Nacka kommun

Granskning av kommunens hantering av skyddade personuppgifter

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

EY har på uppdrag av Nacka kommuns revisorer granskat kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur kommunen säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både medborgare och anställda vid kommunen. Granskningen har omfattat kommunstyrelsen, socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning. Vår övergripande bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga.

De olika enheterna har vidtagit diverse åtgärder i sitt löpande arbete för att förhindra röjning av skyddade personuppgifter. Detta är delvis inom det ordinarie sekretessarbetet som omfattar alla kunder, men även riktade åtgärder. Inom ramen för det riktade arbetet har enheterna på eget initiativ och i varierande grad upprättat rutinbeskrivningar och processer för hanteringen av skyddade personuppgifter. Överlag bedömer vi att dessa är ändamålsenliga och tillämpliga men har också identifierat brister och förbättringsområden, däribland striktare behörighetsbegränsningar i IT-system och mindre manuell hantering av skyddade personuppgifter.

Kommunen har ingen övergripande styrning inom området och de granskade nämnderna har inte heller beslutat om egna styrdokument. Vår bedömning är att även med hänsyn till Nackas kommuns styrmodell är en politiskt beslutad strategisk inriktning inom området nödvändig. Varken kommunstyrelsen eller de granskade nämnderna har gjort någon uppföljning inom området avseende exempelvis enheternas arbetsrutiner, kompetensutveckling eller avvikelsehantering. Det har heller inte genomförts risk- och konsekvensanalyser avseende röjning av skyddade personuppgifter inom ramen för internkontrollarbetet. Således bedömer vi att de inte har säkerställt att ett ändamålsenligt arbete bedrivs.

Det genomförs ingen systematisk och kommunövergripande fortlöpande kompetensutveckling inom området och det finns inget särskilt utrymme för rutinförankring. Enheterna genomför själva en viss rutinförankring och kompetensutveckling genom att löpande behandla frågan internt på möten. Vår bedömning är dock att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn vilket enligt oss är den största risken i hanteringen av skyddade personuppgifter.

Avvikelser avseende skyddade personuppgifter behandlas i samma process som andra personuppgiftsincidenter. Detta inkluderar anmälning till Integritetsskyddsmyndigheten enligt lagstadgad tidsram. Då incidenter avseende skyddade personuppgifter inte särskiljs från andra personuppgiftsincidenter finns en risk att förutsättningarna för uppföljning av incidenter, särskilt från nämndernas sida, blir sämre.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen att:

- Upprätta och anta ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter. Ett sådant styrdokument bör omfatta inriktningen för arbetet både kommunens kunder och dess medarbetare på en strategisk nivå.

Kommunstyrelsen och samtliga granskade nämnder rekommenderas att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Utbildningsnämnden och nämnden för arbete och försörjning rekommenderas att:

- Utvärdera riskerna för arbetet med skyddade personuppgifter med att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal.

2. Inledning

2.1 Bakgrund

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Från 2011 till 2021 har personer i Sverige med skyddade personuppgifter fördubblats från drygt 12 000 personer till knappt 24 000 personer. Den 1 januari 2019 skärptes lagstiftningen i syfte att öka skyddet för hotade och förföljda personer.

Personer med skyddade personuppgifter riskerar allvarliga problem om kommunens nämnder och bolag röjer skyddade uppgifter. Kommunen och bolagen bör därför ha säkra rutiner och riktlinjer för att säkerställa korrekt hantering av dessa uppgifter. Det är väsentligt att dessa arbetssätt och metoder är välkända hos samtliga medarbetare då i princip samtliga kan komma i kontakt med skyddade personuppgifter via kundkontakter eller som kollega.

Revisionen har beslutat genomföra en fördjupad granskning av kommunens arbete med rutiner, kunskapsspridning och säkerhetsfrågor vad gäller hanteringen av skyddade personuppgifter. Lekmannarevisorerna genomför samma granskning i Nacka vatten och avfall AB (NVOA) samt i Nacka Energi AB (NEAB).

2.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma hur kommunen och bolagen säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Granskningen avser skyddade personuppgifter för såväl anställd personal som för kommuninvånare.

I granskningen besvaras följande revisionsfrågor:

- Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?
- Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?
- Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?
- Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?
- Har kommunen tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Har kommunen analyserat risken för att skyddade personuppgifter röjs?
- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?
- Har kommunen vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter?
- Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?
- Hur tillvaratas erfarenhet från avvikelser?
- Råder det samsyn inom Nacka kommun och dess bolag kring hur skyddade personuppgifter ska hanteras?

2.3 Ansvarig nämnd och avgränsningar

Granskningen avser kommunstyrelsen, socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning. Av de kommunala bolagen granskas Nacka vatten och avfall AB samt Nacka Energi AB inom ramen för lekmannarevisionen.

2.4 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer med berörda tjänstepersoner samt respektive presidium. Samtliga intervjuade funktioner och granskade underlag framgår av källförteckningen.

Granskningen har följt god revisionssed och har kvalitetssäkrats internt, bland annat genom avstämning mot revisionsfrågor, faktagranskning och strukturerad dokumentation. Utöver intern kvalitetssäkring har samtliga intervjuade haft möjlighet att komma med synpunkter på rapportutkastet, detta för att säkerställa att revisionsrapporten bygger på korrekta uttalanden.

2.5 Revisionskriterier

Med revisionskriterier avses bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna kan hämtas från lagar och förarbeten eller interna regelverk beslutade av fullmäktige/bolagsstämmor. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning. I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725)
- Offentlighets- och sekretesslagen (2009:400)
- Folkbokföringslagen (1991:481)
- Folkbokföringsfördordning (1991:749)
- SFS 2018:695 Lag om ändring i folkbokföringslagen
- Socialtjänstlagen (2001:453)
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer
- COSO-ramverket för intern kontroll
- Best practice kring bedömning av rutiner och intern kontroll vid hantering av skyddade personuppgifter

Dessa beskrivs närmare i bilaga och i kapitel 3.

I revisionsfrågorna används styrdokument, styrande dokument och rutiner som begrepp. Inom ramen för granskningen har vi behandlat styrdokument och styrande dokument som synonymer. Dessa avser dokumentformer som listas i *Styrdokument i Nacka kommun*, vilket inkluderar bland annat föreskrifter, riktlinjer, program och *"Så här gör vi i Nacka"*-dokument. Utifrån detta kan styrdokument beslutas av kommunfullmäktige, kommunstyrelsen, ansvarig nämnd samt stadsdirektör. Vi har tolkat rutin som arbetssättet för att omsätta styrdokumenten i den vardagliga verksamheten. Dokumenterade beskrivningar av rutiner har vi benämnt som rutinbeskrivningar.

3. Kontrollmiljö

Kontrollmiljö består exempelvis av etiska värderingar, ledarskapsresurser och ansvarsfördelning inom organisationen. Kontrollmiljö utgör en betydande del av den kultur som finns i organisationen: Är de anställda medvetna om det interna regelverket? Kan de lyfta etiska frågor? Hur agerar de i avsaknad av regler? Här är ledningens riskhanteringsfilosofi, styrprinciper, integritet och etiska värderingar viktiga. Utöver organisationskultur består kontrollmiljön även av styrdokument.

3.1 Respektive nämnd är personuppgiftsansvarig inom sitt verksamhetsområde

Nacka kommuns styrning och ledning beskrivs som processorienterad. Processerna är uppdelade inom tre kategorier: huvudprocesser, stödprocesser och styrprocesser. Huvudprocesserna har som mål att leverera något direkt till medborgarna. Det kan exempelvis vara utbildning eller social omsorg. Stödprocesserna syftar till att bidra till huvudprocessernas mål genom stöd och styrning till organisationen. Här ingår ett antal delprocesser, bland annat ekonomiprocessen och juridikprocessen. Stadsdirektören är ansvarig för styrprocesserna, vilka syftar till att leda och styra så att kommunfullmäktiges mål och uppdrag uppfylls. Bland styrprocesserna ingår exempelvis uppföljning och utvärdering samt strategisk förnyelse.

I *Mål och budget 2023–2025*[1] framgår att Nacka kommuns styrmodell består av fem olika delar; vision, värdering, ambition, övergripande mål och styrprinciper. Kommunens styrprinciper är:

- Särskiljande av finansiering och produktion
- Konkurrens genom kundval och upphandling
- Konkurrensneutralitet
- Delegerat ansvar och befogenheter

Dessa innebär bland annat att kommunen skiljer på finansiering och produktion. Kommunfullmäktige och nämnder har ansvaret för finansieringen av verksamheterna och produktionen kan vara i privat eller kommunal regi. Den kommunala produktionen är organiserad i en egen del av verksamheten, välfärd skola och välfärd samhällsservice, som är ansvarsmässigt underställd kommunstyrelsen. Vidare innebär principerna att ansvaret ska ligga på lägsta effektiva nivå. I Nacka har den kommunala produktionen således stort utrymme att själva besluta hur deras verksamhet utformas.

Varje nämnd är personuppgiftsansvarig för de personuppgifter som behandlas inom sitt verksamhetsområde. Om en nämnd ska behandla personuppgifter i de kommungemensamma system för vilka kommunstyrelsen är personuppgiftsansvarig ska personuppgiftsbehandlingen ske i enlighet med de instruktioner som lämnas av kommunstyrelsen. Om en nämnd/kommunstyrelsen ska behandla personuppgifter i system för vilka annan nämnd är personuppgiftsansvarig ska personuppgiftsbehandlingen ske i enlighet med de instruktioner som lämnas av den personuppgiftsansvariga nämnden.

[1] Fastställd av kommunfullmäktige 2022-11-14 § 289.

Nacka kommuns *Informationssäkerhetsstrategi*[2] utgör det styrande dokumentet för kommunens informationssäkerhetsarbete och är därmed av relevans för hanteringen av skyddade personuppgifter. Av strategin framgår att informationssäkerhetsarbetet ska präglas av förtroende för medarbetares och leverantörers förmåga att hantera informationstillgångar på ett säkert sätt. Kommunstyrelsen har det övergripande ansvaret för kommunens informationssäkerhet och stadsledningskontoret ska säkerställa att det finns funktioner som har förmåga att stötta, samordna och följa upp informationssäkerhetsarbetet samt att det finns ett användarnära stöd. Varje nämnd ansvarar för att informationstillgångar inom sitt ansvarsområde hanteras enligt gällande lagstiftning och strategi. Informationssäkerhetsarbetet ska vara uppbyggt så det är lätt att hantera information korrekt, vilket bland annat innefattar att det finns lättillgänglig kunskap om informationssäkerhetsarbetet och att det finns utbildning som är tillgänglig för alla.

Vid granskningstillfället pågår en revidering av informationssäkerhetsstrategin. Av utkast till den nya strategin framgår fyra strategiska inriktningar som informationssäkerhetsarbetet ska bygga på:

- Identifiera och analysera tillgångar, krav och risker
- Utforma informationssäkerhetsarbetet efter säkerställda behov
- Arbeta aktivt, inkluderande och framåtlutat
- Systematisk uppföljning, lärande och förbättringar

Detta innefattar bland annat att verksamheterna regelbundet ska följa upp efterlevnaden av sina mål, handlingsplaner, säkerhetsåtgärder och prioriteringar för att säkerställa att avsedd verkan uppnåtts. En målsättning i framtagandet av den nya strategin är att tydliggöra struktur för uppföljning och det förbättrande arbetet.

