



Dataskyddsombudens rapport 2024

Linköpings kommuns nämnder

Datum: 2025-01-31
Mottagare: Kommundirektören
Handläggare: Dataskyddsombuden
Organisation: Linköpings kommun

Innehåll

Sammanfattning	4
1. Inledning	5
2. Dataskyddsorganisationen	6
2.1. Dataskyddsombudens roll	6
2.2. Dataskyddssamordnare och nätverk	6
3. Registerförteckningen (Artikel 30-register)	8
Rekommenderat fortsatt arbete	9
4. Konsekvensbedömning avseende dataskydd	10
Rekommenderat fortsatt arbete	11
5. Registrerades rättigheter	12
Rekommenderat fortsatt arbete	13
6. Incidentrapportering	14
Rekommenderat fortsatt arbete	16
7. Dataskyddsombudets internutbildningar hos kommunen	17
Rekommenderat fortsatt arbete	17
8. Dataskyddsombudens granskningar hos kommunen	18

Sammanfattning

Dataskyddsombuden bedömer att det fortsatt finns stor förbättringspotential i kommunens dataskyddsarbete. Dataskyddsombuden ser att det sker en stor positiv utveckling och rekommenderar respektive förvaltning att i samråd med sitt dataskyddsombud prioritera bland de rekommendationer som lyfts i denna rapport.

De rekommendationer som lämnades i föregående års rapport kvarstår. Vidare rekommenderar dataskyddsombuden starkt att förvaltningarna fortsätter utveckla dataskyddsarbetet inom och mellan förvaltningarna. I denna årsrapport presenterar dataskyddsombuden åtgärder för att adressera uppmärksammade brister men för att åtgärderna ska få önskvärd effekt behöver tid och resurser avsättas på respektive förvaltning.

Dataskyddsombudens tidigare rekommendation kring prioritering av registerförteckningens revidering kvarstår. En komplett och aktuell förteckning är en grundläggande förutsättning för ett välfungerande och effektivt dataskyddsarbete. Förvaltningarna rekommenderas att se över befintliga processer för att införliva dataskyddsarbetet i de fungerande processer som finns och som är kända inom den egna förvaltningens verksamheter. Därutöver bör förvaltningarna inventera och höja kunskapsnivån inom dataskydd.

Dataskyddsombuden önskar att varje förvaltning möjliggör framtagande av mer statistik för dataskyddsarbetet så att nyckeltal, exempelvis för antalet upptäckta och hanterade personuppgiftsincidenter, hanterade begäran av rättigheter eller antalet tecknade personuppgiftsbiträdesavtal, kan jämföras över tid. På så vis kan bättre slutsatser om dataskyddsarbetet inom kommunen dras och eventuella åtgärder planeras. I kommande årsrapporter planerar dataskyddsombuden att tydliggöra dataskyddsarbetets framsteg i tabeller och diagram.

1. Inledning

Denna rapport är framtagen av Linköpings kommuns (Kommunens) dataskyddsombud. Varje nämnd inom kommunen är självständigt personuppgiftsansvarig för de personuppgiftsbehandlingar som utförs inom dess ansvarsområde. Nämnderna inom kommunen arbetar i stor utsträckning med dataskyddsarbetet utifrån ett kommungemensamt arbetssätt. Dataskyddsombuden har därför valt att ta fram en gemensam rapport och i rapporten kommer nämnderna med tillhörande förvaltningar gemensamt benämnas *kommunen*.

I dataskyddsförordningen¹ framgår att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges högsta ledning. Sådan direktrapportering kan, enligt *Riktlinjerna om dataskyddsombud*², till exempel ske i form av en årsrapport och säkerställer att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer samt det pågående dataskyddsarbetet.

Denna årsrapport omfattar 2024 års dataskyddsarbete inom kommunen. Rapporten sammanfattar det dataskyddsarbete som skett under det gångna året och bör fungera som en vägledning för kommande års arbete. I rapporten framgår vissa utvalda områden inom dataskyddet. Områdena har valts ut med beaktande av deras aktualitet i det gångna årets dataskyddsarbete. I takt med att dataskyddsarbetet utvecklas och förändras kan de utvalda områdena komma att variera över tid.

Syftet med denna årsrapport är dels att informera ledningen, dels att skapa ett planeringsunderlag inför kommande års dataskyddsarbete.

¹ EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

² Artikel 29-arbetsgruppens Riktlinjer om dataskyddsombud, 16/SV, WP 243 rev.01.

