Revisionsrapport 2023:6

Nacka vatten och avfall AB

Granskning av bolagets hantering av skyddade personuppgifter

Nacka kommun

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer 2
2. Inledning 4
   2.1 Bakgrund 4
   2.2 Syfte och revisionsfrågor 4
   2.3 Ansvarig bolagsstyrelse 5
   2.4 Metod och genomförande 5
   2.5 Revisionskriterier 5
3. Kontrollmiljö 6
   3.1 Nacka vatten och avfall AB är personuppgiftsansvarig inom sitt verksamhetsområde 6
   3.2 Organisation och ansvarsfördelning för hanteringen av skyddade personuppgifter 6
   3.3 Styrande dokument och bolagsspecifika rutiner 6
   3.4 Det finns behov av ytterligare kompetensutveckling 7
   3.5 Bedömning 8
4. Riskbedömningar 9
   4.1 Risken har analyserats men inte inom ramen för bolagets internkontrollarbete 9
   4.2 Bedömning 9
5. Kontrollaktiviteter – Bolagets rutiner och arbetssätt 11
   5.1 Behandling av skyddade personuppgifter i IT- och verksamhetssystem 11
   5.2 Hantering och kommunicering av skyddade personuppgifter 11
   5.3 Det saknas en rutin för hanteringen av medarbetare med skyddade personuppgifter 12
   5.4 Bedömning 12
6. Avvikelsehantering 14
   6.1 Det finns inga rapporterade avvikelser avseende skyddade personuppgifter 14
   6.2 Bedömning 14
7. Svar på revisionsfrågor 15

Bilaga 1 Källförteckning 17

Bilaga 2 Revisionskriterier 18

1. Sammanfattande bedömning och rekommendationer

EY har på uppdrag av Nacka kommuns lekmannarevisorer granskat Nacka vatten och avfall AB:s (NVOA) hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur styrelse och VD för NVOA säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både kunder och anställda i bolaget. Vår övergripande bedömning är att styrelsen och VD inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga.

Det saknas en tydlig organisation och ansvarsfördelning för hantering av kunder och framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Det finns en arbetsrutin, som endast till viss del säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Dokumenten är dessutom inte antaget av bolagets styrelse eller VD. Vi bedömer att bolaget bör upprätta en övergripande riktlinje och att styrelsen eller VD bör fastställa denna givet områdets komplexitet och medföljande risker som kräver insyn i hanteringen samt regelbunden uppföljning.

Nya medarbetare ska introduceras till bolagets arbetsrutiner gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen vilket vi ser positivt på. Däremot bedömer vi 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.

Vi noterar därutöver att bolaget inte har genomfört risk- och konsekvensanalyser kring hanteringen av skyddade personuppgifter inom ramen för bolagets systematiska internkontrollarbete, vilket vi bedömer vara en brist. Vi delar intervjuades uppfattning att skyddade personuppgifter bör prioriteras framgent genom att utgöra en del av bolagets systematiska arbete och följa ett årshjul genom att exempelvis uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år.

Avdelningen kundrelationer har vidtagit åtgärder för hanteringen av skyddade personuppgifter. Vi bedömer dock att det finns vissa brister i nuvarande hantering, däribland avsaknad av automatiska behörighets- och åtkomstbegränsningar inbyggda i verksamhetssystemen, att vissa nuvarande arbetsprocesser delvis kräver manuell hantering samt att det inte genomförs loggkontroller. Bolaget är medvetna om bristerna och har eller ska utifrån genomförd risk- och väsentlighetsanalys vidta ytterligare åtgärder.

Det saknas ett avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det inte går att identifiera skyddade personuppgifter från övriga avvikelser. 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.

Utifrån granskningens iakttagelser rekommenderar vi styrelsen och VD i Nacka vatten och avfall AB att:

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

- Upprätta och anta en riktlinje av övergripande karaktär för hanteringen av skyddade personuppgifter.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet.
- 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.

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.

Lekmannarevisionen har beslutat genomföra en fördjupad granskning av Nacka vatten och avfall AB:s arbete med rutiner, kunskapsspridning och säkerhetsfrågor vad gäller hanteringen av skyddade personuppgifter.