Kommunen har ett dataskyddsombud med uppdrag enligt GPDR, vilket innefattar att vara rådgivande och granskande för dataskyddet. Detta inkluderar bland annat att agera rådgivande vid personuppgiftsincidenter med eventuell anmälan till Integritetsskyddsmyndigheten (IMY). Därutöver finns det dataskyddssamordnare på varje enhet som har i uppdrag att utföra det operativa dataskyddsarbetet.

För ytterligare beskrivning av kommunstyrelsens och nämndernas ansvarsområden inom granskningsområdet hänvisar vi till bilaga 3.

3.2 Styrande dokument och enhetsspecifika rutinbeskrivningar

3.2.1 Det saknas kommunövergripande styrdokument för hanteringen av skyddade personuppgifter

Det finns inget kommunövergripande styrdokument för hantering av skyddade personuppgifter. Vid intervju har detta kopplats till styrmodellen i Nacka. Upplevelsen bland intervjuade är att rutiner för arbetet med skyddade personuppgifter inte behöver beslutas på övergripande nivå, utan att frågan med fördel kan hanteras mer verksamhetsnära i enlighet med Nacka kommuns styrmodell. Samtidigt har flera intervjuade också sett att det finns ett utrymme för mer central styrning inom området och att en utveckling åt det hållet har påbörjats i kommunen. Detta är tänkt att innefatta övergripande aspekter av exempelvis informationssäkerhet och ansvarsfördelning avseende skyddade personuppgifter. Av intervju

[2] Fastställd av kommunfullmäktige 2017-12-11.

framgår att juridik- och kanslistaben muntligt fått i uppdrag att upprätta ett formellt styrdokument om hanteringen av skyddade personuppgifter för beslut i kommunstyrelsen. Detta arbete är dock i inte påbörjat men dokumentet kommer enligt uppgift tas fram under 2023.

Ledningsstaben och digitaliseringsenheten har tagit fram vissa dokument för stöd till verksamheterna som är av relevans för ämnet, även om de inte specifikt avser hanteringen av skyddade personuppgifter. Bland dessa finns:

Guide Lagringsalternativ som syftar till att ge användare information om vilka aspekter som ska beaktas vid lagring av information samt vilka möjligheter som ges. Av guiden framgår bland annat att hanteringen av information kan formas av om den innefattar någon form av sekretess, om den innehåller känsliga eller extra skyddsvärda personuppgifter eller om informationen är känslig av annan karaktär. Information som bedöms vara eller är klassad som känslig eller innehåller större mängder personuppgifter bör hanteras, delas och sparas i ett verksamhetssystem. Om det inte är möjligt ska informationen sparas på miljö endast tillgänglig från Nacka kommuns nät. Vidare framgår att känslig information som behöver delas med extern part kan hanteras via säkra meddelanden. Det framgår inte vem som har fastställt dokumentet men det framgår att det är skrivet av informationssäkerhetssamordnare, digitaliseringsenheten. Vi noterar att begreppet "*Guide*" inte förekommer som nivå på styrande dokument i *Styrdokument i Nacka kommun*.[3]

Även *Guide för hantering av personuppgiftsincidenter* har relevans inom området. Denna innehåller information om hur personuppgiftsincidenter, oavsett om det rör skyddade personuppgifter eller andra personuppgifter, ska hanteras. För närmare beskrivning av rutinen, se avsnitt 6.1. Det framgår inte vem som har fastställt dokumentet.

Kommunen håller på att införa en modell för objektstyrd systemförvaltning. Detta innebär att förvaltningen av system ska struktureras per objekt[4], med olika roller och planer per objekt. För detta tar digitaliseringsenheten fram olika hjälpmedel till verksamheterna. Vi har tagit del av utkast för dessa hjälpmedel. I *Mall för Årshjul 2023* ingår information och IT-säkerhet som ett moment. I en tillhörande checklista för arbetet med årshjulet ingår bland annat informationsklassificering av systemstöd enligt KLASSA[5], relevant för kommunens hantering av skyddade personuppgifter.

Det finns också information om arbetet med skyddade personuppgifter tillgänglig på kommunens hemsida, under området juridik. Detta inkluderar generella rekommendationer om hur skyddade personuppgifter bör hanteras, bland annat att verksamheter bör ha rutiner för arbetet och att e-post inte ska användas för att skicka sekretessbelagda uppgifter. Informationen har tagits fram av juridik- och kanslistaben. Rutinerna har inte varit föremål för politiskt beslut och de är inte tvingande, utan är tänkta att utgöra ett stöd till verksamheterna. Sidan uppdaterades senast den 30 april 2019. Intervjuade menar att sidan inte har behövt uppdateras då informationen fortfarande är aktuell och relevant.

[3] Fastställd 2017-10-XX av kommunstyrelsen.

[4] Objekt avser i detta fall ett system som stödjer en process eller en verksamhet.

[5] Klassa är ett verktyg framtaget av SKR för att stödja kommuner och regioner i att klassificera verksamhetssystem efter exempelvis skyddsnivåer.

3.2.2 De granskade nämnderna har inte beslutat om styrdokument för hanteringen av skyddade personuppgifter

De granskade nämnderna har inte beslutat om några styrdokument inom området. Enheterna har tagit fram egna rutinbeskrivningar. Vi noterar att dessa benämns på flera olika sätt, exempelvis rutin och manual. Det framgår inte vem, om någon, som har fastställt dokumenten. Utifrån *Styrdokument i Nacka* är det otydligt vem som ska besluta om rutiner, medan begrepp som manual eller instruktion inte förekommer alls. I tabellen nedan följer en sammanställning av enhetsspecifika rutinbeskrivningar med relevans för området.

Ansvarig enhet	Fastställd av	Rutinbeskrivning
Välfärd skolas verksamhetsstöd	Framgår ej	Admininstruktioner sekretesshantering användarkonto
Välfärd skolas verksamhetsstöd	Framgår ej	Målsmannadokument skyddad identitet
Välfärd skolas verksamhetsstöd	Framgår ej	Manual – hantering av sekretesskydd, förskola & grundskola
Barn- och familjeenheten och omsorgsenheten	Framgår ej. Det framgår dock att den är "*skapad av*" en specifik person.	Skyddade personuppgifter
Arbets- och etableringsenheten	Framgår ej. Det framgår dock arbetsledare har ansvar för dokumentet i samråd med systemspecialist.	Sekretessmarkerad kund
Arbets- och etableringsenheten	Framgår ej. Det framgår dock arbets- och etableringsenhetens dataskyddssamordnare har ansvar för dokumentet.	Rutin för hantering av personuppgiftsincident
Utbildningsenheten	Framgår ej.	Arbetsbeskrivningar för hanteringen

Process vid anställning och hantering av anställda

Hanteringen av anställda och ansökningshandlingar med skyddade personuppgifter går genom kommunens centrala personalenhet. För detta finns en intern processbeskrivning för manuell hantering av medarbetare med skyddade personuppgifter som avser exempelvis hur anställda med skyddade personuppgifter ska hanteras systemtekniskt. Målsättningen har varit att minimera antalet personer som är bekanta med rutin i detalj, vilket innebär att en begränsad mängd medarbetare inom enheten arbetar med sådana situationer.

Kommunstyrelsen har inte beslutat om några styrdokument inom området.

Välfärd skola

Välfärd skolas verksamhetsstödet har tagit fram rutinbeskrivning för hur skyddade personuppgifter ska hanteras i anslutning till att en elev med skyddade personuppgifter börjar på en skola eller att en elev på en skola får skyddade personuppgifter under pågående läsår. Denna har inte beslutats av kommunstyrelsen. Detta inkluderar teknisk hantering av verksamhetssystem och möten med vårdnadshavare där kontaktmetoder och hanteringen av andra relevanta frågor beslutas. Enligt uppgift har dessa rutinbeskrivningar fungerat väl och

verksamhetsstödet har kontaktats av andra kommuner för frågor om utformning av liknande rutiner.

Rektor på respektive skola svarar för rutiner för det löpande arbetet under läsårets gång. Friskolor är egna huvudmän och omfattas inte av de rutinbeskrivningar som välfärd skolas verksamhetsstöd har tagit fram.

Socialnämnden

Enheterna under social- och äldredirektör, vilket innefattar samtliga verksamheter som socialnämnden ansvarar för, har en gemensam rutinbeskrivning för hanteringen av kunder med skyddade personuppgifter. Beskrivningen finns tillgänglig i ledningssystemet Stratsys för samtliga medarbetare inom enheterna. Nämnden har inte beslutat om rutinbeskrivningen. Intervjuade inom både verksamheten och nämnden upplever att frågan är verksamhetsnära och att nämnden inte bör besluta om rutinbeskrivningar inom området. Intervjuade nämndledamöter menar också att det finns en risk att mer övergripande styrdokument beslutade av nämnden endast blir en pappersprodukt. Vissa intervjuade tjänstepersoner har uppgett att det eventuellt finns ett behov av en mer övergripande policy för att styra arbetet med skyddade personuppgifter.

Nämnden för arbete och försörjning

Rutinbeskrivningen inom nämnden för arbete och försörjnings ansvarsområde gäller för hela arbets- och etableringsenheten. Rutinbeskrivningen avser hur arbete ska bedrivas med kund som har skyddade personuppgifter samt hantering av personuppgiftsincidenter. Nämnden har inte beslutat om rutinbeskrivningarna. Intervjuade uppger att det finns vissa utvecklingsmöjligheter för dessa rutinbeskrivningar (se avsnitt 5.1 och 5.2). *Sekretessmarkerad kund* är senast uppdaterad mars 2023. Enligt uppgift har rutinbeskrivningen nyligen tagits fram efter att frågan har diskuterats internt under en längre tid.

Utbildningsnämnden

Utbildningsenheten hanterar främst personer med skyddade personuppgifter inom ramen för ansökan om plats till förskola eller skola. Detta genomförs manuellt och rutinbeskrivningen utgör en beskrivning av tillvägagångssättet och processbeskrivning för att barn med skyddade personuppgifter ska placeras och registreras på rätt skola. Nämnden har inte beslutat om rutinbeskrivningen och intervjuade inom både verksamheten och nämnden upplever att nämnden lämpligen inte bör besluta om rutin för arbetet i frågan då området är verksamhetsnära.

3.2.3 Det finns behov av ytterligare kompetensutveckling

Vid intervju har uppgetts att det är kommunstyrelsens ansvar att tillse att det finns tillräckliga utbildningar på det övergripande planet inom området. Något sådant ansvar framgår dock inte i styrelsens reglemente. Ledningsstaben tar fram utbildningar för detta syfte. Det är dock varje enskild enhetschef som ska tillse att medarbetare har gått igenom tillräckliga utbildningar och ledningsstaben gör inga kontroller av efterlevnad. Utbildningarna är inte obligatoriska. Ledningsstaben har periodvis skickat ut uppmaningar till medarbetare inom andra enheter att genomgå dessa utbildningar, där drygt hälften har följt länkarna som bifogats. Vissa kommunövergripande utbildningar är av relevans för området. Det finns bland annat en utbildning av hantering av GDPR och en utbildning i informationssäkerhet. Dessa

omfattar offentlighet, sekretess och vikten av att hantera personuppgifter korrekt, men inte specifikt information om skyddade personuppgifter.

Det finns inga kommunövergripande utbildningar som specifikt rör hantering av skyddade personuppgifter. Intervjuade som hanterar frågan på central nivå upplever att det vore överflödigt med en utbildning om hanteringen av skyddade personuppgifter till alla verksamheter då många verksamheter och många medarbetare aldrig berörs av frågan.