2. Dataskyddsorganisationen

2.1. Dataskyddsombudens roll

Rollen som dataskyddsombud är lagstadgad och arbetet bedrivs främst utifrån de uppgifter som framgår av dataskyddsförordningen. Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen efterlever dataskyddsförordningen och kompletterande dataskyddslagstiftning. Dataskyddsombudet ska rapportera till ledningen och utgör kontaktpunkt för tillsynsmyndigheten och de registrerade. Dataskyddsombudet ska vidare informera och ge råd om dataskyddsförordningen samt utföra utbildnings- och informationsinsatser inom dataskyddsområdet.

På grund av sin granskande och rådgivande roll ska dataskyddsombudet inte vara operativ i dataskyddsarbetet. Dataskyddsombudet har inte något eget ansvar för efterlevandet av dataskyddsförordningen utan ansvarar för att rapportera eventuella brister till ledningen.

2.2. Dataskyddssamordnare och nätverk

Dataskyddsorganisationens arbetssätt inklusive dataskyddsnätverk och avstämningsmöten med respektive förvaltnings dataskyddssamordnare har fortsatt under år 2024. Nätverket har under 2024 träffats varje månad med undantag för ett sommaruppehåll, med ett högt deltagande. Avstämningsmötena har fortsatt att, liksom under 2023, bidra till utvecklingen av kommunens dataskyddsarbete och dessa möten är en viktig förutsättning för ett effektivt och riskbaserat dataskyddsarbete. Behovet av dessa möten har varit särskilt stort under 2024 då ett flertal förvaltningar (fyra av åtta) har bytt dataskyddssamordnare bland annat på grund av omorganisering och personalomsättningar under året. Denna förändring har hanterats olika på de olika berörda förvaltningarna, antingen genom att en tillförordnad dataskyddssamordnare tillsattes under tiden arbetsuppgiften fördelades på nytt eller genom att tillsätta resurser när brådskande ärenden uppkommit.

Dataskyddsombuden anser att mötena och nätverket uppfyller sitt syfte och upplever att de även är ett uppskattat stöd av dataskyddssamordnarna. Till stöd för dataskyddssamordnarna har även en tillämpningsanvisning till riktlinjen för dataskydd tagits fram i början av 2024. I tillämpningsanvisningen förtydligas bland annat dataskyddsorganisationens uppbyggnad och de olika rollernas uppdrag och ansvar.

Informationssäkerhetsarbetet som är ett närliggande, och bitvis överlappande, område till dataskyddsarbetet har varit högaktuellt under 2024. Bland annat har informationssäkerhetsansvarig kommunjurist fått en stående plats i dataskyddsnätverket liksom dataskyddsombuden har fått en stående plats i informationssäkerhetsnätverket. I kommunen har även en ny roll, *informationssäkerhetssamordnare* (ISAM), införts på samtliga förvaltningar.

I flera fall har förvaltningens dataskyddssamordnare också blivit utnämnd till förvaltningens ISAM. På grund av att områdena delvis är överlappande har synergieffekter mellan områdena undersökts och arbetet förväntas fortlöpa under kommande år. Sammantaget har detta medfört att relativt mycket tid på avstämningsmöten och i nätverket har använts för att diskutera ramarna samt de likheter och skillnader som finns mellan dataskydd och informationssäkerhet. Diskussionerna har i sin tur lyft nya frågor och utvecklat tidigare uppkomna frågor inom dataskyddsarbetet. Frågor som lyfts har bland annat berört fördelningen av personuppgiftsansvar i mer eller mindre gemensamma system och frågor om hur det praktiska arbetet ska vara fördelat mellan olika förvaltningar. Dataskyddsombuden ser positivt på denna utveckling och rekommenderar att dessa frågor utreds för att nämndernas ansvarsområden ska tydliggöras.

Under året har dataskyddssamordnarnas arbete att revidera registerförteckningen fortsatt och flera verksamheter har nu en uppdaterad registerförteckning medan andra verksamheter är på god väg. Dataskyddsombuden har även i år initierat olika inventeringar. Dataskyddssamordnarna har under hösten dels fått i uppdrag att inventera de behandlingar där fördelningen av personuppgiftsansvaret upplevs oklart, dels har en inventering av konsekvensbedömningar avseende dataskydd initierats. Inventeringen av konsekvensbedömningar genomförs inom ramen för en gemensam inventering tillsammans med informationssäkerhetsorganisationen

3. Registerförteckningen (Artikel 30-register)

Kommunen är enligt dataskyddsförordningen skyldig att föra registerförteckning, vilket är ett register över de personuppgiftsbehandlingar som utförts. Det innebär att de personuppgiftsbehandlingar som registreras i förteckningen, registreras utifrån ändamålet med behandlingen. *Varför har dessa uppgifter samlats in?* Registerförteckningen ska uppdateras löpande så att den vid var tid speglar de behandlingar som är aktuella. På begäran ska registerförteckningen göras tillgänglig för tillsynsmyndigheten.

