Nämnden för arbete och försörjning

2023-10-11
TJÄNSTESKRIVELSE
Dnr: NAF-2023-00241

Revisionsskrivelse 2023-05-24 och revisionsrapport 4, 2023 – Nämnden för arbete och försörjnings hantering av skyddade personuppgifter

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Nämnden för arbete och försörjning antar föreslaget yttrande över revisionsskrivelse 2023-05-24 och revisionsrapport 4, 2023, enligt bilaga 4 till tjänsteskrivelse daterad den 11 oktober 2023.

Sammanfattning av ärendet

Ernst Young (EY) har på uppdrag av Nacka kommuns revisorer granskat nämnden för arbete och försörjnings hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur nämnden säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om nämndens rutiner är ändamålsenliga och tillämpade. Granskningen har förutom nämnden för arbete och försörjning omfattat kommunstyrelsen, socialnämnden och utbildningsnämnden. I revisionsskrivelse 2023-05-24 och revisionsrapport 4, 2023 lämnar revisorerna sju rekommendationer till nämnden för arbete och försörjning. Övergripande avser rekommendationerna rutiner, utbildning och kontroller. Överlag instämmer nämnden i rekommendationerna men påtalar att rutiner finns och att det på enheten redan pågår ett utvecklingsarbete inom området avseende det som har identifierats. Baserat på revisorernas rekommendationer har ett yttrande tagits fram.

Ärendet

Innehållet i revisionsgranskningen i korthet samt revisorernas rekommendationer

Ernst Young (EY) har på uppdrag av Nacka kommuns revisorer granskat nämnden för arbete och försörjnings hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur nämnden säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om nämndens rutiner är ändamålsenliga och tillämpade. Granskningen har även omfattat kommunstyrelsen, socialnämnden och utbildningsnämnden.

I revisionsskrivelsens utlåtande finns sex rekommendationer vilka gäller för samtliga nämnder inklusive kommunstyrelsen. Kommunstyrelsen ges även rekommendation att upprätta ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter. En rekommendation ges utöver dessa specifikt till nämnden för arbete och försörjning och utbildningsnämnden.

Revisorernas övergripande bedömning är att kommunstyrelsen och de granskande nämnderna inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga. Processer och rutinbeskrivningar som tillämpas på enhetsnivå bedömer revisorerna som tillämpbara och ändamålsenliga men vissa brister och förbättringsområden har identifierats.

I det dagliga operativa arbetet på arbets- och etableringsenheten beaktas alltid sekretess oavsett om det avser en person som har skyddade personuppgifter i form av de tre skyddskategorierna, sekretessmarkering, skyddad folkbokföring, fingerade personuppgifter eller inte. Enheten har säkerställt att åtgärder av mer riktad karaktär såsom rutiner för ändamålet samt löpande enhetsdialog kring sekretess och skyddade personuppgifter ingår som en del i det systematiska kvalitets- och uppföljningsarbetet.

Vidare menar revisorerna att det för nämndens målgrupper som omfattas av skyddade personuppgifter behöver ske löpande risk- och konsekvensanalyser som en del av internkontrollplanen. Risk- och konsekvensanalyser har dock genomförts och revisorerna framför att det finns en säkerhets- och riskmedvetenhet på enheten avseende hantering av skyddade personuppgifter. frekvent

Enligt revisorerna skulle ett kommunövergripande styrdokument bidra till att tydliggöra samt säkerställa en enhetlig riktning avseende hanteringen av skyddade personuppgifter. På kommunövergripande nivå kommer arbetet att påbörjas under hösten 2023 med framtagandet av styrdokumentet som kan komma att inkludera risk- och konsekvensanalys. Styrdokumentet kommer att vara vägledande i enhetens fortsatta arbete.

Brister i kompetensutveckling inom området har identifierats. Revisorerna påtalar vikten av att hålla kunskapen aktuell även för den som inte frekvent möter målgruppen som omfattas av skyddade personuppgifter. En obligatorisk specifikt riktad och regelbundet återkommande utbildning stärker grundkunskaperna inom ämnet vilket förväntas bidra till att säkerställa än högre korrekt hantering av skyddade personuppgifter.

Inom området IT-säkerhet ger revisorerna rekommendationer avseende behörighetstilldelning, kontroll av användarloggar samt uppföljning av avvikelser specifikt för målgruppen med skyddade personuppgifter.