Varken kommunstyrelsen eller de granskade nämnderna har gjort någon särskild uppföljning av arbetet med skyddade personuppgifter avseende kompetensutveckling och rutinförankring.

Socialnämnden

Varken omsorgsenheten eller barn- och familjeenheten har regelbundna utbildningar som specifikt behandlar skyddade personuppgifter. En introduktion genomförs för alla nyanställda där det klarläggs hur arbete ska bedrivas och var relevanta dokument går att återfinna. Om detta alltid genomförs som tilltänkt är dock osäkert då en intervjuad handläggare uppger sig inte känna igen detta. Skyddade personuppgifter ingår i denna introduktion. Därutöver sker diskussioner på arbetsplatsträffar och interna möten där frågan ibland behandlas. Intervjuade har fört fram att det viktigaste är att chefer och handläggare som regelbundet möter frågan har bra kunskap. Upplevelsen bland intervjuade är också att exempelvis handläggare som hanterar våld i nära relationer är väl bevandrade med dokument, men att vissa andra delar inte är lika insatta. Samtidigt har vissa intervjuade också sett en risk att medarbetare som inte är helt vana gör som andra har gjort tidigare, vilket kan medföra negativa konsekvenser om det tidigare agerandet har varit felaktigt. Det har inte kunnat klarläggas om denna riskanalys är baserad på en specifik händelse eller utgör en mer allmän uppfattning. Det finns en återkommande kort utbildningsserie som avser informationssäkerhet, men denna har inte behandlat skyddade personuppgifter specifikt. Det har även funnits informationstillfällen där processen för hanteringen av personuppgiftsincidenter har förklarats.

Nämnden för arbete och försörjning

Arbets- och etableringsenheten genomför inga egna regelbundna utbildningar för medarbetare som specifikt handlar om skyddade personuppgifter. Enheten har dock en utbildning för nyanställda som inkluderar information om arbetssätt för hantering av skyddade personuppgifter. Informationstillfällen om GDPR och dataskydd har förts in i årshjulet och intervjuade är öppna för att motsvarande skulle kunna införas för skyddade personuppgifter.

Vissa medarbetare har deltagit i utbildningar om skyddade personuppgifter som Skatteverket anordnar. Efter dessa har erfarenheterna tagits med och diskuterats på möten inom enheten. Handläggare som hanterar fall med våld i nära relationer har deltagit i en utbildning inom det området som enligt uppgift också omfattar skyddade personuppgifter.

Utöver utbildningar sker en förankring av rutinerna genom att frågan diskuteras på enhetens regelbundna möten och arbetsplatsträffar. De dokumenterade rutinerna i sig diskuteras i huvudsak på förekommen anledning, exempelvis vid avvikelser, men enligt uppgift förs också en mer allmän diskussion om sekretessarbete. Intervjuade upplever dock att det finns en god kunskap om hur arbetet med skyddade personuppgifter ska bedrivas och att medarbetare kan be om hjälp vid behov. Samtidigt har intervjuade också varit öppna för att skyddade personuppgifter skulle kunna införas som en bestämd och periodvis återkommande punkt för enhetens interna möten.

Utbildningsnämnden

Utbildningsenheten har inte några särskilda utbildningar för hanteringen av skyddade personuppgifter. En diskussion har enligt uppgift förts inom enheten gällande utbildning inom området, men uppfattningen bland de intervjuade är att arbetet med rådande rutin fungerar bra och att medarbetare som behöver vara väl insatta i arbetet också är det. Diskussioner förs i övrigt på interna möten vid behov.

3.3 Bedömning

Vår bedömning är att det saknas styrande dokument för hantering av skyddade personuppgifter. Det finns vissa kommunövergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men det finns inget beslutat kommunövergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter. Vi noterar att det finns vissa kommunövergripande rutinbeskrivningar med bäring på området, samt en vägledning inom området från juridik- och kanslistaben på kommunens hemsida. Vår bedömning är att avsaknaden av övergripande styrdokument utgör en svaghet i arbetet. Givet att det är ett område som kräver stor varsamhet och att det inte alltid finns en tillräcklig insyn i frågan på enhetsnivå är vår bedömning att det bör beslutas om ett övergripande styrande dokument för hanteringen av skyddade personuppgifter på en generell nivå, exempelvis som en policy.

De granskade nämnderna har inte heller beslutat om några styrdokument inom området. Vi instämmer i att området är verksamhetsnära och nämnderna inte bör besluta om några rutinbeskrivningar, men vår bedömning är att de bör besluta om en riktning i arbetet. Detta är särskilt relevant med hänsyn till att det inte finns kommunövergripande styrdokument. Vi noterar att varje enhet har tagit fram egna rutinbeskrivningar för hanteringen av skyddade personuppgifter. Vi bedömer således att det finns rutiner inom området men att dessa inte har förutsättningar att spegla de styrande dokumenten då det inte finns några styrande dokument. Enheternas rutinbeskrivningar utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att de har utrymme för utveckling.

Enheterna under de granskade nämnderna har alla liknande tillvägagångssätt för att göra rutinerna kända. Rutiner diskuteras på interna möten och arbetsplatsträffar, chefer kan uppmärksamma medarbetare på rutinerna vid behov och de diskuteras också på förekommen anledning. Rutinbeskrivningarna säkerställer delvis en tillräcklig vägledning på såväl övergripande som detaljerad nivå för kommunens medarbetare. Vi bedömer att de bör kompletteras efter genomförd risk- och väsentlighetsanalys.

Utöver rutinförankring genom interna diskussioner genomförs inte någon övergripande och systematisk kompetensutveckling specifikt för hanteringen av skyddade personuppgifter. Det finns kommunövergripande utbildningar inom exempelvis informationssäkerhet och en juridisk introduktionskurs för nyanställda som omfattar personuppgiftshantering generellt men inte skyddade personuppgifter specifikt. Enheterna under de granskade nämnderna har till största del inte heller genomfört några utbildningar eller liknande kompetensutveckling för hanteringen av skyddade personuppgifter, med undantag för arbets- och etableringsenheten. Utifrån detta bedömer vi att det inte genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter, men vi noterar att det genomförs fortlöpande kompetensutveckling som har relevans för området, exempelvis inom informationssäkerhet och GDPR.

Baserat på den begränsade kompetensutvecklingen som finns och utvecklingsområdena i styrdokument och arbetsrutiner bedömer vi att det inte finns ett tillräckligt stöd till medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter.

Det finns inga kommunövergripande styrdokument inom området men enheterna är medvetna om att de ska bedriva ett eget arbete med skyddade personuppgifter. Vi noterar att varken kommunstyrelsen eller de granskade nämnderna har genomfört någon särskild uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter. Med hänsyn till Nackas kommuns styrmodell och avsaknaden av övergripande styrdokument bedömer vi att det skulle finnas ett värde i att nämnderna och kommunstyrelsen stärker uppföljningen inom området. Vår bedömning är därför att respektive *enhet* till viss del har tillsett tillräcklig uppföljning och kontroll av rutinbeskrivningarnas efterlevnad, men att kommunstyrelsen och nämnderna inte är involverade i arbetet i tillräcklig utsträckning.

4. Riskbedömningar

Riskanalys handlar om att identifiera interna och externa risker som en organisation riskerar att utsättas för. Till analysen hör också att kvantifiera hur stor sannolikhet det är att identifierad risk inträffar samt vilka konsekvenserna skulle bli för organisationen. Utifrån verksamhetens behov kan det finnas anledningar att göra riskanalyser på olika nivåer och i olika omfattning i organisationen för att hantera risker på ett ändamålsenligt sätt.

4.1 Risken för och konsekvensen av röjning av skyddade personuppgifter har inte analyserats inom ramen för internkontrollarbetet

Risker för röjning av skyddade personuppgifter ingår inte i någon av kommunstyrelsens eller de granskande nämndernas respektive internkontrollplaner för 2023. Det finns dock risker som har identifierats som tangerar frågor kopplade till skyddade personuppgifter. Bland intervjuade finns därutöver en samlad bild av att risken för röjning av skyddade personuppgifter diskuteras internt inom de olika verksamheterna och att riskanalyser genomförs kontinuerligt i det dagliga arbetet, dock inte inom ramen för internkontrollarbetet.

Kommunstyrelsen

I kommunstyrelsens *Internkontrollplan 2023*[6] ingår *"Bristande efterlevnad av dataskyddsförordningen"* och *"Brister i informationssäkerhet"* som riskområden, med en risknivå på hög (12) och medium (9). Kommunstyrelsen har inte genomfört någon riskanalys i annan form inom området. Av intervju har framkommit att hanteringen av skyddade personuppgifter är en fråga som ofta ingår i riskanalyser avseende specifika system. För välfärd skolas verksamhetsstöd har inte en formell riskanalys som inkluderar skyddade personuppgifter genomförts, men intervjuade betonar att processen som ledde till framtagandet av den nuvarande rutinen utgick ifrån en större, men informell, risk- och väsentlighetsanalys inom området.

Socialnämnden

I *Internkontrollplan för socialnämnden år 2023*[7] ingår *"Bristande efterlevnad av dataskyddsförordningen"* som riskområde med risknivå medium (6). Socialnämnden har inte genomfört någon riskanalys i annan form inom området. Vid intervju har framförts att risken avseende skyddade personuppgifter, särskilt kopplat till sannolikheten för röjning, inte har bedömts vara stor nog för att inkluderas i internkontrollen. Om ett flertal incidenter skulle inträffa skulle också riskbedömningen se annorlunda ut. Intervjuade upplever samtidigt att det är en fråga som analyseras och diskuteras internt och att det skulle upptäckas om det fanns större brister. Av intervju har också framkommit att risken avseende röjning av skyddade personuppgifter har diskuterats bland annat avseende det verksamhetssystem som omsorgsenheten och barn- och familjeenheten använder sig av.

Nämnden för arbete och försörjning

I nämnden för arbete och försörjnings *Internkontrollplan 2023*[8] ingår *"Avbrott, intrång eller fel i verksamhetssystem"* vilket inkluderar risk för personuppgiftsincidenter som ett riskområde

[6] Fastställd av kommunstyrelsen 2022-12-05 § 311.

[7] Fastställd av socialnämnden 2022-12-13 § 164.

[8] Fastställd av arbets- och företagsnämnden, nuvarande nämnden för arbete och försörjning, 2022-12-14 § 70.

med risknivå hög (16). Nämnden för arbete och försörjning har inte genomfört någon riskanalys i annan form inom området. Intervjuade har uppgett att det skulle kunna finnas ett värde i att inkludera skyddade personuppgifter i internkontrollplanen då konsekvenserna vid röjning kan vara allvarliga. Vidare har intervjuade uppmärksammat den riskanalys som görs i samband med informationsklassning som delvis relevant för området. Den riskanalysen utgår dock från det övergripande sekretessarbetet och avser inte specifikt skyddade personuppgifter.

Utbildningsnämnden

I *Internkontrollplan utbildningsnämnden 2023*[9] ingår *"Personuppgifter sprids på ett sätt som strider mot regelverket"* som riskområde med risknivå medium (9). Utbildningsnämnden har inte genomfört någon riskanalys i annan form inom området. Av intervju har framkommit att röjningen av skyddade personuppgifter inte har betraktats som en tillräckligt allvarlig risk att ta med i internkontrollplanen och intervjuade betraktar risken för röjning inom ramen för utbildningsenhetens verksamhet som väldigt liten. Frågan har dock enligt uppgift diskuterats löpande och de intervjuade upplever att det finns en god medvetenhet inom enheten.