Registerförteckningen beskrivs ofta som en av hörnstenarna i dataskyddsarbetet. I registerförteckningen ska viss information såsom ändamål, mottagare och eventuell tredjelandsoverföring anges. Detta innebär att registerförteckningen är ett verktyg för personuppgiftsansvarig att på ett effektivt sätt få en överblick över sina personuppgiftsbehandlingar. Registerförteckningen utgör också ett stöd i andra dataskyddsprocesser såsom vid hanteringen av begäran om registerutdrag och är en förutsättning för att på ett adekvat sätt kunna hantera olika händelser i omvärlden såsom exempelvis upphörande av adekvansbeslut för ett tredje land eller attacker mot olika system.

Kommunens nämnder har samlat sina registerförteckningar i ett gemensamt system och de hanteras på samma kommungemensamma sätt, därför kommer registerförteckningarna i det följande benämnas *registerförteckningen*.

Arbetet som initierades sommaren 2023 med att revidera registerförteckningen genom att ta bort inaktuella registreringar och uppdatera övriga har ännu inte slutförts hos merparten av förvaltningarna vid utgången av 2024. Merparten av förvaltningarna har dock påbörjat arbetet att inventera och registrera personuppgiftsbehandlingar som utförs inom ansvarsområdet. Registerförteckningen innehåller vid årsskiftet 2024/2025 totalt 252 stycken registrerade personuppgiftsbehandlingar varav 146 stycken har skapats eller uppdaterats mellan våren 2023 då revideringen påbörjades och årsslutet 2024. Av det totala antalet registrerade personuppgiftsbehandlingar utgör 76 stycken av dessa slutförda/färdigställda registreringar medan övriga 176 är påbörjade.

Dataskyddsombuden bedömer att dataskyddssamordnarna under året både har hittat ett enhetligt sätt och en adekvat nivå att registrera personuppgiftsbehandlingarna på, vilket resulterat i att registerförteckningen blivit tydligare än tidigare. Fler registreringar än tidigare innehåller kompletta nyckeluppgifter såsom ändamål och mottagare.

Enligt tillämpningsanvisningen för dataskydd är det dataskyddssamordnaren som själv eller genom annan registrerar information om personuppgiftsbehandlingarna i registerförteckningen. Detta innebär att dataskyddssamordnaren behöver ta del av den information som ska registreras i registerförteckningen för att kunna fullgöra sitt uppdrag. För att jämna ut arbetsbelastningen över tid behöver förvaltningens processer för införande, förändring och avveckling av personuppgiftsbehandlingar inklusive system innefatta att meddela dataskyddssamordnaren om ändringar för att möjliggöra en uppdaterad registerförteckning. Om befintliga processer inte förändras såsom rekommenderat riskerar registerförteckningen att bli inaktuell, vilket i sin tur medför ökad risk för negativ påverkan på

andra processer såsom felaktiga och olagliga tredjelandsoverföringar eller ett försvårat incidentarbete.

I arbetet med att inventera personuppgiftsbehandlingar till registerförteckningen har flera behandlingar uppmärksammats där det inte är tydligt klarlagt hur personuppgiftsansvaret är fördelat. Personuppgiftsansvaret behöver vara tydliggjort för att nämnderna ska veta vilket ansvar som åligger respektive nämnd enligt dataskyddsförordningen och för att exempelvis kunna möjliggöra korrekt hantering av andra processer inom dataskyddsarbetet. Med bakgrund av detta har dataskyddsombuden initierat ett arbete för dataskyddsamordnarna att inventera sådana behandlingar. Denna inventering förväntas avslutas under våren 2025.

Rekommenderat fortsatt arbete

De rekommendationer som lämnades i föregående rapport 2023 kvarstår.

Kommunen rekommenderas fortsätta arbetet med registerförteckningen så att registerförteckningen blir komplett och aktuell. Arbetet med registerförteckningen rekommenderas därefter fortlöpa kontinuerligt så att registerförteckningen vid var tid är uppdaterad. Förvaltningens och tillhörande objekts processer bör möjliggöra för dataskyddsamordnaren att löpande kunna uppdatera registerförteckningen.