2.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma hur styrelse och VD för Nacka vatten och avfall AB säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Granskningen avser skyddade personuppgifter för såväl anställd personal som för kunder.

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 styrelse och VD tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Har styrelse och VD analyserat risken för att skyddade personuppgifter röjs?
- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?
- Har styrelse och VD 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 Nacka vatten och avfall AB kring hur skyddade personuppgifter ska hanteras?

2.3 Ansvarig bolagsstyrelse

Granskningen avser Nacka vatten och avfall AB.

2.4 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer. 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 och bolagsstämma. 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
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer
- Ägardirektiv
- 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.

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, integritet och etiska värderingar viktiga. Utöver organisationskultur består kontrollmiljön även av styrdokument, till exempel rutiner och riktlinjer.

3.1 Nacka vatten och avfall AB är personuppgiftsansvarig inom sitt verksamhetsområde

Nacka vatten och avfall AB (NVOA) är ett av Nacka kommuns helägda bolag genom Nacka Stadshus AB. Den primära verksamheten är att leverera säkra vatten- och avfallstjänster för alla som besöker, lever och verkar i Nacka kommun. Nacka kommun har gett i uppdrag till NVOA att förvalta och ansvara för utbyggnad, drift och underhåll av vattennätet samt att ansvara för såväl återvinning som avfallshantering.

Enligt NVOA:s ägardirektiv ska bolaget bidra till kommunens vision om "öppenhet och mångfald" och kommunens övergripande mål samtliga följa kommunens övriga styrande dokument. Bolaget ska följa Nacka kommuns fyra styrprinciper, vilket innebär att:

- bolaget genom en öppen och transparent redovisning av sina intäkter och kostnader ska bidra till att kommunfullmäktige har ett rättvisande underlag för fastställande av nätavgifter och delårsrapporter,
- bolaget uppnår samma kvalitet på levererade tjänster som övriga leverantörer i kommunen,
- bolaget genom kunskapsdelning samverkar med andra utförare av liknande tjänster,
- bolaget genom varje ansvarsnivå säkerställer att beslut fattas så nära slutkunden som möjligt.

Personuppgiftsansvaret följer kommunkoncernens ansvarsfördelning; varje nämnd/styrelse är personuppgiftsansvarig för de personuppgifter som behandlas inom sitt verksamhetsområde. Det innebär att NVOA:s styrelse har ansvaret för att kundernas personuppgifter behandlas lagligt, säkert och i övrigt korrekt i bolaget.

3.2 Organisation och ansvarsfördelning för hanteringen av skyddade personuppgifter

Ansvarig för hanteringen av skyddade personuppgifter inom NVOA är bolagets dataskyddssamordnare, ytterst ansvarig är bolagets VD/styrelsen. Avdelning kundrelationer hanterar bolagets kunder med skyddade personuppgifter. Inom avdelningen finns två medarbetare med särskilt ansvar för hanteringen av kunder med skyddade personuppgifter. Kommunens centrala dataskyddsombud kan också indirekt genom att påtala brister i personuppgiftshantering i de årliga granskningsrapporterna påverka bolagets hantering av skyddade personuppgifter, men saknar dock formellt ansvar.

3.3 Styrande dokument och bolagsspecifika rutiner

Nacka kommuns *Informationssäkerhetsstrategi*, fastställd av kommunfullmäktige den 11 december 2017, utgör det styrande dokumentet för kommunens informationssäkerhetsarbete

och är därmed av relevans för hanteringen av skyddade personuppgifter även i bolaget. Av strategin framgår att informationssäkerhetsarbetet ska präglas av förtroende för medarbetares och leverantörers förmåga att hantera informationstillgångar på ett säkert sätt. Varje nämnd/bolag ansvarar för att informationstillgångar inom sitt ansvarsområde hanteras enligt gällande lagstiftning och strategin. Informationssäkerhetsarbetet ska vara uppbyggt så det är lätt att hantera information korrekt, vilket innefattar bland annat att det finns lättillgänglig kunskap om informationssäkerhetsarbetet och att det finns utbildning som är tillgänglig gör 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, inkluderade och framåtlutat
- Systematisk uppföljning, lärande och förbättringar

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

Det finns inget koncernövergripande styrdokument för hantering av skyddade personuppgifter specifikt. Vid intervju har detta kopplats till styrmodellen i Nacka. Upplevelsen bland intervjuade är att riktlinjer och/eller rutiner för arbetet med skyddade personuppgifter inte behöver beslutas på övergripande nivå, utan att frågan med fördel kan hanteras mer verksamhetsnära i bolaget.

