Kommunstyrelsen

2023-09-18
TJÄNSTESKRIVELSE
Dnr: KFKS-2023-00574

Revisionsskrivelse och revisionsrapport 4 2023 – Granskning av kommunens hantering av skyddade personuppgifter

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta följande.

Kommunstyrelsen antar yttrande över revisionsrapport och revisionsskrivelse enligt bilaga 3 till tjänsteskrivelse daterad den 30 augusti 2023.

Sammanfattning av ärendet

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.

Utifrån revisorernas rekommendationer har ett yttrande tagits fram utifrån de rekommendationer som revisorerna lämnat till kommunstyrelsen.

Ärendet

Innehållet i revisionsgranskningen i korthet samt revisorernas 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.

Revisorernas 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 revisorerna att dessa är ändamålsenliga och tillämpliga men det har också identifierats brister och förbättringsområden, däribland striktare behörighetsbegränsningar i IT-system och mindre manuell hantering av skyddade personuppgifter.

Kommunen bedöms inte ha någon övergripande styrning inom området och de granskade nämnderna har inte heller beslutat om egna styrdokument. Revisorernas bedömning är att även om Nacka kommuns styrmodell är politiskt beslutad är en 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. Revisorernas 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 för 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.

Stadsledningskontorets utredning samt förslag på yttrande

Denna tjänsteskrivelse avser enbart de rekommendationer som revisorerna lämnat till kommunstyrelsen. Granskningen som omfattar socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning bereds och beslutas inom respektive nämnd. Av nedan följer stadsledningskontorets bedömning avseende de olika rekommendationer som revisorerna lämnar i ärendet.

I sammanhanget kan inledningsvis noteras det inte finns några särskilda uppgifter om hur många personer som har skyddade personuppgifter inom kommunens alla olika verksamheter. Personer som har skyddade personuppgifter kan utgöras av såväl anställda, elever, kunder, allmänhet med mera. Även om antalet personer med skyddade personuppgifter, som är i kontakt med kommunen, inte beräknas vara så många är det av stor vikt att varje enskilt fall hanteras säkert och korrekt för att säkerställa skyddet för den enskilde och dess anhöriga. Utifrån statistik från de två senaste åren har det skett en incident per år relaterat till röjande av skyddade identiteter.

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

Stadsledningskontoret ser ett behov av ett kommunövergripande styrdokument för hantering av skyddade personuppgifter. Hitintills har kommunen, via medarbetarsidorna på nacka.se, gett vägledning om hur arbetet med skyddade personuppgifter bör se ut och vikten av att i varje enskilt fall göra en riskbedömning och handlingsplan. Utifrån den bredd av verksamheter som finns i kommunen (exempelvis elever, biståndssökande, bygglovssökande och medarbetare) har det funnits skäl att varje enhet prioriterar att anta egna rutiner inom sina respektive ansvarsområden för att säkerställa att de som har skyddade personuppgifter får rätt skydd inom den specifika verksamheten. Många statliga myndigheter såsom exempelvis Skolverket, Socialstyrelsen och Integritetsskyddsmyndigheten har även tagit fram specifika vägledningar som är mer verksamhetsspecifika och som kommunens verksamheter kunnat ta avstamp i vid utformande av egna rutiner. Stadsledningskontoret kan dock instämma i revisorernas bedömning om att det finns skäl för ett kommunövergripande styrdokument som anger kommunens ramar och inriktning inom området vilket bland annat inbegriper *vad* kommunens verksamheter förväntas göra för att stärka skyddet för personer med skyddade personuppgifter. Respektive verksamheter bör dock även fortsättningsvis besluta om *hur* detta ska i praktiken utifrån verksamheterna behov och särskilda målgrupper. Ett styrdokument behöver även ange hur en systematisk uppföljning ska ske beträffande hanteringen av skyddade personuppgifter för att säkerställa en god efterlevnad av det styrande dokumentet. Genom ett gemensamt styrande dokument får såväl chefer som medarbetare ett stöd och verktyg i arbetet med hantering av skyddade personuppgifter. Stadsledningskontoret kommer under hösten 2023 påbörja arbetet med att ta fram ett förslag till styrdokument inom området.

Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.

Utarbetandet av risk- och konsekvensanalyser bör kunna inrymmas i ett kommunövergripande styrdokument som stadsledningskontoret planerar att ta fram. Möjligheten att inkludera hanteringen av skyddade personuppgifter i respektive nämnds internkontrollplan finns redan idag. Vad som ingår i respektive nämnds interkontrollplan bygger på en genomförd väsentlighets- och riskanalys inom nämndens ansvarsområde. Om en nämnd identifierar att hanteringen av skyddade personuppgifter har ett högt riskvärde inom nämnden blir risken ett område som förs in i nämndens internkontrollplan. Denna arbetsgång finns redan angiven i Reglemente för intern kontroll.

Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
Vad gäller behovet av ett kommunövergripande styrdokument hänvisas till bedömningen i revisorernas första punkt (sida 3). I ett sådant styrdokument bör även kunna inrymmas kommunens hantering av skyddade personuppgifter vad gäller medarbetare utifrån kommunstyrelsens arbetsgivaransvar. Att därutöver anta ett styrande dokument inom kommunstyrelsens ansvarsområde bedöms i dagsläget inte vara nödvändigt. Det viktigaste är istället att respektive verksamhetsområde, inom kommunstyrelsens ansvar, utarbetar interna rutiner som är anpassade utifrån verksamhetens målgrupper så att skyddade personuppgifter hanteras korrekt. Denna prioritering bör även framgå av det kommunövergripande styrdokumentet. På så sätt får kommunstyrelsen förutsättningar att regelbundet kan följa upp att enheter och verksamheter genomför detta arbete.

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.
När ett kommunövergripande styrdokument är antaget finns goda förutsättningar att genomföra utbildningsinsatser för medarbetare i kommunen. Vikten av utbildningsinsatser för medarbetare kan även anges i det styrande dokumentet så att kommunstyrelsen kan följa upp att så även sker i praktiken. I dagsläget finns det i kommunen tillgång till digitala verktyg i kommunen för att genomföra utbildningsinsatser och sådana utbildningsinsatser kan då även följas upp på olika nivåer i kommunen vilket är positivt. Redan idag pågår det centralt inom kommunen inventering över lämpliga utbildningsinsatser som medarbetare bör genomgå dels vid nyanställning, dels som återkommande utbildningsinsatser. I detta arbeta är det naturligt att bygga in hur kommunen hanterar skyddade personuppgifter.

Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
Styrdokumentet ”Så här gör vi i Nacka – IT-säkerhet” anger ett flertal krav på hur åtkomst och behörigheter ska hanteras. Dokumentet förtydligar också att de rekommendationer som framkommer vid informationsklassningar och riskanalyser från IT-säkerhetsamordnare, informationssäkerhetssamordnare samt dataskyddsombud ska beaktas och anses som vägledande. Informationsinsatser för att höja medvetandet om de krav som ställs i detta dokument är planerade till hösten 2023.
Ett förtydligande gällande krav på att genom risk- och konsekvensanalys finna en lämplig nivå på en strikt behörighetsstyrning för varje behandling av skyddade personuppgifter inom berörda verksamheter bör förtydligas i det kommungemensamma styrdokument som är planerat till hösten 2023.

Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
Brister i styrningen gällande vilket ansvar som verksamheterna har för att upprätta verksamhetsspecifika rutiner och krav på loggar har identifierats. Det finns behov av att upprätta ett övergripande styrdokument från vilket de olika verksamheterna kan skapa rutiner för *hur* loggkontroller ska ske samt vilka krav som ska ställas på loggarna. Styrdokumentet ”Så här gör vi i Nacka – IT-säkerhet” anger omfattningen av och syftet för den loggkontroll som sker inom ramarna för digitaliseringsenhetens ansvarsområde, men då hanteringen av loggar kan anses som känslig information måste verksamheterna i viss utsträckning själva ställa krav på detta och tillse att så sker.

Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.
Avvikelser vad gäller skyddade personuppgifter innebär som huvudregel att en så kallad personuppgiftsincident även inträffar. Då skyddade personuppgifter anses vara en ”extra skyddsvärd personuppgift” enligt dataskyddsförordningen innebär det att avvikelser/incidenter kopplat till denna form av personuppgift ska anmälas som en personuppgiftsincident till kommunens dataskyddsombud. Vid allvarligare överträdelser ska en anmälan även ske till Integritetsskyddsmyndigheten. Personuppgiftincidenter följs årligen upp av kommunens dataskyddsombud i respektive nämnd i samband med dataskyddsombudets årsrapport. Beslut avseende personuppgiftsincidenter fattas på delegation utifrån respektive nämnds delegationsordning. Utifrån att delegationsbeslut anmäls på nämndsammanträdena får både nämnden och allmänheten en insyn om anmälda incidenter. Det kan således konstateras att det finns upparbetade rutiner för avvikelsehantering inom området. För att kunna följa upp om en personuppgiftsincident avser just en incident kopplat till skyddade personuppgifter bedöms dock kommunens rapporteringsmall behöva modifieras så att det tydligt anges att det avser en skyddad personuppgift. En revidering av rapporteringsmallen kommer ske under hösten 2023 vilket innebär att det därefter finns goda förutsättningar att systematiskt följa upp avvikelser inom området. Om det därutöver finns behov av förtydliga incidentprocessen ytterligare kan detta regleras i det kommande kommunövergripande styrdokumentet som tas fram inom området.

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. En god hantering av skyddade personuppgifter är däremot av vikt för alla enskilda som är i behov av skyddade personuppgifter däribland barn och unga.

Handlingar i ärendet

1. Tjänsteskrivelse daterad den 18 september 2023
2. Revisionsskrivelse 2023-05-24
3. Revisionsrapport 4, 2023
4. Förslag på yttrande

Maria Rönnberg
Kanslidirektör/stadsjurist
Stadsledningskontoret

Anneli Sagnérius
Kommunjurist
Juridik- och kanslistaben