Dataskyddssamordnaren kan med fördel ta del av relevant objektplan för att på så vis ha kännedom om objektets planer för införande, förändring och avveckling för det kommande året.

4. Konsekvensbedömning avseende dataskydd

Enligt dataskyddsförordningen ska den personuppgiftsansvarige med beaktande av bland annat behandlingens beskaffenhet och risker vidta lämpliga säkerhetsåtgärder. En konsekvensbedömning avseende dataskydd är en organisatorisk säkerhetsåtgärd som åligger den personuppgiftsansvarige att genomföra inför införande av en personuppgiftsbehandling som sannolikt leder till hög risk för de registrerades fri- och rättigheter. Syftet med processen är att kontinuerligt identifiera och minimera riskerna som behandlingen innebär för de registrerade. I processen ska den tänkta behandlingen ses över från början till slut och riskerna analyseras för att lämpliga säkerhetsåtgärder ska kunna vidtas. Konsekvensbedömningen möjliggör dessutom att en stor del av de dokumentationskrav gällande de grundläggande principerna i dataskyddsförordningen uppfylls.

Skyldigheten att genomföra en konsekvensbedömning åligger personuppgiftsansvarig i de fall en personuppgiftsbehandling som sannolikt leder till hög risk planeras. För att underlätta bedömningen kring vilka behandlingar som anses utgöra hög risk har tillsynsmyndigheten ställt upp ett antal kriterier för vad som anses utgöra riskhöjande faktorer, såsom behandling av känsliga personuppgifter i stor omfattning eller användning av ny och innovativ teknik. Skyldigheten att genomföra processen föreligger även när en högriskbehandling förändras och eftersom såväl organisationens behov som riskerna utvecklas över tid innebär denna skyldighet att konsekvensbedömningen bör revideras regelbundet. Notera att även en pågående personuppgiftsbehandling som tidigare inte krävt en konsekvensbedömning kan förändras så att skyldigheten att genomföra en konsekvensbedömning uppstår.

I en mellan dataskydd och informationssäkerhet gemensam inventering ska konsekvensbedömningar inventeras. Inventeringen ska dels visa på de konsekvensbedömningar som hittills har genomförts, dels belysa om det felaktigt saknas konsekvensbedömningar för pågående personuppgiftsbehandlingar.

Ansvar för att vidta lämpliga säkerhetsåtgärder enligt dataskyddsförordningen innebär ett ansvar att vid behov revidera genomförda konsekvensbedömningar. Det är därför en förutsättning att verksamheten har god kännedom om de konsekvensbedömningar som har genomförts av pågående personuppgiftsbehandlingar.

För att möjliggöra för dataskyddsombuden att övervaka genomförandet av konsekvensbedömningar behöver verksamheterna löpande uppdatera dataskyddsombuden om status för påbörjade konsekvensbedömningar. Dataskyddsombuden har därför, i samband med verksamhetens inventering, inventerat de konsekvensbedömningar avseende dataskydd som dataskyddsombuden blivit involverade i sedan dataskyddsförordningens ikraftträdande.

I tabellen på nästa sida presenteras det totala antalet konsekvensbedömningar som dataskyddsombuden har kännedom om, vid datumet för denna rapport, med den status som dataskyddsombuden senast blivit informerade om.

Totalt antal påbörjade konsekvensbedömningar inklusive förhandsbedömningar	41
Antal genomförda	20
Antal pågående	9
Antal vilande/avslutade projekt utan påbörjat införande	3
Antal okänd status	9
Antal uppdaterade	0

Dataskyddsombuden bedömer att de konsekvensbedömningar som genomförts i alltför stor omfattning håller en för låg nivå när konsekvensbedömningen för första gången överlämnas till dataskyddsombuden för översyn. Detta medför att processen för att uppnå en godtagbar konsekvensbedömning blir ineffektiv och i många fall långdragen, vilket dataskyddsombuden upplever att flertalet projekt inte tar höjd för.

För att framöver förebygga ovanstående problematik kommer dataskyddsombuden erbjuda en utbildning i konsekvensbedömningar avseende dataskydd två gånger per termin under år 2025 och löpande därefter utifrån behov. Med start från och med januari 2026 bör minst en av personerna som deltar i arbetet med konsekvensbedömningar ha genomgått denna utbildning.