I NVOA finns dock en bolagsspecifik arbetsrutin för hantering av skyddade personuppgifter, riktad till avdelningen kundrelationer. Det framgår inte om det är en rutin eller en riktlinje och det framgår inte heller vem som står som ägare eller har beslutat om dokumentet. Arbetsrutinen reviderades i mars 2023. Arbetsrutinen utgör ett stöd och vägledning för anställda inom NVOA vid hantering av skyddade personuppgifter. I den beskrivs bland annat detaljerad hantering av skyddade personuppgifter inom NVOA, däribland:

- behandling av skyddade personuppgifter i IT-system,
- utskrift av sekretessfakturor,
- rutin för flyttanmälan,
- hantering av inkommande ärenden
- utmaningar och risker med bolagets hantering av skyddade personuppgifter.

Av dokumentet framgår inte hur ofta den ska uppdateras, information kring ansvarsfördelning eller incidenthantering.

3.4 Det finns behov av ytterligare kompetensutveckling

Nya medarbetare ska alltid introduceras till bolagets arbetsrutin gällande hantering av skyddade personuppgifter. Respektive avdelningschef ansvarar för att medarbetarna har goda kunskaper om hanteringen av skyddade personuppgifter och sekretessbestämmelserna samt

för att kunskapsnivån bibehålls över tid genom utbildningar. Utbildning av nyanställda ingår i den obligatoriska utbildningsplanen. Innehållet i utbildningarna anpassas och baseras på resultatet av bolagets internkontroller. Vid nyanställning ingår utbildningar som rör dataskyddshantering, GDPR och skyddade personuppgifter.

Intervjuade beskriver dock dels att arbetet med att sprida bolagets rutiner kan stärkas, dels att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske årligen. Framförallt framhävs behovet av att stärka grundkunskaperna bland de medarbetare som sällan stöter på skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn.

3.5 Bedömning

Vår bedömning är att NVOA inte i tillräcklig utsträckning har säkerställt en god kontrollmiljö avseende risken för röjning av skyddade personuppgifter. Det finns relativt tydlig organisation och ansvarsfördelning för hantering av kunder med skyddade personuppgifter. Det saknas dock rutiner för framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Vi bedömer det delvis finnas en riskmedveten kultur där hanteringen av skyddade personuppgifter i viss utsträckning behandlas inom ramen för bolagets dataskyddsarbete, även om kopplingen kan bli tydligare. Den framtagna arbetsrutinen bedömer vi sakna nödvändig information, däribland hur ofta den ska uppdateras, information kring ansvarsfördelning, incidenthantering samt mer utförliga beskrivningar av risker i verksamheten. Det framgår inte heller vem som är ansvarig för den. Den är således inte ändamålsenlig då den inte kan säkerställa en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Stödet för medarbetarna bedömer vi därför inte vara tillräckligt.

Enligt bolagets arbetsrutiner ska nya medarbetare introduceras till arbetsrutinen gällande hantering av skyddade personuppgifter vilket vi ser positivt på. Det sker dock ingen formaliserad utbildning i hanteringen av skyddade personuppgifter regelbundet. Vi bedömer därför att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter 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.