Slutligen rekommenderas nämnden för arbete och försörjning och utbildningsnämnden att utvärdera eventuella risker avseende negativ påverkan i hanteringen av skyddade personuppgifter med anledning av att enheterna delar kontorslokal.

Revisorerna rekommenderar nämnden för arbete och försörjning att:

1. Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
2. Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
3. Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enhetens arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.
4. Begränsa åtkomsten till personuppgifterna genom strikt behörighetshantering.
5. Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
6. Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.
7. Utvärdera risken att arbetet med skyddade personuppgifter påverkas negativt av att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal.

Rekommendationerna behöver åtgärdas för att nämnden för arbete och försörjning ska anses uppfylla efterlevnaden av hantering av personer med skyddade personuppgifter till fullo. Ett yttrande från nämnden ska vara kommunfullmäktiges revisorer tillhanda senast den 15 november 2023.

Arbets- och etableringsenhetens utredning samt förslag på yttrande

Arbets- och etableringsenheten har i nuläget omkring 20 hushåll som omfattas av skyddade personuppgifter i någon av de tre skyddskategorierna.

Samtliga anställda på enheten är väl förtrogna med offentlighet- och sekretesslagstiftningen. Enheten arbetar systematiskt med rapportering av avvikelser, lagstiftningen gällande Lex Sarah samt personuppgiftsincidenter enligt dataskyddsförordningen. Enheten har sedan januari i år inrättat en ny roll som kvalitets- och säkerhetssamordnare för att i än högre grad fokusera på risk- och konsekvensbedömningar och kvalitetsaspekter inom nämndens olika delar samt dess efterlevnad. Rollen som kvalitets- och säkerhetssamordnare samspelar i hög grad med enhetens dataskyddssamordnare då frågorna kring hantering av personuppgifter ofta tangerar varandra.

Rutin avseende handläggning av personer med skyddad identitet är upprättad och kommunicerad internt. Internutbildning kring offentlighets- och sekretesslagen sker årligen av enhetens jurist. Inom ramen för enhetens dataskyddsarbete inbegrips frågor kring hantering av personuppgifter. I enlighet med det systematiska kvalitetsarbetet hålls utbildning och dialog kring dataskyddsförordningen, vars syfte är att skydda den enskildes fri- och rättigheter. Såväl personuppgiftsincidenter som avvikelser och Lex Sarah rapporteras löpande till nämnden. Om en incident inträffar föranleder det alltid dialog och analys inom verksamheten med syfte att vidta åtgärder så att händelsen inte upprepas.

Enhetens bedömning avseende de rekommendationer som revisorerna lämnar i ärendet.

1 Rekommendation att upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
I Reglementet för internkontroll (KFKS 2020/444) beskrivs arbetsgången för hur framtagandet av riskområden ska ske på nämndnivå. Det är möjligt att detta område inkluderas i internkontrollplanen om det påvisas i väsentlighets- och riskanalysen att riskvärdet är högt. I nämndens senast beslutade interkontrollplan som utgör en bilaga till tertialbokslut 2 (NAF-2023-00015) framgår en identifierad risk avseende ”avbrott, intrång eller fel i verksamhetssystem”, där målgruppen med skyddade personuppgifter har riskbedömts.

Enheten anser att det är av relevans att genomföra en risk- och konsekvensanalys specifikt för målgruppen. Röjning av dessa uppgifter kan leda till än mer allvarliga konsekvenser än vid röjning av personuppgifter som inte omfattas av någon skyddskategori. En risk- och konsekvensanalys kommer att genomföras under hösten 2023 för att specifikt bedöma hanteringen av skyddade personuppgifter. Hantering av alla typer av personuppgifter ryms inom enhetens dataskyddsarbete. Riskanalyser genomförs i samband med informationsklassning av uppgifter i verksamhetssystem, personer med skyddade personuppgifter riskbedöms specifikt som målgrupp.

2 Rekommendation att upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
Som revisorerna har påtalat har enheten en framtagen rutin avseende hantering av skyddade personuppgifter, denna revideras och kommuniceras regelbundet, senast under våren 2023. Enheten kommer i samband med att det kommunövergripande styrdokumentet inom området beslutas, att verkställa det på enhetsnivå. Detta kommer att ske genom att styrdokumentet bryts ner, beslutas, implementeras och systematiskt följs upp på enhetsnivå som en del av årshjulet för det systematiska kvalitetsarbetet. Syftet med styrdokumentet och rutinen är att skapa de bästa förutsättningarna för att nå hög efterlevnad inom området. Rutinbeskrivningen kommer att revideras för att det tydligare ska framgå önskade kontaktvägar för en person som har skyddade

personuppgifter. Information om att nogsamt beakta sekretess vid kommunikation i det delade kontorslandskapet avseende skyddade personuppgifter, kommer även att tydliggöras i rutinbeskrivningen.