Rekommenderat fortsatt arbete

Förvaltningen rekommenderas att regelbundet se över genomförda konsekvensbedömningar för att säkerställa att de är uppdaterade under hela personuppgiftsbehandlings livstid.

Förvaltningen rekommenderas dessutom se över sina processer så att eventuella statusförändringar i projekt meddelas dataskyddsombuden för att möjliggöra dataskyddsombudens övervakning av arbetet med konsekvensbedömningar. Processerna bör även ses över för att säkerställa att konsekvensbedömningens slutsatser når relevant riskägare innan personuppgiftsbehandlingen påbörjas.

Dataskyddsombuden rekommenderar att relevanta personer från förvaltningarna deltar på utbildningen som kommer erbjudas under 2025 så att arbetet kring konsekvensbedömningar effektiviseras.

5. Registrerades rättigheter

De registrerade har ett antal rättigheter enligt dataskyddsförordningen. Det finns inga formkrav för hur begäran om att utöva rättigheterna ska se ut. När en begäran inkommer ska den hanteras utan onödigt dröjsmål, senast inom en månad. Tidsfristen kan dock under vissa omständigheter förlängas. Kommunen ska alltid hantera begäran om rättigheter som inkommer, detta innebär dock inte att begäran alltid kan tillmötesgå.

De registrerade har rätt att begära att:

- få tillgång till sina personuppgifter (registerutdrag)
- personuppgifter raderas
- personuppgifter rättas
- begränsa en personuppgiftsbehandling,
- invända mot en behandlingen,
- utöva rättigheter vid automatiserade beslut och
- få dataportabilitet.

De olika rättigheterna utövas i olika stor omfattning av kommunens registrerade, delvis på grund av verksamheternas beskaffenhet. Inom kommunen är begäran om registerutdrag mest förekommande medan dataportabilitet nästan aldrig blir tillämplig.

2024 års planerade granskning avsåg de kommunala nämndernas praktiska hantering av begäran om registerutdrag.³ Under granskningen framkom att det finns ett flertal brister i den praktiska hanteringen. Inom ramen för granskningen lämnade dataskyddsombuden rekommendationer på åtgärder för att omhänderta de brister som uppmärksammats.

Dataskyddsombuden har under året genomfört två utbildningar kring hanteringen av registerutdrag. En av dessa genomfördes för registratorsnätverket i syfte att klargöra gränsdragningen mellan registerutdrag och begäran om allmän handling. Som ett svar på resultatet av granskningen erbjöd dataskyddsombuden dessutom de som deltar i hanteringen av begäran om registerutdrag, en utbildning som genomfördes i november. Denna utbildning kommer även att erbjudas vid åtminstone ett tillfälle under våren 2025. Dataskyddsombuden bedömer att utbildningsinsatserna genererat en utveckling av både hanteringen av registerutdrag samt höjt kunskapsnivån på förvaltningarna. Dataskyddsombudens bedömning är dock att det finns ett behov av fortsatt utbildning inom området och att förvaltningsspecifika rutiner bör hållas uppdaterade alternativt, om sådana saknas, tas fram.

³ Läs mer om denna granskning under avsnitt *Dataskyddsombudens granskningar hos kommunen*.

Rekommenderat fortsatt arbete

Dataskyddsbuden rekommenderar att förvaltningarna tar fram förvaltningsspecifika rutiner kring handläggning av begäran om rättigheterna och ser över befintliga sådana. Dataskyddsbuden rekommenderar att förvaltningarna prioriterar rutiner utifrån vanligast förekommande begärda rättighet. Dataskyddsbuden kommer framöver föreslå utbildningar då behov uppmärksammas men även erbjuda stående utbildningar för hanteringen av begäran om registerutdrag. Dataskyddsbuden ser gärna att dessa utbildningstillfällen nyttjas framöver för att fortsatt höja kunskapsnivån inom kommunen.

Dataskyddsbuden planerar att framöver följa upp kommunens hantering av de registrerades rättigheter samt kontrollera att detta sker inom rätt tid (1 månad). Förvaltningarna bör därför på förfrågan kunna besvara vilka typer av begäranden som inkommit samt datum för förfrågan och när dessa har besvarats.