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 har analyserats men inte inom ramen för bolagets internkontrollarbete

I dataskyddsombudets årliga granskningsrapport för 2022 identifieras ett antal förbättringar. Däribland konstateras att bolaget endast delvis har genomfört riskbedömningar för att bedöma om konsekvensbedömning krävs eller inte i syfte att identifiera om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas. Det saknas konsekvensbedömningar för sociala medier, kamerabevakning, Office 365 och HR/personal-processen där känsliga personuppgifter hanteras eller enskilda medarbetare kartläggs. Dataskyddsombudet rekommenderar även att säkerställa att konsekvensbedömningar görs i framtiden (om kriterierna för detta uppfylls) när personuppgifter behandlas på nya sätt, exempelvis i ett nytt digitaliseringsprojekt. Därutöver konstateras att bolaget saknar personuppgiftsbiträdesavtal (PUB-avtal) i de fall Nacka kommun agerar som biträde. Dataskyddsombudet rekommenderar bolaget att teckna PUB-avtal med kommunen eller, om det visar sig att Nacka kommun och bolaget gemensamt är personuppgiftsansvariga, överenskommelse som reglerar hanteringen av personuppgifter. Känsliga och extra skyddsvärda personuppgifter bedöms hanteras enligt bolagets särskilda rutiner.

Enligt intervjuade arbetar NVOA aktivt med att stärka riskanalysarbetet i flera olika led. Som en konsekvens av detta har det genomförts en risk- och konsekvensanalys kring hanteringen av skyddade personuppgifter, dock inte inom ramen för bolagets internkontrollprocess. Styrelsen har således inte involverats i riskanalysarbetet, men planeras enligt uppgift att vara det under hösten 2023. Riskanalysen genomfördes under våren 2022 och uppdaterades i februari 2023. De två områdena som analyseras är telefoni- och ärendehantering och postutskick. Riskerna som analyserats är spridning av personuppgifter (riskvärde 8 av 16), spridning till tredje part (riskvärde 4 av 16) och sen registrering av skyddade personuppgifter (riskvärde 6 av 16). Beskrivna åtgärder är bland annat mer utbildning i informationssäkerhet för kundservice samt att fler i kundservice lär sig att registrera skyddade personuppgifter korrekt.

Enligt intervjuade finns det en målsättning att hanteringen av skyddade personuppgifter ska prioriteras framgent genom att utgöra en del av bolagets systematiska dataskyddsarbete och följa ett årshjul genom att exempelvis uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år.

4.2 Bedömning

Vi ser positivt på att risken för röjning av skyddade personuppgifter har analyserats inom ramen för bolagets riskanalysarbete där tre specifika risker har analyserats. Vår uppfattning är dock att riskanalysen inte är tillräckligt omfattande mot bakgrund av identifierade brister kring hanteringen av skyddade personuppgifter som framkommer i granskningen. Vi noterar därutöver att bolaget inte har genomfört risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter inom ramen för bolagets systematiska internkontrollarbete, vilket vi

bedömer vara en brist. Vi delar intervjuades uppfattning att skyddade personuppgifter bör prioriteras framgent genom att utgöra en del av bolagets systematiska arbete och följa ett årshjul genom att exempelvis uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Vi bedömer att det i kombination med risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter inom ramen för styrelsens internkontrollarbete skulle innebära förhöjd prioritet och därigenom öka kunskaperna om eventuella brister samt risker för att vidta ytterligare ändamålsenliga åtgärder.

5. Kontrollaktiviteter – Bolagets 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 verksamhetens olika 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. Gemensamt är att aktiviteterna syftar till att reducera risk i någon omfattning.

5.1 Behandling av skyddade personuppgifter i IT- och verksamhetssystem

Skyddade personuppgifter ska enligt intervjuade hanteras med mycket stor försiktighet. Det ska på ett tydligt sätt framgå för de användare som har åtkomstbehörighet till skyddade personuppgifter att uppgifterna är markerade för skyddad folkbokföring eller har sekretessmarkering, både i IT-system och på utskrifter. Enligt intervjuade har bolagets dataskyddsarbete stärkts avsevärt de senaste åren, däribland har systemen anpassats till ny lagstiftning som kräver säker personuppgiftsbehandling.