3 Rekommendation att genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enhetens arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.

Av stadsledningskontorets yttrande framgår att kommunövergripande utbildningsinsatser inom området kan bli aktuellt då styrdokumentet har implementerats (KFKS-2023-00574). På arbets- och etableringsenheten är en grundläggande internutbildning inplanerad under hösten 2023 och sedan återkommande i verksamhets årshjul avseende efterlevnaden av dataskyddsförordningen. I september i kompetensutvecklades fem medarbetare med olika professioner via en extern halvdagsutbildning inom området hantering av skyddade personuppgifter. Kunskapsdelning och internutbildning inom området sker under hösten. Arbetsrutiner avseende hantering av skyddade personuppgifter är reviderade och förankrade i medarbetargrupperna, även detta moment återkommer löpande i enhetens årshjul. Genom enhetens dataskyddsarbete fokuseras på frågor kopplat till personuppgifter, då handläggare på enheten hanterar såväl känsliga som extra skyddsvärda personuppgifter dagligen. Återkommande internutbildning om dataskyddsförordningen och efterlevnaden av densamma sker enligt årshjul, två tillfällen per år samt vid behov och alltid i samband med anmäld personuppgiftsincident.

4 Rekommendation att begränsa åtkomsten till personuppgifterna genom strikt behörighetshantering.

Enheten tillämpar rutinbeskrivning avseende behörighetshantering vilken är reviderad och kommunicerad våren 2023. Uppföljning av rutinen återfinns som aktivitet i enhetens årshjul för efterlevnaden av dataskyddsförordningen. Samverkan i frågor kopplat till behörighetsstyrning sker vid behov mellan enhetens olika professioner. Expertis från digitaliseringsenheten finns att rådfråga i förekommande fall. Som stöd i arbetet finns sedan september 2023 ett styrdokument inom området, ”Så här gör vi i Nacka – IT-säkerhet”, vilket anger ett flertal krav på hur åtkomst och behörigheter ska hanteras. På kommunövergripande nivå planeras att under hösten 2023 informationsinsatser för att höja medvetandet om de krav som ställs (KFKS-2023-00574).

5 Rekommendation att genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.

Nämnden för arbete- och försörjning instämmer i rekommendationen.
Revisorerna ser risker med anledning av att arbets- och etableringsenheten inte tillämpar begränsad behörighet för ärenden som omfattas av skyddade personuppgifter. Samtliga medarbetare beaktar sekretess- och offentlighetslagstiftningen i allt arbete rörande individärenden. Frågan kommer dock att utredas under hösten 2023 för att se över om dedikerade handläggare ska utses för målgruppen som har skyddade personuppgifter.

Det har identifierats brister i styrningen gällande vilket ansvar som åligger enheterna avseende att upprätta verksamhetsspecifika rutiner samt krav på loggar. Det finns behov av att upprätta ett övergripande styrdokument från vilket de olika enheterna kan skapa rutiner för hur loggkontroller ska ske samt vilka krav som ska ställas på loggarna (KFKS-2023-00574). På arbets- och etableringsenheten pågår redan ett arbete med att ta fram en rutinbeskrivning avseende kontroller av användarloggar. Kunskap inom området har inhämtats från Nackas informationssäkerhetssamordnare och från systemförvaltare inom sociala omsorgsprocessen, allt i linje med en lärande organisation.

6 Rekommendation att säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Enheten har rutinbeskrivningar för avvikelsehantering och personuppgiftsincidenter i enlighet med dataskyddsförordningen. Rutinerna är väl kända och följs av enhetens medarbetare. I enlighet med enhetens systematiska kvalitetsarbete följs avvikelser och personuppgiftsincidenter upp i nära anslutning till inträffad händelse samt på aggregerad nivå. Kommuns dataskyddsombud granskar årligen nämndens efterlevnad av dataskyddsförordningen där personuppgiftsincidenter är ett område. Årets granskning påvisar god efterlevnad (NAF-2023-00197). I de fall en avvikelse omfattar röjande av skyddade personuppgifter innebär det som huvudprincip även att en personuppgiftsincident har inträffat. Detta med anledning av att skyddade personuppgifter kategoriseras som ”en extra skyddsvärd uppgift” enligt dataskyddsförordningen.