6. Incidentrapportering

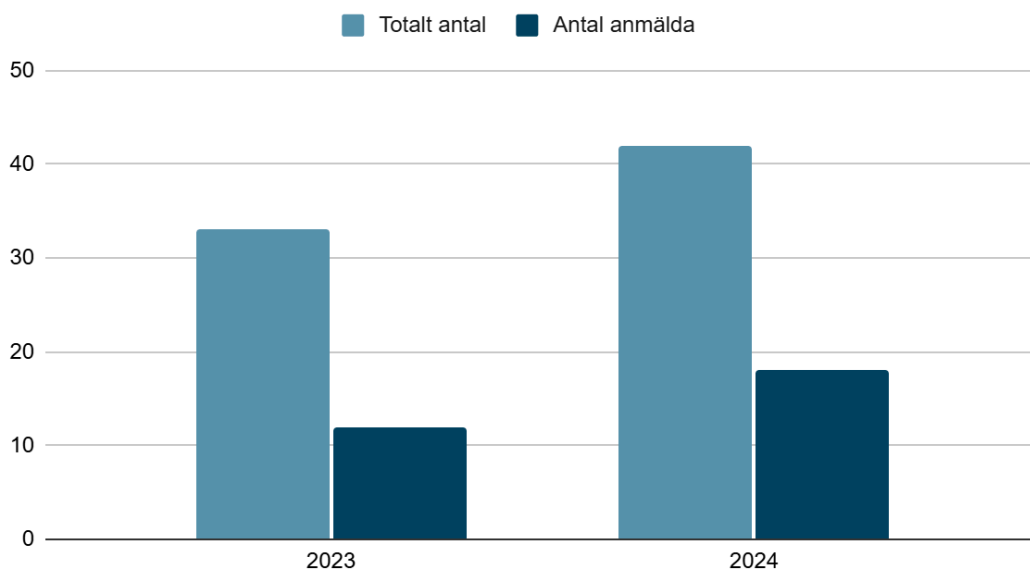
För att kunna leva upp till skyldigheterna enligt dataskyddsförordningen avseende incidenthantering är det viktigt att kommunen har rutiner för att kunna upptäcka, rapportera, utreda och då lagstiftningen kräver det anmäla personuppgiftsincidenter.

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. En personuppgiftsincident kan få allvarliga konsekvenser för de registrerade. Likaså kan tilltron till den organisation som behandlar personuppgifter påverkas negativt om incidenten inte hanteras på ett lämpligt sätt.

Den personuppgiftsansvarige måste dokumentera samtliga personuppgiftsincidenter samt anmäla allvarligare sådana till tillsynsmyndigheten. Sådan anmälan ska ske inom 72 timmar från det att personuppgiftsincidenten har upptäckts. Under vissa omständigheter ska även de registrerade informeras om incidenten.

Under 2024 uppmärksammades drygt 40 stycken misstänkta personuppgiftsincidenter i kommunen varav 20 stycken anmäldes till tillsynsmyndigheten. De vanligaste orsakerna till de uppmärksammade incidenterna var felskickade brev och e-post, tekniska fel i samband med uppdateringar samt bristfällig/felaktig behörighetsstyrning som medfört obehörigt röjande av eller obehörig åtkomst till personuppgifter. Drygt 60 procent av det totala antalet incidenter utreddes, rapporterades samt dokumenterades inom 72 timmar.

Antal upptäckta och anmälda personuppgiftsincidenter



Bilden illustrerar antalet rapporterade incidenter för åren 2023 och 2024. De ljusblå staplarna i diagrammet visar det totala antalet internt rapporterade incidenter och de mörkblå staplarna belyser det totala antalet anmälda incidenter.

För att kunna ge bättre råd till verksamheterna och för att verksamheterna lättare ska kunna arbeta med prevention av incidenter har dataskyddsombuden under hösten analyserat de incidenter som anmäldes till tillsynsmyndigheten under 2023 respektive 2024.

Under 2023 inträffade drygt 30 stycken personuppgiftsincidenter i kommunen varav 12 anmäldes till tillsynsmyndigheten. Den vanligaste orsaken till anmälningspliktig incident angavs vara den mänskliga faktorn och felskickade brev eller e-post vilket medfört obehörigt röjande av personuppgifter. Störst antal incidenter upptäcktes av medarbetare. Cirka 60 procent av de anmälningspliktiga incidenterna rapporterades inom den lagstadgade tidsfristen på 72 timmar. De incidenter som anmäldes efter att tidsfristen löpt ut tillhörde samma personuppgiftsansvariga nämnd.