Nacka kommun tillhandahåller information om NVOA:s kunder har skyddade personuppgifter. Informationen skickas en gång i veckan via funktionen säkra meddelanden till två kundhandläggare i bolagets kundservice. Uppgifterna består av personnummer, vilket typ av skyddade personuppgifter det avser samt från vilket datum det börjar gälla. Därefter uppdateras uppgifterna i bolagets kunddatabas samt i ärendehanteringssystemet med ett sekretesskydd och meddelandet från kommunen raderas. Processen är manuell och görs av en handläggare. Det sker således ingen kryptering av de skyddade personuppgifterna i kunddatabasen och i ärendehanteringssystemet vilket beskrivs vara en brist som enligt intervjuade ökar risken för röjning av skyddade personuppgifter. Enligt intervjuade har leverantören till systemet informerat bolaget om att det är möjligt att anpassa systemet för att kunna kryptera informationen, men att funktionen ännu inte har implementerats.

Därutöver finns inga behörighets- och åtkomstbegränsningar inbyggda i systemen. På kundavdelningen har behörigheten till hanteringen av skyddade personuppgifter begränsats till två personer. Enligt arbetsrutinen lämnar övriga medarbetare inom kundavdelningen alltid över samtliga ärenden som involverar hantering av skyddade personuppgifter till de utvalda medarbetarna, oavsett vad ärendet handlar om. Att två utvalda medarbetare hanterar alla kunder med skyddade personuppgifter beskrivs av intervjuade innebära att kunderna hanteras korrekt. Det beskrivs dock också innebära en ökad risk då det kräver att den kundtjänstmedarbetare som inte har behörighet att hantera skyddade personuppgifter identifierar att det rör sig om skyddade personuppgifter och påkallar en av de två utvalda medarbetarna för vidare hantering.

5.2 Hantering och kommunicering av skyddade personuppgifter

Som kommunalt bolag omfattas NVOA av den grundlagsstadgade offentlighetsprincipen. Denna princip medför en skyldighet att på begäran tillhandahålla, genom kopia eller på plats, allmänna handlingar. Oavsett om en sekretessmarkering eller skyddad folkbokföring finns ska verksamheten alltid göra en prövning vid en begäran om utlämnande av allmän handling. Finns det sekretessmarkering eller skyddad folkbokföring ska dessa fungera som en

varningssignal, samt utgöra en del av underlaget vid bedömningen om en handling ska lämnas ut.

Kommunicering med kund som har skyddade personuppgifter, däribland utskick av fakturor, sker via brev som skickas med Skatteverkets förmedlingsuppdrag. Det finns detaljerade beskrivningar i bolagets rutin kring tillvägagångssätt. Förloppet kräver hantering av fysiska papper med mycket känsliga uppgifter. Fakturahanteringen är inte behörighetsbegränsad. Enligt intervjuade beskrivs rutinerna dock vara förankrade bland samtliga medarbetare och det finns således en trygghet i hanteringen.

Kommunikation via e-post ska aldrig tillämpas vid hantering av skyddade personuppgifter. Däremot framställs det av intervjuade som ett problem och risk att personer med skyddade personuppgifter inte är tillräckligt vaksamma och skickar känsliga uppgifter via mejl till bolaget som då riskerar att få spridning. Det finns rutiner för medarbetare som beskriver hur sådana ärenden ska hanteras. Bolaget använder funktionen säkra meddelanden, det vill säga elektronisk kommunikation med hjälp av elektronisk legitimation, vid kommunicering med kund som har skyddade personuppgifter.

5.3 Det saknas en rutin för hanteringen av medarbetare med skyddade personuppgifter

NVOA har inte upprättat en rutin för hantering av medarbetare eller ansökningshandlingar med skyddade personuppgifter. Intervjuade hänvisar avsaknaden av en rutin till att bolaget inte har haft medarbetare eller ansökningshandlingar med skyddade personuppgifter. Om bolaget skulle komma i kontakt med ansökningshandlingar med skyddade personuppgifter eller om en anställd i bolaget skulle få skyddade personuppgifter uppger intervjuade att kommunens HR- och personalenhet skulle kontaktas för rådgivning. Det saknas kännedom om hur medarbetare med skyddade personuppgifter ska hanteras enligt kommunens rutiner och huruvida det finns en kommunövergripande rutin för medarbetare med skyddade personuppgifter. Intervjuade uppger att det för närvarande inte finns något behov av att upprätta en bolagsspecifik rutin för hanteringen av medarbetare med skyddade personuppgifter.