Säkerhetsaspekter

Ingen enhet har genomfört någon riktad analys kopplade till potentiella säkerhetsrisker i anslutning till hantering av antingen kunder eller medarbetare med skyddade personuppgifter. Det uppges dock att handläggare som hanterar kunder med skyddade personuppgifter vid behov anpassar arbetsform vid exempelvis besök, både för att skydda sig själva och att skydda kunden. Detta är dock inte dokumenterat i någon särskild rutin för någon av enheterna. Varför framgår inte.

Intervjuade inom enheterna har inte bedömt att en analys gällande medarbetare med skyddade personuppgifter har varit relevant. Intervjuade vid ledningsstaben och vid personalenheten uppger att det inte genomförs någon särskild säkerhetsanalys när personer med skyddade personuppgifter ska anställas och att ansvaret för eventuella säkerhetsaspekter ligger hos ansvarig chef, med stöd av kommunens säkerhetsenhet vid behov.

4.2 Bedömning

Kommunstyrelsen och de granskade nämnderna har inte analyserat risken för att skyddade personuppgifter röjs, vilket vi bedömer är en brist. Skyddade personuppgifter ingår inte i någon av kommunstyrelsens eller de granskade nämndernas internkontrollplaner och har inte ingått i de formella risk- och väsentlighetsanalyserna. Vi noterar dock att enheterna har genomfört vissa riskbedömningar inom området. Intervjuade menar att frågan har behandlats internt vid möten och arbetsplatsträffar och vår bedömning är att det finns en riskmedvetenhet i enheterna. Med hänsyn till de allvarliga konsekvenser som en röjning av skyddade personuppgifter kan få ser vi att området åtminstone bör utvärderas i risk- och väsentlighetsanalys. Detta kan också stärka kommunstyrelsens och nämndernas insyn och uppföljning inom området.

Vad gäller säkerhetsfrågor kopplade till skyddade personuppgifter har ingen enhet genomfört någon formell riktad analys kopplade till potentiella säkerhetsrisker i anslutning till hantering antingen medborgare eller medarbetare med skyddade personuppgifter. Vi ser dock att det finns en säkerhets- och riskmedvetenhet inom enheterna avseende arbetet med skyddade

[9] Fastställd av utbildningsnämnden 2022-12-08 § 74.

personuppgifter, bland annat genom att det finns en riskbedömning i anslutning till utförande av arbetet. Då varken kommunstyrelsen eller de granskade på något spårbart sätt tagit del av dessa eller säkerställt att arbetet är tillräckligt bedömer vi dock att de inte har analyserat säkerhetsfrågor kopplade till skyddade personuppgifter.

5. Kontrollaktiviteter – Nämndernas rutiner och arbetssätt

Åtgärder eller ”kontrollaktiviteter” utgörs av de aktiviteter som en organisation företar för att minska eller eliminera risker. Kontrollaktiviteter anges ofta i en internkontrollplan och syftar då till att följa upp att verksamhetens kontroller fungerar ändamålsenligt (se avsnitt 4.1). Verksamhetens åtgärder/kontroller finns ofta integrerade i processer och kan se olika ut, till exempel inom ramen för dataskyddsarbetet/informationssäkerhetsarbetet, stöd och behörighet i IT- och verksamhetssystem, interna och externa kommunikationskanaler samt hanteringen av medarbetare med skyddade personuppgifter. Gemensamt är att aktiviteterna syftar till att reducera risker.

Varken kommunstyrelsen eller de granskade nämnderna har beslutat om några styrande dokument inom området. Kommunstyrelsen och de granskade nämnderna har inte heller tagit del av någon uppföljning av det arbete som enheterna bedrivit eller på något spårbart sätt säkerställt att åtgärder vidtas av de enheter som kommunstyrelsen eller respektive nämnd har ansvar för. Vid intervju har kommunstyrelsens och de granskade nämndernas presidier uppgett att de känner sig trygga med hanteringen av skyddade personuppgifter inom sina respektive ansvarsområden. Vi noterar att de inte har gjort några systematiska eller återkommande kontroller för att säkerställa att detta är berättigat. Intervjuade nämndledamöter har dock också menat att det kan vara ett aktuellt för respektive nämnd att fråga enheterna om deras arbetsrutiner.

5.1 Behandling av skyddade personuppgifter i IT- och verksamhetssystem

Det finns inget övergripande beslut gällande vilken utformning och funktionalitet IT- och verksamhetssystem ska ha avseende skyddade personuppgifter. Varje verksamhet har möjlighet att själv utforma arbetet med skyddade personuppgifter i deras respektive verksamhetssystem. Exempelvis avgör verksamheterna själva, inom ramen för systemens funktionalitet, om behörighet och åtkomst för att arbeta med skyddade personuppgifter ska vara begränsat till några få eller allmänt tillgänglig. Vi noterar dock att det i den av juridik- och kanslistaben framtagna rekommendationen på kommunens hemsida framförs att åtkomsten till personuppgifter bör begränsas genom strikt behörighetsindelning. Verksamheterna har möjlighet att önska kravställning om funktionalitet för hantering av skyddade personuppgifter vid upphandling, men intervjuade uppger också att behovet av systemanpassning inom det området måste balanseras mot övriga krav på verksamhetssystem.

Informationsägare har ansvar för informationssäkerhetsarbetet. Detta inkluderar informationsklassning och systemsäkerhetsanalyser.

[redacted]

Kommunstyrelsen

Merparten av enheterna under kommunstyrelsen hanterar till stor del inte skyddade personuppgifter i sina verksamhetssystem. Eventuella personuppgifter i ärendehanteringssystemet eller i handlingar som ska läggas fram till kommunstyrelsen hanteras manuellt.

Inom ramen för välfärd skola har varje enskild kommunal skola till uppgift att administrera sina system. Välfärd skolas verksamhetsstöd har som tidigare beskrivits (se avsnitt 3.2) tagit fram en vägledning för att möjliggöra barn med skyddade personuppgifter att läggas in i källsystem

och elevhanteringssystem utan att faktiska personuppgifter framgår. Detta kräver en manuell inläggning i systemen. För att de kommunala skolorna ska kunna hantera elever med skyddade personuppgifter i sina system krävs således att de får korrekt information. Om en elev med skyddade personuppgifter ska börja på en skola kommer den informationen från utbildningsenheten vid ansökan, men om en elev får skyddade personuppgifter under pågående läsår måste vårdnadshavare informera om det. Detta är på grund av systemtekniska begränsningar.

Socialnämnden

Barn- och familjeenheten och omsorgsenheten använder samma verksamhetssystem för att hantera brukare. I detta system går det att sekretessmarkera personer. Detta innebär att uppgifter om exempelvis adress inte framgår. Under en längre tid krävdes ingen särskild behörighet i systemet för att komma åt enskilda akter. Alla akter, inklusive de som är sekretessmarkerade, var tillgängliga för alla inom organisationen. Exempelvis kunde alla inom omsorgsenheten se alla sekretessmarkerade kunder hos omsorgsenheten. Intervjuade uppger att detta sågs som en säkerhetsrisk, särskilt avseende att vissa hade behörighet i flera organisationer vilket ledde till att de kunde se alla sekretessmarkerade inom hela socialnämndens ansvarsområde. Frågan påtalades enligt uppgift till leverantören under en längre tid. Diverse tekniska problem försenade införandet av ytterligare begränsningar. Nyligen har dock enheten själva infört behörighetsbegränsningar så att [redacted] kan se det.

Av intervju har framkommit att enheterna rör sig mot en helt digital hantering av ärenden, vilket innebär att en del uppgifter måste skannas in i verksamhetssystemet. Vid intervju uppgav vissa en osäkerhet kring hur skyddade personuppgifter ska hanteras i och med detta och svårigheterna kring behörighetsbegränsningar i systemet. Då behörighetsbegränsningar nu har införts borde problemet vara löst.

Intervjuade ser också att systemstödet skulle kunna stärkas med begränsningar i vad som kan skrivas i de sekretessmarkerade akterna. I nuläget är det till stor del upp till handläggarna själva att avgöra vad som är lämpligt att skriva in. Detta uppges fungera bra om en handläggare är vad vid att hantera skyddade personuppgifter, men för en handläggare som inte är tillräckligt rutinerad upplever intervjuade att tydligare begränsningar i systemet vore hjälpsamt.

[redacted] Av nämndens internkontrollplan för 2023 framgår att loggkontroll ska genomföras enligt fastställd rutin som ett moment för att hantera risken för bristande efterlevnad av dataskyddsförordningen, dock inte med anledning av skyddade personuppgifter.

Nämnden för arbete och försörjning

Det går att sekretessmarkera personer i arbets- och etableringsenhetens verksamhetssystem. Systemet utgår ifrån folkbokföringen vilket innebär att personer med skyddade personuppgifter per automatik blir sekretessmarkerade när de läggs. Detta medför att systemet markerad att personen är sekretessmarkerad samt att vissa uppgifter som exempelvis adress inte framgår. [redacted] Om en person ansöker digitalt om ekonomiskt bistånd framgår inte namn, [redacted]

[redacted]
Enligt uppgift har ett arbete påbörjats med att helt digitalisera alla akter, men det är inte slutfört.

Det finns [redacted] Detta har varit ett avsiktligt beslut i syfte att förebygga personberoende vid ärendehantering. Intervjuade påtalar att en begränsning i behörighet att hantera sekretessmarkerade personer också skulle kunna innebära en risk för att personer med skyddade personuppgifter får sämre service om exempelvis de som hanterar ärenden involverande skyddade personuppgifter blir sjuka. Intervjuade uppger också att det är mot reglerna för handläggare att utan anledning öppna upp andra handläggares ärenden och att risken med avsaknaden av behörighetsbegränsning också är liten då det över lag finns en stark sekretessmedvetenhet, särskilt för sekretessmarkerade personer.

[redacted]

Utbildningsnämnden

Utbildningsenheten har en manuell hantering av barn med skyddade personuppgifter. Elever med skyddade personuppgifter läggs in manuellt i enhetens verksamhetssystem. Denna process följer en dokumenterad rutin, se avsnitt 3.2. Hanteringen är manuell då en automatisk hantering inte är möjlig i de nuvarande verksamhetssystemen. Barn med skyddade personuppgifter kan markeras i systemet. [redacted]

Det finns inget automatiserat system för att stämma av om en elev har skyddade personuppgifter. Vårdnadshavare måste skicka in ansökan om förskol- eller skolplats via telefon eller via att en fysisk blankett skickas in. Om en elev får skyddade personuppgifter under läsåret kan vårdnadshavare meddela detta till utbildningsenheten, exempelvis via telefon. Detta kan även upptäckas om utbildningsenheten gör en manuell kontroll via Skatteverkets folkbokföring.

Enligt uppgift har en upphandling påbörjats för ett nytt verksamhetssystem. Hos enheten finns en förhoppning att ett eventuellt nytt system kan medföra en mer automatisk hantering. Utbildningsenheten genomför inte upphandlingen men har möjlighet kravställa. Oavsett kravställning är utfallet dock beroende av marknadsutbudet. I nuläget finns en upplevelse bland intervjuade att den manuella hanteringen fungerar och är trygg, om än mer tidskrävande än vad en automatisk hantering eventuellt skulle kunna vara.