Störst antal anmälda incidenter under 2024 upptäcktes av utomstående/registrerade. Den vanligaste orsaken till incident angavs fortsatt vara den mänskliga faktorn och felskickade brev eller e-post vilket har medfört obehörigt röjande av personuppgifter. Cirka 50 procent av de anmälningspliktiga incidenterna anmäldes inom den lagstadgade tidsfristen på 72 timmar.

Dataskyddsombuden har noterat att antalet internt rapporterade incidenter under året har ökat. Det är främst i de verksamheter som tidigare har rapporterat incidenter i låg grad som ökningen har skett. En anledning kan vara att de utbildningsinsatser som genomförts under året har ökat förståelsen. Dataskyddsombuden bedömer fortsatt att antalet internt rapporterade incidenter borde vara högre, med beaktande av verksamheternas art. Det låga antalet personuppgiftsincidenter som når dataskyddsombuden indikerar därmed att det finns ett mörkertal. Dataskyddsombuden noterar att kunskapsnivån gällande personuppgiftsincidenter fortsatt varierar mellan och inom förvaltningarna.

Dataskyddsombuden bedömer att de flesta verksamheter i kommunen har en aktiv och fungerande incidenthantering. Dataskyddsombuden noterar vidare att samma verksamhet har rapporterat ett flertal likartade incidenter vilket pekar på att verksamheten har god kännedom om skyldigheten att rapportera incidenter men inte fullt ut vidtagit lämpliga åtgärder för att minimera risken för att liknande incidenter uppstår på nytt.

Dataskyddsombuden uppmärksammar att många av de anmälningspliktiga incidenterna, till skillnad från de dokumenterade, inte hanterats så skyndsamt som vore önskvärt med beaktande av dataskyddsförordningens tidsfrister. Dataskyddsombuden ser därför att det finns ett fortsatt stort behov av både utbildning och förvaltningsspecifika rutiner för hantering av misstänkta personuppgiftsincidenter, så att de lagstadgade tidsfristerna efterlevs i högre utsträckning.

Rekommenderat fortsatt arbete

Dataskyddsbuden rekommenderar förvaltningarna att i enlighet med tillämpningsanvisningen ta fram förvaltningsspecifika rutiner kring hantering av personuppgiftsincidenter och se över eventuella befintliga sådana.

Den analys som dataskyddsbuden genomfört visar att kommunen generellt sett följer tidsfristen för att utreda incidenter inom 72 timmar från upptäckt i mindre omfattning än tidigare. Förvaltningarna rekommenderas därför sprida information om och utbilda medarbetare i de interna rutiner som finns. Dataskyddsbuden kommer att föreslå utbildningar då sådana behov uppmärksammas men det är upp till förvaltningen att dessa utbildningstillfällen nyttjas av relevanta medarbetare.

7. Dataskyddsombudets internutbildningar hos kommunen

Utbildning är ett effektivt sätt att proaktivt stärka dataskyddet i kommunen. Kunskap om dataskydd och behandling av personuppgifter behöver finnas spridd i kommunen och underhållas över tid genom att medarbetare kontinuerligt utbildas inom området.

På utvecklingsportalen finns en e-utbildning om dataskydd (GDPR - en grundkurs) som är obligatorisk för alla chefer och som finns tillgänglig för alla anställda inom kommunen. 171 personer genomförde utbildningen under 2024. 122 personer tilldelades utbildningen under 2024 varav 87 av dessa slutförde utbildningen under samma år.

Efterfrågan av den grundläggande utbildningen inom dataskydd har minskat till förmån för något mer riktade utbildningsinsatser, vilket dataskyddsombuden bedömer är positivt. Detta har medfört att ett antal utbildningar inom olika områden av dataskydd har genomförts under 2024. Tillsammans med kommunjuristerna har verksamheter utbildats i gränserna mellan dataskydd, informationssäkerhet samt offentlighet och sekretess. Dataskyddsombuden har dessutom fortsatt genomföra utbildning om registerutdrag och utvidgat denna till att omfatta alla funktioner som är delaktiga i processen.

Dataskyddsombuden har under året uppmärksammat att även i de fall ett liknande utbildningsbehov finns i de olika förvaltningarna, efterfrågar de olika förvaltningarna utbildningar i olika omfattning. Dataskyddsombuden efterfrågar utbildningsbehov löpande under året och i de fall en förvaltning har efterfrågat utbildning har en sådan genomförts. I ett par fall har dataskyddsombuden även i år förberett efterfrågade utbildningsinsatser som sedan inte blivit av på grund av uppskjutna eller uteblivna bokningar.