Bolaget beskrivs ha en öppen arbetsplatskultur vilket bland annat innefattar att det publiceras bilder på anställda i sociala medier och i interna kommunikationskanaler. Det beskrivs därigenom finnas anledning att resonera kring den öppna arbetskulturen framgent med hänvisning till skyddade personuppgifter.

5.4 Bedömning

Vår bedömning är att NVOA har vidtagit vissa åtgärder för att minska risken för röjning av skyddade personuppgifter, men att åtgärderna kan bli fler och skarpare.

Avdelning kundrelationer har upprättat arbetsrutiner för hanteringen av skyddade personuppgifter i syfte att minska risken för röjning av skyddade personuppgifter. Däribland specifika arbetsrutiner kring förfrågan om allmän handling, behandling av skyddade personuppgifter i IT- och verksamhetssystem samt säkra rutiner för hantering och kommunicering av skyddade personuppgifter.

Vi bedömer dock att det finns vissa brister i nuvarande hantering. En brist är att det inte sker en automatiserad kryptering av de skyddade personuppgifterna i kunddatabasen och i ärendehanteringssystemet. De skyddade personuppgifterna markeras manuellt. Ovan beskrivning av manuell hantering av skyddade personuppgifter kräver kunskap och extra

varsam hantering vilket ökar risken för felhantering och röjning orsakad av den mänskliga faktorn.

NVOA har inte genomfört kontroller av användarloggar med anledning av risken för röjning av skyddade personuppgifter. Loggkontroller är ett effektivt verktyg för att säkerställa att obehöriga inte får tillgång till skyddade personuppgifter i IT- och verksamhetssystemen. Vi bedömer att sådana bör genomföras som en organisatorisk säkerhetsåtgärd för att kompensera påtalade brister i systemstödens avsaknad av behörighetbegränsningar.

Därutöver bedömer vi det vara en brist att NVOA inte har analyserat risken för hantering av medarbetare eller ansökningshandlingar med skyddade personuppgifter. Det finns av den anledningen inte rutiner för hanteringen. Bolaget hänvisar till att kommunens HR- och personalenhet skulle kontaktas för rådgivning, men då det saknas kännedom om hur medarbetare med skyddade personuppgifter ska hanteras enligt kommunens rutiner och huruvida det finns en kommunövergripande rutin för medarbetare med skyddade personuppgifter bedömer vi att NVOA bör stärka dessa rutiner. Därutöver bedömer vi det vara aktuellt att se över nuvarande rutiner avseende publicering av bilder på anställda i sociala medier och i interna kommunikationskanaler.

6. Avvikelsehantering

6.1 Det finns inga rapporterade avvikelser avseende skyddade personuppgifter

Samtliga personuppgiftsincidenter ska rapporteras enligt särskild rutin för personuppgiftsincident. Det finns ingen egen process för avvikelser gällande skyddade personuppgifter. Det framgår inte om dokumentation görs i särskild mall innehållandes en riskbedömning av personuppgiftsincidenten.

Nacka kommuns dataskyddsombuds granskningsrapport konstateras att en incident rapporterats under 2022, vilket enligt rapporten kan bero på att inga andra incidenter skett men också på att inträffade incidenter inte rapporterats på grund av okunskap om definitionen av en incident. Ingen av de rapporterade incidenter rörde skyddade personuppgifter. Det har aldrig rapporterats någon incident avseende hanteringen av skyddade personuppgifter.

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. 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.