Enhetens verksamhetssystem är enligt uppgift informationsklassade. Denna klassning har genomförts i samband med den nya upphandlingen.

[redacted] Intervjuade ser inte att det finns någon större risk för röjning inom ramen för utbildningsenhetens verksamhetsområde. Denna bedömning är dock inte utifrån en formell riskanalys.

5.2 Vidtagna åtgärder

Kommungemensamma åtgärder

Kommunen har ett verktyg, *Säkra meddelanden*, som är tänkt att möjliggöra att skicka meddelanden med känslig information på ett säkert och lagenligt sätt. Alla inom kommunen har tillgång till detta verktyg och samtliga enheter under de granskade nämnderna använder sig, i varierande grad, av *Säkra meddelanden*. För att kunna skicka eller att ta emot meddelanden krävs inloggning med bank-id eller annan stark autentisering.

Flera enheter tar av och till emot fysisk post. Post som ska till dessa kommer in till receptionen och fördelas sedan internt. [redacted]

Kommunstyrelsen

Det vardagliga arbetet med skyddade personuppgifter inom välfärd skolas område hanteras på skolnivå. Välfärd skolas verksamhetsstöd har somt tidigare konstaterats tagit fram rutiner som stöd till skolorna. Utöver systemtekniskt stöd framgår av dessa också mer allmän information om hur barn med skyddade personuppgifter ska hanteras. Av denna framgår att skolan ska ha ett möte med vårdnadshavare där dessa gemensamt går igenom en checklista för hur barnet ska hanteras. Checklistan täcker ett flertal områden, både exempelvis hur vårdnadshavaren vill att kontakt med skolan ska ske och det ansvar som vilar på den skyddade person och på vårdnadshavaren. Inför varje nytt läsår ska rektor, eller av rektor utsedd person, kontakta vårdnadshavaren och kontrollera om det finns förändringar gällande sekretesskyddet och om vårdnadshavaren vill ändra något i överenskommelsen med skolan. Vidare framgår också andra regler för hur frågan ska hanteras, exempelvis att grundskolebetyg ska förvaras fysiskt i ett låst arkiv på skolan och att post till personer med skyddade personuppgifter bör skickas via Skatteverkets förmedlingsuppdrag.

Det görs ingen särskild uppföljning av hur dessa rutiner efterlevs i praktiken.

Socialnämnden

Enheterna under socialnämnden har tagit fram en egen arbetsrutin för hanteringen av personer med skyddade personuppgifter. Av rutinen framgår bland annat handlingar som skickas digitalt ska skickas med hjälp av säkra meddelanden. Om handläggare är osäkra ska de dessutom kontrollera att ingen annan person har tillgång till personens bank-id. Post ska skickas via Skatteverkets förmedlingsuppdrag. Motringning ska genomföras om någon ringer och uppger sig komma från en annan myndighet och begär ut uppgifter om person med skyddade personuppgifter. Vidare ska handläggare tillse att tjänsteman som representerar den enskilde har fullmakt. Av intervju har framkommit en viss osäkerhet gällande hur känd rutinen är som ett eget dokument, men rutinen stämmer överens med det övergripande arbetssättet som det har beskrivits på intervju.

Utöver rutinen betonar intervjuade att hanteringen av skyddade personuppgifter till stor del sker utifrån det vanliga sekretessarbetet. Detta avser då inte specifikt personer med skyddade personuppgifter, utan alla personer som enheterna hanterar. Det gäller som rutin att personuppgifter inte ska mejlas eller förvaras i teams.

Fysiska akter förvaras i låsta arkiv och papper ska aldrig lämnas framme på skrivbord. Handläggare ska i stället plocka fram det material de behöver ur arkiven vid behov och

därefter lägga tillbaka materialet när de är klara. Detta är av begränsad relevans i det dagliga arbetet då enheterna ska fasa ut fysiska akter. Intervjuade upplever dock att detta efterlevs bra – material lämnas inte framme obevakat.

Intervjuade upplever att det är vanligt att handläggare stämmer av kontaktvägar, önskade kontakttider och liknande information med alla brukare, oavsett om de har skyddade personuppgifter eller ej. Detta är dock inte en beslutad rutin. Relevant information från dialog med kunder antecknas i journal eller i verksamhetssystemet, vilket inkluderar kommunikationsvägar och liknande.

Det finns inget standardiserat arbetssätt för samverkan med andra enheter som exempelvis utbildningsenheten eller arbets- och etableringsenheten, utan det sker efter behov.

Nämnden för arbete och försörjning

Arbets- och etableringsenheten har tagit fram en egen rutinbeskrivning för hanteringen av personer med skyddade personuppgifter, *Sekretessmarkerad kund*. Av beskrivningen framgår att ny kund alltid ska tillfrågas om önskade kontaktvägar. Detta innefattar dels hur personen vill bli kontaktad, dels vilka kontaktuppgifter som enheten ska kontakta. Vidare ska handläggare stämma av vilka uppgifter som personen önskar ska framgå i verksamhetssystemet. Kunden ska också få bestämma vart post ska skickas. Av intervju har framkommit att enheten använder sig av Skatteverkets förmedlingstjänst om det önskas av kunden. Enligt uppgift dokumenterar sedan handläggare efter avstämning med kunden önskade kommunikationsvägar och liknande uppgifter i journalen.

Utöver rutinbeskrivningen menar intervjuade att merparten av arbetet med skyddade personuppgifter hanteras inom ramen för det ordinarie sekretessarbetet, dock med en ytterligare betoning på vikten av sekretess och varsamhet. Detta inkluderar ett antal olika åtgärder för att hantera sekretessfrågor, även utöver de som medföljer automatiskt i verksamhetssystemet. Inom enheten gäller allmänt att kommunikation med kund i första hand ska ske via telefonsamtal. Personuppgifter ska aldrig mejlas och i regel ska handläggare undvika att mejla om möjligt. Om underlag behöver skickas kan det hanteras genom post eller genom säkra meddelanden. Intervjuade har dock påtalat att det finns problem med säkra meddelanden avseende att det är enkelt att förväxla personer som meddelanden skickas till. Det har hänt att underlag har skickats till fel handläggare i en situation där det är två medarbetare som har samma namn.

Fysiska uppgifter som inkommer till enheten ska i regel skannas in och därefter makuleras och förvaras i låsta tunnor. I undantagsfall då uppgifter inte omedelbart kan skannas in ska de förvaras i låsta lådor som handläggarna själva har hand om. All post som kommer in till enheten hämtas i receptionen av en administratör och förvaras i ett låst postrum. Om administratören har fullmakt öppnar denne förslutna kuvert och skannar in underlagen som därefter makuleras.

Enheten delar kontor med utbildningsenheten. Som en del i detta har enheten ett förebyggande arbete där det undviks att exempelvis diskutera känsliga eller sekretessbelagda uppgifter öppet. Sådana diskussioner ska i stället hanteras i mindre grupprum. Det finns också en rutin att datorer inte ska lämnas olåsta. Intervjuade ser dock att det finns en viss risk i att enheten inte har egna kontor. Detta gäller särskilt med hänseende till att utbildningsenheten svarar under en annan nämnd som har sitt eget personuppgiftsansvar. Vid intervju har framförts att instruktioner för hanteringen av denna risk bör inkluderas i enhetens rutin för sekretessbelagd kund.

Kommunikation med andra enheter sker i den graden det är relevant för ärendet. För detta gäller som rutin att sekretessbelagd information inte delas utan åtminstone muntlig, helst skriftlig, bekräftelse från kund att det är acceptabelt.

Utbildningsnämnden

Som tidigare konstaterats hanterar utbildningsenheten barn med skyddade personuppgifter manuellt. Vårdnadshavare med barn med skyddade personuppgifter kan endast söka skolplats via telefonsamtal eller via en fysisk blankett. Utbildningsenheten har som regel att kontakt med vårdnadshavare som har barn med skyddade personuppgifter inte ska ske via mejl. Om en vårdnadshavare har mejlat enheten ringer enheten upp vårdnadshavaren – de mejlar inte tillbaka. Säkra meddelanden används och då i huvudsak för att skicka uppgifter till skolorna.

I samband med intervju identifierades risk när barn har skyddade personuppgifter på grund av hot från en av föräldrarna. Denne förälder kan fortfarande vara vårdnadshavare och besitta rätt att ta del av uppgifter som rör barnet. Båda vårdnadshavarna har laglig rätt att få kallelser till bokförd hemadress. Det finns en "lucka i lagen" som är svår att undvika. I vissa fall saknas kunskap om att den andra vårdnadshavaren är hotet som eleven ska skyddas från.

Ansökan om skolplats via fysisk blankett lämnas in i receptionen och hamnar hos utbildningsenheten via den interna postgången. I detta finns som tidigare konstaterat en möjlig risk.

När barn med skyddade personuppgifter ska börja på en förskola eller skola ska denna se till att barnets vårdnadshavare skriver på ett kontrakt. Detta kontrakt skickas sedan till utbildningsenheten som förvarar kontrakten i ett låst arkivskåp med begränsad åtkomst.

Då utbildningsenheten endast arbetar med utplacering av barn samt fördelning av skolpeng upprättar inte enheten några handlingsplaner för eleverna. Det är i stället de individuella skolornas ansvarsområde.

Som tidigare konstaterats delar utbildningsenheten kontor med arbets- och etableringsenheten. Samma risker med detta finns för utbildningsenheten som för arbets- och etableringsenheten.

5.3 Hantering av medarbetare med skyddade personuppgifter

Personal- och löneadministration hanteras centralt i kommunen av kommunens personalenhet. Anställda med skyddade personuppgifter hanteras av en begränsad mängd medarbetare. All kontakt mellan personalenheten och medarbetarna med skyddade personuppgifter ska gå via enhetschef, även om medarbetaren själv vill kunna kontakta personalenheten direkt. Detta inkluderar att enhetschef får lämna över påskrivet fysiskt anställningsavtal till personalenheten. Dessa avtal förvaras i ett låst arkivskåp. I nuläget används inte digitala anställningsavtal för medarbetare med skyddade personuppgifter, men intervjuade har uppgett att det kan komma att införas i framtiden då det digitala underskriftsverktyg som kommunen använder sig av är GDPR-säkert. Personer med skyddade personuppgifter framgår inte på exempelvis kommunens lönelistor. Om en person med skyddade personuppgifter är en del av en rekryteringsprocess ska personens ansökan hanteras manuellt. Om personen har skickat in sin ansökan via det vanliga digitala systemet för rekrytering ska denna ändå hanteras manuellt därefter.

Personalenheten har inte några rutiner för hur det vardagliga arbetet inom verksamheterna ska hanteras avseende medarbetare med skyddade personuppgifter. I stället ser avdelningen att det får beslutas av enhetschef i samverkan med den enskilde medarbetaren. Av intervju

har framkommit att verksamheterna har liknande perspektiv på hur medarbetare med skyddade personuppgifter ska hanteras. I stort utgår detta från att medarbetare själva får bestämma exempelvis om det vill medverka i bild som används internt och hur många som ska känna till att de har skyddade personuppgifter.

5.4 Bedömning

Vår sammantagna bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att åtgärder har vidtagits för att minska risken för röjning av skyddade personuppgifter. Vi noterar att enheterna dock har vidtagit ett antal olika åtgärder, även om vi också bedömer att det samtidigt finns utrymme för förbättringar som presenteras nedan. Enheterna har upprättat egna rutiner, till viss del beskrivna i rutinbeskrivningar, för hanteringen av skyddade personuppgifter. Dessa har en varierande utformning och innehåller olika mängder detaljer om hur arbetet ska bedrivas.

