningens arbetssätt betonar den operativa hanteringen av incidenter. Rapportering och utvärdering görs inte inom ramen för en rutin, men det finns inofficiella och informella dialoger inom IT-avdelningen. Lärande görs genom diskussioner om hanteringen och förbättringar som kan göras. Då rutinerna inte inkluderar informationssäkerhetshändelser eller personuppgiftsincidenter sker inte lärandeprocesser kring rapporteringen.

8.5.1 Analys och bedömning:

Nämnderna arbetar med att årligen utbilda medarbetarna i frågor rörande personuppgiftshantering genom ett e-learning-verktyg. Det finns fortsatt inofficiella lärandeprocesser där man utvärderar det operativa arbetet på ett icke-formaliserat sätt genom informella kanaler. Genom att etablera utvärderingar och lärandeprocesser kan detta användas som underlag vid utbildningstillfällen.

Dataskyddsombudet rekommenderar att:

- Kommunstyrelsen integrerar uppföljning och lärandeprocesser som nödvändiga steg i befintliga rutiner.
- Kommunstyrelsens medarbetare fortsätter att årligen utbildas i informationssäkerhet och personuppgiftsincidenter.

8.6 Insamling och säkrande av bevis

Inom de systemen med möjlighet till loggkontroller finns en integrerad spårbarhet och mekanismer för att samla in och säkra bevis efter informationssäkerhetshändelser och personuppgiftsincidenter. Vid händelser och incidenter i systemen hänvisas medarbetare inom nämnden till IT-avdelningen. Inom verksamheten arbetar man främst med dokumentation av händelseprocessen och genom rapporter kan bevis säkerställas.

Kryptering används som en teknisk skyddsåtgärd för att skydda informationen exempelvis vid stöld av datorer och mobiltelefoner. Det finns ett etablerat arbetssätt och rutiner för utlämning av information vid förfrågningar till polismyndigheten. Systemen loggar vem som fått systemåtkomst samt att åtkomsten till systemens baksida är ytterst begränsad och är endast tillgänglig för priviligierade användare. Vid åtkomst loggas alltid inloggningsuppgifter för användaren vilket innebär spårningsmöjligheter inom systemen.

8.6.1 Analys och bedömning:

För att säkerställa att bevisföring bevaras är det viktigt att inkludera insamling av bevis i rutiner kring informationssäkerhetshändelser och personuppgiftsincidenter för att inte missa viktig bevisföring under hanteringen av incidenten eller händelsen.

Dataskyddsombudet rekommenderar att:

- Kommunstyrelsen och IT-avdelning arbetar fram ett gemensamt arbetssätt för att säkerställa bevisföring genom dubblering av system och loggar, korrekt och noggrann dokumentation under hanteringen samt återkommande dialog kring processen.

- Nämnden tar fram en rutin för insamling och säkrande av bevis.
- Nämnden överväger att upphandla ett kriminaltekniskt stöd vid allvarliga incidenter.

9 Inkomna personuppgiftsincidenter under 1 september 2020 – 31 augusti 2021

Totalt inkom 63 anmälningar i Lunds kommun inom den angivna tidsramen. Av dem rapporterades 23 till en tillsynsmyndighet. Incidenterna som inkom var av följande kategori:

- Obehörigt röjande: 33st
- Obehörig åtkomst: 19st
- Ändring av personuppgifter: 2st
- Förlust/stöld: 2st

Barn och skolnämnden anmälde 28 incidenter.

Utbildningsnämnden anmälde 14 incidenter.

Kultur och fritidsnämnden anmälde 2 incidenter.

Kommunstyrelsen anmälde 7 incidenter

Socialnämnden anmälde 2 incidenter.

Vård och omsorgsnämnden anmälde 5 incidenter.

Tekniska nämnden anmälde 1 incident.

Överförmyndarförnämnden anmälde 3 incidenter.

(Det inkom även 7 incidenter som inte omfattade kommunens verksamhet.)

10 Avslutningsvis

Granskningen av Lunds kommuns nämnder och IT-avdelning kring incidenthantering har resulterat i att man kan konstatera att nämnderna har etablerade rutiner och tydlig ansvarsfördelning vid personuppgiftsincidenter och informationssäkerhetshändelser. Riktlinjer och rutiner för bedömning, rapportering och hantering av incidenter och händelser finns etablerade i nämnderna.

Resultatet av granskningen har visat att det med stor sannolikhet finns ett mörkertal i informationssäkerhetshändelser och personuppgiftsincidenter som sker i såväl kommunstyrelsen, nämnderna som på IT-avdelningen. Bristande kunskap i vad som utgör en personuppgiftsincident och informationssäkerhetshändelse samt i rapporteringsrutinerna för inträffade incidenter och händelser kan ligga till grund för att incidenter och händelser går obemärkta och inte rapporteras. Kommunikationen mellan kommunstyrelsen, nämnder och IT-avdelning bör därmed stärkas för att

säkra kontinuerlig dialog kring rutinerna samt säkerställande att incidenter och händelser rapporteras och hanteras i de korrekta kanalerna.

Dataskyddsombudet rekommenderar att kommunstyrelsen i samråd med IT-avdelningen arbetar fram tydliga rapporterings- och hanteringsrutiner för informationssäkerhetshändelser och personuppgiftsincidenter. Kommunstyrelsens samtliga medarbetare bör informeras och utbildas i dessa rutiner. Vidare rekommenderar dataskyddsombudet ökade utbildningsinsatser för samtliga medarbetare i informationssäkerhet och dataskyddsfrågor för att höja kunskapsnivån för såväl kommunstyrelsens medarbetare som IT-avdelning.

Dataskyddsombudet bedömer att Lunds kommun bedriver ett förebyggande arbete genom olika säkerhetsåtgärder som såväl nämnder som IT-avdelning tar. Dataskyddsombudet konstaterar däremot att det förberedande arbetet för hur informationssäkerhetshändelser upptäcks och identifieras som personuppgiftsincidenter inte är lika omfattande. Dataskyddsombudet rekommenderar således att kommunstyrelsen, nämnderna och IT-avdelning utvecklar sin förberedande förmåga genom allokering av resurser, samordning, rutiner och utbildning.

SIGNATURES **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 13 pages before this page
Tämä asiakirja sisältää 13 sivua ennen tätä sivua
Detta dokument innehåller 13 sidor före denna sida
Dokumentet inneholder 13 sider før denne siden
Dette dokument indeholder 13 sider før denne side

authority to sign	asemavaltuutus	ställningsfullmakt	autoritet til å signere	myndighed til at underskrive
representative	nimenkirjoitusoikeus	firmateckningsrätt	representant	repræsentant
custodial	huoltaja/edunvalvoja	förvaltare	foresatte/verge	frihedsberøvende