Revisorerna påtalar att avvikelsehantering gällande skyddade personuppgifter inte kan särskiljas från avvikelser av annan karaktär, samma brist återfinns i hanteringen av personuppgiftsincidenter. Enheten har åtgärdat hanteringen avseende detta genom att uppdatera rutinerna för avvikelserapportering och personuppgiftsincidenter. På kommunövergripande nivå kommer e-tjänsten som hanterar anmälan om personuppgiftsincidenter att revideras under hösten 2023. Detta så att det i samband med anmälan framgår om incidenten är kopplat till skyddade personuppgifter eller inte (KFKS-2023-00574).

7 Rekommendation att utvärdera risken att arbetet med skyddade personuppgifter påverkas negativt av att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal.

Beaktandet av sekretess gäller all hantering av personuppgifter, oavsett om det avser en person som har skyddade personuppgifter eller inte. Nämnden för arbete och försörjning har inte identifierat negativa påverkansfaktorer som specifikt kan drabba personer med skyddade personuppgifter kopplat till att arbets- och etableringsenheten och utbildningsenheten delar kontorslokaler. Samtliga anställda på båda enheterna är väl förtrogna med offentlighet- och sekretesslagstiftningen och sekretessförbindelse signeras vid anställningsavtalets ingående.

Nacka kommuns övergripande arbetssätt i Nacka stadshus är baserat på öppna kontorslandskap sedan flertalet år tillbaka. Alla enheter utgår från en så kallad hemvist. Arbetsmodellen innebär att det är så kallad fri sittning i stadshuset samt att alla medarbetare kan boka merparten av de mötes- och konferensrum som finns att tillgå. Även i andra kontorslandskap än den egna hemvisten. Arbetssättet medför att det är många personer i rörelse i stadshuset. Att arbeta i öppna kontorslandskap ställer krav på den enskilde medarbetarens ansvar, särskilt i frågor avseende sekretess. I enlighet med det systematiska arbetsmiljöarbetet genomförs risk- och konsekvensbedömningar då det föreligger organisatoriska förändringar i verksamheten. Uppföljning sker löpande. Arbetet sker i samverkan mellan arbetsgivare och arbetstagare samt fackliga organisationer. Vid dessa risk- och konsekvensbedömningar har frågan om risken för att personuppgifter och sekretessbelagd information röjs med anledning samlokaliseringen identifierats. Risken har undersökts, riskbedömts och beslutade åtgärder har vidtagits vilka följs upp i enlighet med det systematiska kvalitetsarbetet.

Inför samlokaliseringen av enheterna hösten 2022 har arbets- och etableringsenheten genomfört risk- och konsekvensbedömning, vilken även har följts upp. Ett gemensamt enhetsmöte mellan arbets- och etableringsenheten och utbildningsenheten genomfördes i samband med samlokaliseringen med fokus på dialog specifikt kring sekretessfrågan. Arbets- och etableringsenheten och utbildningsenheten har en väl utvecklad samverkan och regelbunden översyn med uppföljning av kontorslandskapets spelregler. Syftet med samverkan är att identifiera utvecklings- och förbättringsåtgärder men också påtala vad som fungerar bra och vad som har förbättrats sedan sist.

Arbets- och etableringsenhetens medarbetare lägger hög vikt i att beakta sekretess i kontorslandskapet och är högst medvetna om de konsekvenser som röjande av personuppgifter kan innebära.

Ekonomiska konsekvenser

Förslaget till beslut om yttrande medför inga ekonomiska konsekvenser.

Konsekvenser för barn

Förslaget till beslut om yttrande medför inga direkta konsekvenser för barn. Nämnden för arbete och försörjning verkar för att i alla led säkerställa en korrekt hantering av skyddade personuppgifter för alla enskilda som har behov av detta ingripande skydd från samhället. Av Barnkonventionens paragraf 16 framgår specifikt att barn har rätt till ett privatliv. ”Inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin

heder och sitt anseende. Barnet har rätt till lagens skydd mot sådana ingripanden eller angrepp”[1].

Handlingar i ärendet

1. Tjänsteskrivelse daterad den 13 oktober 2023
2. Revisionsskrivelse 2023-05-24
3. Revisionsrapport 4, 2023
4. Förslag på yttrande daterat den 11 oktober 2023

Pia Stark
Enhetschef
Arbets- och etableringsenheten

Ghita Flinckman
Förändringsledare, dataskyddssamordnare
Arbets- och etableringsenheten

[1] Läs texten | unicef.se