Merparten av enheterna under kommunstyrelsen hanterar i allmänhet inte skyddade personuppgifter. Det kommunala skolväsendet ligger dock under kommunstyrelsen. Inom skolväsendet har respektive rektor ansvar för hur arbetet med skyddade personuppgifter bedrivs på respektive skola. Välfärd skolas verksamhetsstöd har också tagit fram en rutinbeskrivning till stöd som gäller för samtliga kommunala skolor. Denna täcker in många aspekter av hanteringen av barn med skyddade personuppgifter, vilket inkluderar att upprätta en överenskommelse med vårdnadshavare avseende hur barnet ska hanteras. Vår bedömning är att rutinbeskrivningen är ändamålsenlig och att välfärd skolas verksamhetsstöd har lagt grund för ett fungerande arbete med elever med skyddade personuppgifter på de kommunala skolorna. Samtidigt bedömer vi också att kommunstyrelsen måste säkerställa att skolorna inom välfärd skola också efterlever dessa rutiner.

Enheterna under socialnämnden har tagit fram en gemensam rutinbeskrivning för arbetet med skyddade personuppgifter. Denna täcker i huvudsak hur arbetet med skyddade personuppgifter ska bedrivas, men vissa åtgärder som kommer genom det vanliga sekretessarbetet täcks inte in, exempelvis avstämning med kund om önskade kontaktvägar. [redacted]

Arbets- och etableringsenhetens rutin ger endast en väldigt översiktlig beskrivning om hur arbetet med skyddade personuppgifter ska bedrivas. Mycket av det vardagliga sekretessarbetet, exempelvis att kommunikation med kund i första hand ska göras via telefon, framgår inte av rutinen. Vår bedömning är att även om det kan upplevas överflödigt är det viktigt att rutinbeskrivningen betonar vikten av sekretessarbetet. Vi instämmer med intervjuade att rutinbeskrivningen också bör inkludera information om kommunikation i kontoret då enheten delar kontorslandskap med utbildningsenheten. [redacted] Vi gör bedömningen att det förvisso finns en rutinbeskrivning inom nämnden för arbete och försörjnings ansvarsområde, men att denna har flera och betydande utvecklingsområden, exempelvis avseende behovet av försiktighet vid muntlig kommunikation i kontorslandskapet.

Utbildningsenheten har tagit fram en egen rutinbeskrivning och processbeskrivning för hanteringen av personer med skyddade personuppgifter. Rutinbeskrivningen avser i huvudsak

den manuella hanteringen av personer med skyddade personuppgifter, men även vissa tillvägagångssätt gällande kommunikation och liknande. Därutöver finns ytterligare åtgärder som vidtas gällande barn med skyddade personuppgifter. Intervjuade menar att det endast finns mycket begränsade röjningsrisker genom enhetens arbete, vilket vi instämmer i. Vi vill dock betona att även om risken är liten, är den möjliga konsekvensen mycket stor. Vår bedömning är att enhetens rutin är ändamålsenlig givet enhetens uppdrag. Vi ser dock samma risk för utbildningsenheten som för arbets- och etableringsenheten avseende de delade kontorslokalerna.

6. Avvikelsehantering

6.1 Rutiner för personuppgiftsincidenter

Incidenter avseende skyddade personuppgifter hanteras inom ramen för den ordinära avvikelsehanteringen för personuppgiftsincidenter. Personuppgiftsincidenter hanteras utifrån en central dataskyddsombudsprocess.

Hanteringen av personuppgiftsincidenter framgår i en rutin framtagen av ledningsstaben. *Guide för hantering av personuppgiftsincidenter* riktar sig till enhetschefer, dataskyddssamordnare och andra som har i uppgift att hantera personuppgiftsincidenter på enhet. Av guiden framgår vad som räknas som en personuppgiftsincident, syftet med att rapportera personuppgiftsincidenter, krav enligt dataskyddsförordningen samt tillvägagångssättet vid en personuppgiftsincident. Vidare framgår att en incident inte behöver anmälas till Integritetsskyddsmyndigheten om det är osannolikt att incidenten lett eller kan leda till bland annat brott mot sekretess eller tystnadsplikt, obehag eller fysisk oro samt fysisk påverkan. Det tydliggörs också att den drabbade ska informeras utan dröjsmål i dessa situationer. Guiden innehåller inte några specifika regler eller instruktioner för hanteringen av skyddade personuppgifter. En processkarta finns som bilaga till guiden vilken tydliggör arbetsflöde och ansvarsfördelning vid personuppgiftsincidenter. Av guiden framgår att enhetschef har delegation att fatta beslut om att, i samråd med dataskyddsombudet, anmäla en personuppgiftsincident till Integritetsskyddsmyndigheten. Av intervju har framkommit att det i praktiken är dataskyddsombudet som genomför själva anmälan, efter beslut från enhetschef.

I guiden uppges också att det preventiva arbetet är en viktig del i incidenthanteringsprocessen. För att framtida incidenter ska kunna förhindras på ett effektivt sätt måste rotorsaken till en incident utredas. Dels måste den direkta orsaken till incidenten analyseras, dels måste även de bakomliggande orsakerna klarläggas. Det framgår ingen specifik arbetsprocess för uppföljningen och det förebyggande arbetet.

Kommunstyrelsen och de granskade nämnderna följer enligt dataskyddsombudets årsrapporter för 2021[10] kommunens centrala process för personuppgiftsincidenter.

Kommunstyrelsen

Enheterna arbetar efter den kommungemensamma processen för personuppgiftsincidenter. Av intervju har beskrivits att för det kommunala skolväsendet under kommunstyrelsens ansvar är det en funktion vid välfärd skolas verksamhetsstöd som, tillsammans med skolchef och personuppgiftsansvarig vid berörd skola, ska ta kontakt med dataskyddsombudet vid personuppgiftsincident.

Det finns ingen gemensam rutin för kommunstyrelsens ansvarsområden för att tillvarata kunskap och erfarenhet efter personuppgiftsincidenter. Varje skola hanterar i stället sådana lärdomar själva och eventuell rutinutvärdering sker på skolnivå och inte övergripande.

[10] Rapporterna för 2022 var fortfarande under arbete vid granskningstillfället.

Av *Delegationsordning för kommunstyrelsen*[11] framgår att enhetschef/rektor/verksamhetschef i samråd med dataskyddsombud får besluta om att anmäla personuppgiftsincident till tillsynsmyndighet.

Socialnämnden

Barn- och familjeenheten och omsorgsenheten arbetar båda utifrån den kommungemensamma processen för personuppgiftsincidenter. Om en avvikelse har upptäckts ska enligt uppgift personen som upptäckt avvikelsen kontakta ansvariga inom enheten, bland annat enhetschef. Därefter följer den centrala processen. Enheterna har ingen separat process för avvikelser som involverar skyddade personuppgifter, utan frågan hanteras inom det vanliga arbetet med personuppgiftsincidenter.

Lärdomar och uppföljning efter incident sker främst genom att händelsen uppmärksammas inom gruppen på interna möten eller arbetsplatsträff.

Av *Delegationsordning Socialnämnden*[12] framgår att enhetschef i samråd med dataskyddsombud får besluta om att anmäla personuppgiftsincident till tillsynsmyndighet.

Nämnden för arbete och försörjning

Enheten för arbete och etablering följer kommunens centrala process för hantering av personuppgiftsincidenter. För detta har enheten också tagit fram en egen *"Rutin för hantering av personuppgiftsincident"*. Av rutinen framgår vad som utgör en personuppgiftsincident och arbetsprocessen när en incident har uppmärksammats. Den som upptäcker incidenter ska samråda med enhetens dataskyddssamordnare, alternativt enhetschef i dataskyddssamordnares frånvaro, och rapportera incidenten i det system som används för den kommungemensamma processen. Samordnaren utreder, bedömer och dokumenterar därefter incidenten och beslutar i samråd med enhetschef om incidenten ska anmälas till IMY. Det formella beslutet om anmälan tas av enhetschefen på delegation. Avvikelser med skyddade personuppgifter hanteras inom ramen för den ordinarie processen för personuppgiftsincidenter och rutinen innehåller inte några specifika instruktioner för skyddade personuppgifter.

Om en avvikelse har noterats diskuteras det enligt uppgift alltid i efterhand på internt möte. Detta involverar bland annat att medarbetare går igenom och diskuterar vad som har hänt, varför det är en avvikelse och hur de ska arbeta för att liknande inte ska hända igen. Vid behov kan detta även involvera att granska och utvärdera rådande rutiner. Intervjuade upplever att det finns ett öppet och lärande samtalsklimat inom enheten. Av rutinen för hantering av personuppgiftsincidenter framgår som en del av processen att eventuella åtgärder ska vidtas för att säkerställa att liknande incidenter inte inträffar igen.

Av *Delegationsordning för nämnden för arbete och försörjning*[13] framgår att enhetschef i samråd med dataskyddsombud får besluta om att anmäla personuppgiftsincident till tillsynsmyndighet.

Utbildningsnämnden

Utbildningsenheten följer den kommungemensamma processen för personuppgiftsincidenter. Enhetschef får koppla in och hantera frågan i samverkan med kommunens dataskyddsombud.

[11] Fastställd av kommunstyrelsen 2022-12-05.

[12] Fastställd av Socialnämnden 2022-09-27.

[13] Fastställd av nämnden för arbete och försörjning 2023-01-17.

Om en formell anmälan till integritetsskyddsmyndigheten ska upprättas sker det som ett delegationsbeslut av biträdande enhetschef. Därutöver ska vårdnadshavare och relevant skola informeras om vad som skett. Det finns ingen egen separat process för skyddade personuppgifter.

Enheten följer upp avvikelser i form av personuppgiftsincidenter på samma sätt som andra avvikelser. Diskussioner förs på interna möten om förebyggande arbete och vad som har gått fel. Personen som är ansvarig för avvikelsen informeras också om vad denna har gjort för fel.

Av *Utbildningsnämnden delegationsordning*[14] framgår att biträdande enhetschef i samråd med dataskyddsombud får besluta om att anmäla personuppgiftsincident till tillsynsmyndighet.

6.2 Bedömning

Vi bedömer att det inte finns ett avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns ingen egen process för avvikelser gällande skyddade personuppgifter. I Nacka kommun finns en central process för hanteringen av personuppgiftsincidenter och avvikelser avseende skyddade personuppgifter hanteras i denna process. Samtliga enheter under de granskade nämnderna följer processen. Av den kommungemensamma guiden för personuppgiftsincidenter framgår inte någon särskild information om skyddade personuppgifter, men utifrån guiden är det i vår bedömning ändå tydligt att avvikelser avseende skyddade personuppgifter måste anmälas till Integritetsskyddsmyndigheten inom 72 timmar. I övrigt framgår dock inte något om att avvikelser med skyddade personuppgifter måste hanteras särskilt skyndsamt.

Enheten för arbete och etablering har en egen rutinbeskrivning för personuppgiftsincidenter som bygger vidare på den kommungemensamma, men inte heller denna berör skyddade personuppgifter. Övriga verksamheter har inga egna dokumenterade rutinbeskrivningar för personuppgiftsincidenter. Vår bedömning är att det behöver tydliggöras att incidenter med skyddade personuppgifter måste hanteras särskilt varsamt och skyndsamt, givet de möjliga konsekvenserna av en röjning. Då incidenter avseende skyddade personuppgifter inte på något sätt särskiljs från övriga personuppgiftsincidenter är vår bedömning även att det finns begränsade förutsättningar för en övergripande uppföljning inom området.