Dataskyddsombuden planerade att under 2024 införa en återkommande utbildning om genomförandet av en konsekvensbedömning avseende dataskydd. Denna utbildning planeras istället att införas under våren 2025.

Dataskyddsombuden vill dessutom lyfta att mindre utbildningsinsatser kring dataskydd sker kontinuerligt, till exempel vid olika möten eller inom ramen för enskilda frågor.

Rekommenderat fortsatt arbete

Förvaltningarna rekommenderas inventera och uppmärksamma utbildningsbehov kontinuerligt. Dataskyddsombuden välkomnar fortsatt alla utbildningsförfrågningar.

Dataskyddsombuden rekommenderar att relevanta personer från förvaltningarna deltar på de återkommande och föreslagna utbildningar som dataskyddsombuden erbjuder samt att det säkerställs att obligatoriska utbildningar i dataskydd genomförs.

8. Dataskyddsombudens granskningar hos kommunen

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen, ett verktyg för detta är granskningar. Genom granskningarna får förvaltningarna ett strukturerat underlag för att utveckla och förbättra dataskyddsarbetet.

Dataskyddsombuden bedömde tidigare att kommunens dataskyddsarbete har haft större nytta av dataskyddsombudens rådgivning och informella granskningar snarare än av större formella granskningar. Dataskyddsombuden har därför prioriterat detta för att höja kunskapsnivån i kommunen och på så sätt uppnå ökat dataskydd. Dataskyddsombuden uppmärksammar att dataskyddsarbetet i kommunen fortsätter visa på god utveckling, vilket medför att fokus förflyttas från informella granskningar till att i större utsträckning riktas mot genomförandet av formella granskningar. Den totala granskning av kommunens dataskyddsarbete som dataskyddsombuden genomför kommer dock fortsatt vara uppdelad mellan formella och informella granskningar. Dataskyddsombuden granskar exempelvis de konsekvensbedömningar som förvaltningarna överlämnar i informella granskningar genom att lämna synpunkter och rekommendationer i utbildande syfte under processens gång.

Under våren 2024 genomfördes den planerade uppföljningen av 2020 års granskning avseende kommunstyrelsens registerförteckning inom HR-området som planerat. Uppföljningsrapporten överlämnades till dataskyddssamordnaren och representant för enheten.

Den paus i den löpande granskningen av kommunens registerförteckning som gjordes 2023 till förmån för en revidering var initialt planerad att slutföras under 2023. Då denna tidsplan inte följdes fortlöpte revideringen av registerförteckningen under 2024. Dataskyddsombuden noterar att revideringen fortsatt inte är slutförd varför den förväntas fortsätta under 2025. De olika förvaltningarna har kommit olika långt i revideringen varav vissa är mer eller mindre klara. För dessa förvaltningar har den löpande granskningen återupptagits i takt med att nya eller förändrade personuppgiftsbehandlingar registrerats.

Under 2024 genomfördes en planerad formell granskning avseende den praktiska hanteringen av registerutdrag. Under granskningen framkom att det finns ett flertal brister i den praktiska hanteringen, bland annat gällande involverade funktioners ansvar och omfattningen av personuppgiftsbehandlingarna som ska kontrolleras i hanteringen⁴. De flesta verksamheter uppmanades därför att inkomma med en åtgärdsplan för att omhänderta de brister som verksamheten själva valt att prioritera. Alla åtgärdsplaner är ännu inte inkomna och flera åtgärdsplaner var försenade men lämnades in efter påminnelse. Dataskyddsombuden har tagit emot 5/6 sådana åtgärdsplaner hittills. Den förvaltning som ännu inte inkommit med sin åtgärdsplan har haft svårigheter att ta fram en sådan då det inte har varit klargjort vem som bär ansvaret för att en sådan tas fram.

⁴ Läs mer om detta i respektive nämnds granskningsrapport eller i *Sammanställning av dataskyddsombudens granskning 2024*.

Med anledning av upprepade personuppgiftsincidenter inom ett och samma system, som kommunstyrelsen ansvarar för, öppnades en riktad granskning under oktober 2024. Granskningen förväntas fortgå under våren 2025.

Under 2024 års kick-off presenterade dataskyddsombuden utgångspunkten för 2025 års planerade formella granskning. Granskningen kommer genomföras med utgångspunkt i artikel 32 i dataskyddsförordningen.

Dataskyddsombuden planerar även att under 2025 genomföra mindre granskningar i form av stickprovskontroller bland annat angående kommunens kunskap om dataskydd och personuppgiftsbehandling.