7. Svar på revisionsfrågor

Fråga	Svar
Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?	Nej. Styrelse eller VD har inte beslutat om ett styrande dokument för hantering av skyddade personuppgifter. Avdelningen kundrelationer har upprättat en arbetsrutin, med okänd klassificering, vilken vi bedömer sakna tillräcklig information på såväl övergripande som detaljerad nivå för bolagets medarbetare. Vi bedömer därför att styrelse eller VD bör upprätta och anta en övergripande riktlinje i syfte att säkerställa tillräcklig insyn och uppföljning i bolagets arbete kring hanteringen av skyddade personuppgifter.
Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?	Nya medarbetare introduceras till arbetsrutinen gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen. Det framgår inte med vilken regelbundenhet information ges.
Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?	Nej. Det saknas en tydlig organisation och ansvarsfördelning för hantering av kunder och framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Tillgängligt stöd till medarbetare genom arbetsrutinen bedömer vi inte är tillräckligt.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Det sker ingen fortlöpande kompetensutveckling vilket vi bedömer vara en brist. 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.
Har styrelsen och VD tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Nej. Skyddade personuppgifter utgör inte en del av bolagets systematiska dataskyddsarbete genom att följa ett årshjul, bl.a. innefattande uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Styrelsen har inte genomfört någon uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter. Vi noterar att det finns en sådan målsättning.
Har styrelsen och VD analyserat risken för att skyddade personuppgifter röjs?	Nej. Avdelningen kundrelationer har genomfört en risk- och väsentlighetsanalys kring hanteringen av skyddade personuppgifter, dock inte inom ramen för bolagets internkontrollprocess. Styrelsen har således inte involverats i riskanalysarbetet, men planeras enligt uppgift att vara det under hösten 2023.
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?	Ja. I avdelningen kundrelationers genomförda risk- och väsentlighetsanalys har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats. Utifrån identifierade risker och brister har åtgärder vidtagits eller ska vidtas i närtid.
Har styrelsen och VD vidtagit åtgärder för att minska risken för röjning	Nej. Styrelse eller VD har inte beslutat om ett styrande dokument för hantering av skyddade personuppgifter samt inte genomfört en risk- och väsentlighetsanalys inom ramen för bolagets internkontrollprocess.

av skyddade personuppgifter?	Däremot har avdelningen för kundrelationer genomfört en risk- och väsentlighetsanalys och utifrån denna vidtagit vissa åtgärder för att minska risken för röjning av skyddade personuppgifter. Vi noterar samtidigt att åtgärderna kan bli fler och skarpare. Bolaget är medvetna om bristerna och har eller ska utifrån avdelningen kundrelationers genomförda risk- och väsentlighetsanalys vidta ytterligare åtgärder.
Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?	Nej. Vi bedömer att det inte finns ett avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns ingen egen process för avvikelser gällande skyddade personuppgifter. 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.
Hur tillvaratas erfarenhet från avvikelser?	Det saknas rutiner för hur erfarenheter från avvikelser ska tillvaratas. Bolaget har aldrig rapporterat någon incident eller avvikelse avseende hanteringen av skyddade personuppgifter.
Råder det samsyn inom Nacka kommun och Nacka vatten och avfall AB kring hur skyddade personuppgifter ska hanteras?	Nej. Det råder inte samsyn gällande arbetsrutiner och det operativa arbetet med skyddade personuppgifter i kommunen och i bolaget. Exempelvis har olika enheter i kommunen och bolagen 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.

Stockholm den 24 maj 2023

David Leinsköld
Verksamhetsrevisor, EY

Daniel Larsson
Verksamhetsrevisor, EY

Bilaga 1 Källförteckning

Intervjuade funktioner

- VD
- Ekonomichef
- Financial controller
- Avdelningschef verksamhetsstöd och HR
- Kundstrateg avdelning kundrelationer och kundservice

Granskad dokumentation

- Ägardirektiv för Nacka vatten och avfall AB
- Bolagsordning Nacka vatten och avfall AB
- Informationssäkerhetsstrategi (dnr KFKS 2017/990)
- Rutin skyddade personuppgifter avdelning kundrelationer

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.

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. Siffran är inte exakt 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[1] 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 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).

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

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[2] 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.

[2] I och med att ett kommunalt bolag i regel är ett aktiebolag betraktas det inte vara en myndighet. De kommunala bolagen är dock att jämställa med myndighet om kommunen utövar ett rättsligt bestämmande inflytande över bolaget, vilket Nacka kommun gör över NVOA.