[14] Fastställd av utbildningsnämnden 2022-12-08.

7. Svar på revisionsfrågor

Fråga	Svar
Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?	Nej. Kommunstyrelsen har inte beslutat om något styrande dokument för hantering av skyddade personuppgifter. Juridik- och kanslistaben har tagit fram rutiner för hanteringen av skyddade personuppgifter som finns tillgängliga på kommunens hemsida, men dessa är tänkt att utgöra ett stöd och är inte bindande för de kommunala verksamheterna. De granskade nämnderna har inte beslutat om styrande rutiner, men enheterna under de granskade nämnderna har tagit fram arbetsrutiner utifrån det egna upplevda behovet.
Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?	Upprättade arbetsrutiner görs i huvudsak kända genom interna möten och arbetsplatsträffar på verksamheterna. Det finns inga styrdokument som specifikt avser skyddade personuppgifter, men styrdokument med indirekt relevans för området görs kända på samma sätt. Skyddade personuppgifter diskuteras i huvudsak på förekommen anledning, exempelvis vid avvikelse. I dessa sammanhang förankras, och vid behov, stärks arbetsrutinerna. Ingen av de granskade nämnderna har genomgång av rutiner för hantering av skyddade personuppgifter som ett återkommande moment i exempelvis ett årshjul.
Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?	Nej. Det finns endast övergripande stöd till verksamheterna från de centrala enheterna och det stödet kan inte härledas till beslutade styrande dokument. Verksamheterna har själva tagit fram arbetsrutiner som ger stöd till medarbetare, men dessa är, i varierande grad, i behov av utveckling.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Det finns inga kommunövergripande utbildningar som specifikt avser skyddade personuppgifter, men det finns utbildningar om personuppgiftsfrågor i förhållande till GDPR och om informationssäkerhet. Enstaka medarbetare på enheterna har i varierande grad deltagit i utomstående utbildningar avseende skyddade personuppgifter. Varken kommunstyrelsen eller de granskade nämnderna har beslutat om sådant deltagande eller annan kompetensutveckling, utan det har varit på enheternas egna initiativ.
Har kommunen tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Nej. Det finns inga kommunövergripande styrdokument inom området men respektive enhet är medvetna om att de ska bedriva ett eget arbete med skyddade personuppgifter. Varken kommunstyrelsen eller de granskade nämnderna har genomfört någon uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter. I praktiken genomförs förankring av rutiner av verksamheterna själva, men detta följs inte upp från nämnden eller kommunens ledning.
Har kommunen analyserat risken för att skyddade personuppgifter röjs?	Nej. Skyddade personuppgifter ingår inte i kommunstyrelsens eller de granskade nämndernas internkontrollplaner och har inte ingått i de formella risk- och väsentlighetsanalyserna. Kommunstyrelsen och de granskade nämnderna har inte heller genomfört någon annan riskanalys inom området. Det finns dock en riskmedvetenhet i enheterna, vilket också illustreras av att verksamheterna har tagit fram egna arbetsrutiner, men kommunstyrelsen och nämnderna har inte gjort något för att säkerställa eller kontrollera detta.

Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?	Nej. Kommunstyrelsen och de granskade nämnderna har inte själva genomfört några analyser inom området. De har inte heller tillsett att säkerhetsfrågor analyseras och åtgärder vidtas av enheterna. Ingen enhet har genomfört någon riktad analys kopplade till potentiella säkerhetsrisker i anslutning till hantering antingen medborgare eller medarbetare med skyddade personuppgifter. Det finns emellertid en säkerhets- och riskmedvetenhet inom enheterna avseende arbetet med skyddade personuppgifter. Detta har dock inte säkerställts av kommunstyrelsen eller de granskade nämnderna.
Har kommunen vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter?	Nej. Varken kommunstyrelsen eller de granskade nämnderna har säkerställt att åtgärder har vidtagits för att minska risken för röjning av skyddade personuppgifter. Enheterna har dock på eget initiativ vidtagit ett antal olika åtgärder, även om det också samtidigt finns utrymme för förbättringar. Enheternas rutiner medför ett antal gynnsamma åtgärder, men det finns brister. I granskningen framgår potentiella förbättringsområden per granskad nämnd och kommunstyrelsen.
Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?	Nej. Kommunen har en gemensam och dokumenterad process för hanteringen av personuppgiftsincidenter. Denna inkluderar anmälning till Integritetsskyddsmyndigheten. Avvikelser avseende hanteringen av skyddade personuppgifter ingår i detta system. Det finns dock inget eget särskilt system för att hantera incidenter med skyddade personuppgifter, vilket försvårar möjligheten till uppföljning och att tillvarata erfarenheter från avvikelser.
Hur tillvaratas erfarenhet från avvikelser?	Varje enskild enhet följer upp och tillvaratar erfarenheter från avvikelser. Enligt ledningsstabens guide för hantering av personuppgiftsincidenter är detta en viktig del av avvikelsehanteringen, men det finns inga kommunövergripande instruktioner för hur det ska gå till. I praktiken sker tillvaratagandet av erfarenhet genom interna diskussioner på respektive verksamhets interna möten och arbetsplatsträffar.
Råder det samsyn inom Nacka kommun och dess bolag kring hur skyddade personuppgifter ska hanteras?	Nej. Det finns visserligen en gemensam principiell uppfattning om ansvarsfördelning utifrån Nacka kommuns styrmodell. Det råder dock inte samsyn gällande arbetsrutiner och det operativa arbetet med skyddade personuppgifter. Exempelvis har olika enheter gjort olika bedömningar gällande digital kontra manuell hantering och gällande behörighetsbegränsningar. Detta speglar också avsaknaden av kommunövergripande styrdokument, vilket gör att saknas en gemensam inriktning för hanteringen av skyddade personuppgifter inom kommunen. Därutöver har bolagen (NEAB och NVOA) granskats inom ramen för lekmannarevisionen. Det råder inte samsyn gällande arbetsrutiner och det operativa arbetet med skyddade personuppgifter mellan kommunen och bolagen. Skillnaderna mellan kommunen och bolagen liknar skillnaderna mellan enheterna inom kommunen.

Stockholm den 24 maj 2023

David Leinsköld
Verksamhetsrevisor, EY

Daniel Larsson
Verksamhetsrevisor, EY

Bilaga 1. Källförteckning

Intervjuade funktioner

- Enhetschef, personalenheten
- Lönespecialist, personalenheten
- Digitaliseringsdirektör
- Enhetschef, digitaliseringsenheten
- Förvaltningsledare
- Tf teknisk chef och IT-arkitekt, digitaliseringsenheten
- Stadsjurist, kanslidirektör, juridik- och kanslistaben
- Tf kanslichef, juridik- och kanslistaben
- Tf gruppchef, arkivregistratur och valorganisationen, juridik- och kanslistaben
- Stabschef, ledningsstaben
- Informationssäkerhetssamordnare
- Säkerhetschef
- Dataskyddsombud
- Digitaliseringsstrateg, välfärd skolas verksamhetsstöd
- IT-projektledare, välfärd skolas verksamhetsstöd
- Enhetschef, utbildningsenheten
- Biträdande enhetschef, utbildningsenheten
- Handläggare, utbildningsenheten
- Handläggare, utbildningsenheten
- Systemspecialist, utbildningsenheten
- Enhetschef, barn- och familjeenheten
- Socialsekreterare, barn- och familjeenheten
- Bosamordnare, barn- och familjeenheten
- Enhetschef, omsorgsenheten
- Verksamhetsspecialist, omsorgsenheten
- Kvalitetsutvecklare, omsorgsenheten
- Handläggare, omsorgsenheten
- Kommunjurist
- Biträdande enhetschef, arbets- och etableringsenheten
- Förändringsledare, arbets- och etableringsenheten
- Arbetsledare, arbets- och etableringsenheten
- Systemspecialist, arbets- och etableringsenheten
- Karriärvägledare, arbets- och etableringsenheten
- Socialsekreterare, arbets- och etableringsenheten
- Ordförande, kommunstyrelsen
- 1:e vice ordförande, kommunstyrelsen
- 2:e vice ordförande, kommunstyrelsen
- Ordförande, nämnden för arbete och försörjning
- 2:e vice ordförande, nämnden för arbete och försörjning
- Ordförande, utbildningsnämnden
- 1:e vice ordförande, utbildningsnämnden
- 2:e vice ordförande, utbildningsnämnden
- Ordförande, socialnämnden,
- 2:e vice ordförande, socialnämnden

Granskad dokumentation

- Reglemente för kommunstyrelsen, fastställt av kommunfullmäktige 2022-12-19 § 297
- Reglemente för socialnämnden, fastställt av kommunfullmäktige 2020-01-27 § 23
- Reglemente för nämnden för arbete och försörjning, fastställt av kommunfullmäktige 2022-11-14 § 290
- Reglemente för utbildningsnämnden, fastställt av kommunfullmäktige 2020-12-14 § 455
- Internkontrollplan 2023, fastställd av kommunstyrelsen 2022-12-05 § 311
- Internkontrollplan för socialnämnden år 2023, fastställd av socialnämnden 2022-12-13 § 164
- Internkontrollplan 2023, fastställd av arbets- och företagsnämnden, nuvarande nämnden för arbete och försörjning, 2022-12-14 § 70
- Internkontrollplan utbildningsnämnden 2023, fastställd av utbildningsnämnden 2022-12-08 § 74
- Dataskyddsombudets årsrapport 2021 (kommunstyrelsen), noterad av kommunstyrelsen 2022-05-23 § 165
- Dataskyddsombudets årsrapport 2021 (socialnämnden), noterad av socialnämnden 2022-05-31
- Dataskyddsombudets årsrapport 2021 (arbets- och företagsnämnden), noterad av arbets- och företagsnämnden, nuvarande nämnden för arbete och försörjning, 2022-05-18 § 27
- Dataskyddsombudets årsrapport 2021 (utbildningsnämnden), noterad av utbildningsnämnden 2022-05-11 § 23
- Informationssäkerhetsstrategi
- Utkast till ny Informationssäkerhetsstrategi, 2023
- Guide för hantering av personuppgiftsincidenter
- Guide lagringsalternativ
- Mall för årshjul 2023
- Checklista årshjul
- Admininstruktioner sekretesshantering användarkonto
- Målsmannadokument skyddad identitet
- Manual – hantering av sekretesskydd, förskola & grundskola
- Skyddade personuppgifter
- Rutin Sekretessmarkerad kund
- Rutin för hantering av personuppgiftsincidenter
- Arbetsbeskrivningar för hanteringen

Bilaga 2. Revisionskriterier

COSO-ramverket för intern kontroll

Det finns varken för kommuner, kommunala bolag, företag eller andra organisationer en formellt fastställd standard för hur den interna kontrollen ska hanteras. I praktiken har dock en amerikansk standard blivit dominerande: The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Målet med COSO och intern kontroll är att säkerställa att risker undviks och ge en trygghet i att organisationens mål uppfylls. COSO-modellens huvudmål är att garantera en ändamålsenlig och kostnadseffektiv verksamhet, tillförlitlig finansiell rapportering och information om verksamheten samt att lagar följs.

COSO-modellen består av fem huvudkomponenter: kontrollmiljö, riskanalys, kontrollaktiviteter, information och kommunikation samt uppföljning. Dessa perspektiv beaktas i revisionsfrågorna samt rapportens analys och bedömningar.

Kommunallagen (2017:725)

Det är enligt 6 kap. 1 § styrelsens uppgift att leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders och eventuella gemensamma nämnder. Kommunstyrelsen ska, enligt 6 kap. 2 §, uppmärksammat följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning.

Kommunallagens 6 kap. 6 § anger att nämnderna var och en inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som beslutats av kommunfullmäktige samt de föreskrifter som gäller för verksamheten. Nämnderna ska även tillse att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. De senaste tio åren har antalet i Sverige dubblerats från drygt 12 000 till knappt 24 000 personer. Enligt Skatteverket utgörs dessa till 59 procent av kvinnor. Vanligast förekommande är sekretessmarkering, som är den minst ingripande formen av skydd, med 82 procent av ärendena medan skyddad folkbokföring, som är ett starkare skydd, utgör 18 procent.

Antalet personer med skyddade personuppgifter motsvarar ca 0,22 procent av befolkningen och matematiskt motsvarar det ca 240 invånare och ett tiotal anställda i Nacka kommun. Siffrorna är inte exakta men visar att det statistiskt handlar om ett fåtal individer. Konsekvensen vid felaktig röjning av dessa personuppgifter kan emellertid vara mycket allvarlig för var och en.

Jämställdhetsmyndigheten har på regeringsuppdrag genomfört kunskapshöjande insatser gällande våldsutsatta personer som lever med skyddade personuppgifter med fokus på kvinnor och barn. I en delrapport[15] intervjuas 86 kvinnor och 15 barn om deras erfarenheter. Närmare tre fjärdedelar av de intervjuade uppger att deras identitet har röjts.

I rapporten konstateras att det i många fall handlar om kvinnor och barn som tvingats flytta på grund av våld och hot från närstående man och att målgruppen är extra utsatt. I princip

[15] *Skyddade personuppgifter – oskyddade personer* (Jämställdhetsmyndigheten 2022:10).

samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

Det finns omfattande lagstiftning som skyddar individen

Skyddade personuppgifter är ett samlingsbegrepp för olika åtgärder som kan vidtas för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Beroende på hotets allvarlighetsgrad finns tre grader av skydd av personuppgifter; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Därutöver finns ytterligare bestämmelser om sekretess som kan aktualiseras för hotade och förföljda personer, bland annat inom offentlighets- och sekretesslagen (2009:400).

Sekretessmarkering är den vanligaste och minst ingripande formen av skydd

Sekretessmarkering är den minst ingripande formen av skydd av personuppgifter som innebär att Skatteverket gör en sekretessmarkering av enskild persons uppgifter i folkbokföringen (se 5 kap. 5 § offentlighets- och sekretesslagen [2009:400], OSL). Syftet är att förhindra att hotande eller förföljande person med hjälp av personuppgifter kan hitta och utsätta person för brott, förföljelse eller trakasserier.

Sekretessmarkeringen är dock inte ett bindande beslut, endast en indikation på att folkbokföringssekretess enligt 22 kap. 1 § OSL kan gälla för uppgifterna. Den fungerar alltså som en påminnelse eller varningssignal hos alla myndigheter om att det finns behov att göra en noggrann sekretessprövning innan personuppgifter lämnas ut.

I praktiken registrerar Skatteverket en sekretessmarkering som aviseras tillsammans med personuppgifterna till alla myndigheter som får grundläggande personuppgifter från Skatteverkets folkbokföringsverksamhet. Det är den enskilde som ansöker om sekretessmarkering hos Skatteverket. Det finns inga formella krav för att beviljas skyddsåtgärden men den enskilde behöver motivera varför den behöver sekretessmarkering med någon form av handling som stödjer att det föreligger ett aktuellt och konkret hot. Det kan till exempel vara en utredning eller ett utlåtande från Polismyndigheten eller socialtjänsten. Sekretessmarkeringen gäller ofta i två år och kan förlängas.

Skyddad folkbokföring ger starkare skydd än sekretessmarkering

Skyddad folkbokföring ger starkare skydd än sekretessmarkering och innebär att en person kan vara folkbokförd på sin gamla folkbokföringsort efter att ha flyttat. De gamla adressuppgifterna tas bort och den nya adressen registreras inte i folkbokföringen och sprids därmed aldrig till andra myndigheter. Uppgifterna om skyddad folkbokföring skickas till andra myndigheter och annan samhällsservice som personen har kontakt med, till exempel sjukvården, Försäkringskassan och kommunen. Det betyder att dessa instanser kan se att personen har skyddad folkbokföring.

Skyddad folkbokföring medges för person som av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt, om åtgärden med hänsyn till den enskildes förmåga och övriga förutsättningar kan antas tillgodose behovet av skydd. Skyddad folkbokföring kan kombineras med andra skyddsåtgärder som exempelvis kontaktförbud om det bedöms lämpligt utifrån den enskildes specifika situation. Skyddad folkbokföring medges efter ansökan från den enskilde. För barn under 18 år får ansökan enbart göras av den ena vårdnadshavaren i det fall syftet är att skydda från den andra vårdnadshavaren.

Fingerade personuppgifter är den starkaste och mest ingripande formen av skydd

År 2015 fanns i Sverige ungefär 160 personer med fingerade personuppgifter. Fingerade uppgifter betyder att personen använder andra personuppgifter än de verkliga. Detta medför dock inte någon rättslig förändring av personens namn eller andra förhållanden. Kopplingen mellan den verkliga och den fingerade identiteten är sekretessbelagd. Med den nya identiteten kan personen vara öppen med sina personuppgifter utan risk att bli hittad. Fingerade personuppgifter har inget skydd i de systemstöd som används i en region eller kommun eftersom de hanteras som vilken person som helst.

Offentlighets- och sekretesslagen reglerar utlämning av allmänna handlingar

Offentlighets- och sekretesslagen (OSL) innehåller bestämmelser för hur myndigheter ska registrera, lämna ut och hantera allmänna handlingar. Det finns också regler om tystnadsplikt och förbud att lämna ut allmänna handlingar.

Utöver de tre skyddsformerna (sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter) finns en särskild generell sekretessbestämmelse som gäller för vissa personuppgifter om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs (21 kap. 3 § första stycket OSL).

Sekretessen gäller uppgift om en enskilds

- bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde stadigvarande eller tillfälligt bor,
- telefonnummer,
- e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med personen.

Sekretessen gäller även för motsvarande uppgifter om personens anhöriga. Bestämmelsen gäller oavsett sammanhang som uppgiften förekommer i.

Bilaga 3. Kommunstyrelsens och nämndernas ansvarsområden

Kommunstyrelsen

Kommunstyrelsen är kommunens ledande förvaltningsorgan. Styrelsen ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt, de föreskrifter som kan finnas i lag eller förordning samt bestämmelser som finns i reglementet.

Av *Reglemente för kommunstyrelse*[16] framgår bland annat att kommunstyrelsen:

- Ska hålla sig omvärldsorienterad och uppmärksamt följa förändringar i samhället som påverkar kommunens förhållanden och ta de initiativ som behövs för att anpassa kommunens verksamhet
- Ska anta styrande dokument för samordning av den kommunala verksamheten
- Ska samordna och upphandla samtliga nämnders IT-tjänster/system. Styrelsen har det övergripande ansvaret för digitalisering vilket inbegriper att vidta åtgärder för att nyttja de möjligheter till utveckling som digitaliseringen ger.
- Ansvarar för kommunens säkerhetsarbete genom att bland annat samordna dataskydd, informationssäkerhet och IT-säkerhet och samordna säkerhetsskydd.
- Utgör kommunens personalorgan. I detta ingår exempelvis att ta personalansvar för samtlig kommunalt anställd personal och att ansvara för de frågor som faller inom personalorganets verksamhetsområde.
- Ska tillhandahålla kommunal produktion av tjänster i den omfattning som efterfrågas. Kommunstyrelsen ansvarar därvid för produktionen av tjänster inom samtliga nämnders ansvarsområden. För tjänster inom ramen för skollagen och andra författningar inom utbildningsområdet innebär det att kommunstyrelsen ansvarar som huvudman för utbildningen i de kommunala förskolorna och skolorna innefattande frågor rörande barns och elevers vardag i utbildningen.

Socialnämnden

Socialnämnden fullgör kommunens uppgifter inom socialtjänsten avseende individ- och familjeomsorg (exklusive ekonomiskt bistånd), kommunal vård och omsorg som inte avser äldre, lag om stöd och service till viss funktionshindrade.

Nämnden har ansvar för finansiering, målformulering, effektivitet och uppföljning av verksamheten samt för att de som verksamheten riktar sig till får en allsidig information om verksamheten och hur den fullgörs. Nämnden är också system- och finansieringsansvarig nämnd för kundvalssystemen inom sina ansvarsområden, vilket enligt *Reglemente för socialnämnden*[17] innefattar bland annat att fortlöpande utveckla kundvalssystemen och att utreda och lämna förslag till kommunfullmäktige om nya kundvalssystem inom nämndens ansvarsområde.

[16] Fastställt av kommunfullmäktige 2022-12-19 § 297.
[17] Fastställt av kommunfullmäktige 2020-01-27 § 23.

Ansvarig processägare inom socialnämndens, samt äldrenämndens, verksamhetsområde är social- och äldredirektör. Under denna finns barn- och familjeenheten, omsorgsenheten och äldreenheten.

Nämnden för arbete och försörjning

Nämnden för arbete och försörjning ansvarar för den kommunala vuxenutbildningen, ensamkommande barn och unga, ekonomiskt bistånd och arbetsmarknadsinsatser. Nämnden ansvarar för finansiering, målformulering, effektivitet och uppföljning av verksamheten inom sitt område. Nämnden är också system och finansieringsansvarig nämnd för kundvalssystemen inom sina ansvarsområden, vilket enligt *Reglemente för nämnden för arbete och försörjning*[18] innefattar bland annat att fortlöpande utveckla kundvalssystemen och att utreda och lämna förslag till kommunfullmäktige om nya kundvalssystem inom nämndens ansvarsområde.

Ansvarig processägare för nämnden för arbete och försörjnings verksamhetsområde är utbildnings- och arbetsmarknadsdirektör. Under denna finns arbets- och etableringsenheten samt utbildningsenheten.

Utbildningsnämnden

Utbildningsnämnden ansvarar för förskoleverksamheten, grundskolan, gymnasieskolan och särskolan. Nämnden är huvudman för och/eller myndighet inom finansiering, målformulering och uppföljning utifrån nationella och kommunala mål, uppföljning och utvärdering av kvalitet på övergripande nivå, kundval och myndighetsutövning/myndighetsuppgifter inom de områden som enligt lag eller annan författning är hemkommunens ansvar.

Nämnden är också system och finansieringsansvarig nämnd för kundvalssystemen inom sina ansvarsområden, vilket enligt *Reglemente för utbildningsnämnden*[19] innefattar bland annat att fortlöpande utveckla kundvalssystemen och att utreda och lämna förslag till kommunfullmäktige om nya kundvalssystem inom nämndens ansvarsområde.

Ansvarig processägare för utbildningsnämndens verksamhetsområde är utbildnings- och arbetsmarknadsdirektör. Under denna finns arbets- och etableringsenheten samt utbildningsenheten.

[18] Fastställt av kommunfullmäktige 2022-11-14 § 290.
[19] Fastställt av kommunfullmäktige 2020-12-14 § 455.