Kommunrevisorerna granskar Umeå Vatten och Avfallskompetens i Norr AB:s hantering av skyddade personuppgifter

2023-12-14

UMEÅ KOMMUN

Angående granskningen

Revisionsuppdraget är ett kommunalt förtroendeuppdrag och revisorerna är direkt ansvariga inför kommunfullmäktige och därmed indirekt inför medborgarna genom den representativa demokratin. Revisionen har uppdrag att granska de verksamheter som styrelser, nämnder och kommunala bolag bedriver.

I formell mening är varje revisor en egen myndighet, men i det praktiska revisionsarbetet sker arbetet gemensamt.

Ytterst syftar revisionen till att undersöka om verksamheten bedrivs i enlighet med uppställda mål och på ett från ekonomisk synpunkt tillfredsställande sätt.

- Revisorernas uppdrag regleras i kommunallag, aktiebolagslag, god revisionssed, ägardirektiv och reglemente.
- Revision ska utföras på ett oberoende sätt.
- Revisorerna genomför grundläggande granskning, granskning av delårsrapport och årsredovisning och fördjupade granskningar.

Revisorerna ska därför objektivt, opartiskt och sakligt, självständigt granska den verksamhet som styrelse, nämnder och beredningar bedriver. Revisorerna ska också bedöma om de förtroendevalda ledamöterna i nämnder och styrelser har tillräcklig styrning och kontroll över verksamhetens ekonomi, prestationer och kvalitet.

Revisorernas uttalanden och bedömningar finns i revisionsberättelser och granskningsrapporter. En ambition i revisorernas arbete är att deras rekommendationer i samband med granskning ska kunna användas av verksamheterna för att åstadkomma effekter i deras förbättringsprocess.

Kontaktuppgifter

Om kommunrevisorernas uppdrag

kommunrevisionen@umea.se

Ordförande i kommunrevisionen

Ewa Miller, ordförande
ewa.miller@umea.se

Umeå Vatten och Avfallskompetens i Norr AB

Granskning av bolagets hantering av skyddade personuppgifter

Umeå 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 Vatten och Avfallskompetens i Norr AB är personuppgiftsansvarig inom sitt verksamhetsområde ... 6
   3.2 Bolaget har inte beslutat om styrdokument för hanteringen av skyddade personuppgifter 6
   3.3 Det finns behov av ytterligare kompetensutveckling 8
   3.4 Bedömning 8
4. Riskbedömningar 10
   4.1 Risken för och konsekvensen av röjning av skyddade personuppgifter har inte analyserats inom ramen för bolagets internkontrollarbete 10
   4.2 Bedömning 10
5. Kontrollaktiviteter – Bolagets rutiner och arbetssätt 11
   5.1 Behandling av skyddade personuppgifter i bolagets IT- och verksamhetssystem samt tillhörande processer 11
   5.2 Bedömning 12
6. Avvikelsehantering 13
   6.1 Det går inte att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter 13
   6.2 Bedömning 13
7. Svar på revisionsfrågor 14

Bilaga 1 Källförteckning 16
Bilaga 2 Revisionskriterier 17

1. Sammanfattande bedömning och rekommendationer

Lekmannarevisorerna har gett det sakkunniga biträdet från EY i uppdrag att granska Umeå Vatten och Avfall AB:s hantering av skyddade personuppgifter. Det finns ingen anställd personal hos Umeå Vatten och Avfall. Bolaget köper alla personella resurser av det majoritetsägda dotterbolaget Vatten och Avfallskompetens i Norr AB (Vakin) som bedriver verksamheten åt Umeå Vatten och Avfall AB. I rapporten hänvisar vi fortsättningsvis till Vatten och Avfallskompetens i Norr AB (Vakin).

Syftet med granskningen har varit att bedöma hur styrelse och VD för Vatten och avfallskompetens i Norr AB säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Granskningen har omfattat skyddade personuppgifter för såväl anställd personal som för kunder. Vår sammanfattande bedömning är att styrelsen och VD inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga samt att bolagets tillämpade rutiner inte är ändamålsenliga.

Övergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen innehåller få skrivningar om hanteringen av skyddade personuppgifter. Detta i kombination med att det inte finns ett beslutat övergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi vara en brist. Vi noterar att det har upprättats en verksamhetsnära rutinbeskrivning för hanteringen av skyddade personuppgifter och tillhörande processer. Rutinbeskrivningen utgör ett värdefullt stöd i sammanhanget, men vi noterar att denna endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att den har utrymme för utveckling.

Vi har också identifierat förbättringsområden i hanteringen av skyddade personuppgifter. Bolagets styrelse har inte gjort någon uppföljning inom området avseende exempelvis arbetsrutiner, kompetensutveckling eller avvikelsehantering. Det har heller inte genomförts risk- och konsekvensanalyser avseende röjning av skyddade personuppgifter inom ramen för det systematiska internkontrollarbetet. Detta med hänvisning till det begränsade antalet kunder med skyddade personuppgifter som hanteras av bolaget. Trots den begränsade mängd kunder är vår bedömning att hanteringen av skyddade personuppgifter bör stärkas 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. Det är ett rimligt förfarande, men då det inte finns möjlighet att särskilja incidenter avseende skyddade personuppgifter från andra personuppgiftsincidenter finns en risk att förutsättningarna för uppföljning av incidenter blir sämre.

Utifrån granskningen iakttagelser rekommenderar vi styrelsen och VD i Vatten och Avfallskompetens i Norr AB att:

- Genomför risk- och konsekvensanalyser specifikt avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta ett styrdokument av övergripande karaktär för hanteringen av skyddade personuppgifter. Riktlinjen bör tydliggöras genom verksamhetsnära rutiner/instruktioner.

- Genomföra regelbundna utbildningar för samtliga medarbetare som hanterar skyddade personuppgifter, exempelvis som en del av ett årshjul. Överväg också att på en övergripande nivå informera samtliga medarbetare om skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter i befintliga system.

2. Inledning

2.1 Bakgrund

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Antalet personer i Sverige med skyddade personuppgifter har de senaste åren ökat. Mellan åren 2011 och 2023 har antalet personer med skyddade personuppgifter ökat från drygt 12 000 personer till drygt 28 000 personer.[1] Den 1 januari 2019 trädde lagändringar i kraft med syfte att öka skyddet för hotade och förföljda personer.

Jämställdhetsmyndigheten publicerade under år 2022 en rapport (2022:10) där flera våldsutsatta kvinnor intervjuades. 86 kvinnor ingick i urvalet. Av dessa uppgav tre av fyra att de någon gång fått sina skyddade personuppgifter röjda. Hälften av de intervjuade kvinnorna har flyttat minst en gång på grund av röjda uppgifter. Flera kvinnor berättar att de röjts på grund av att information om kvinnornas personuppgifter har röjts från till exempel socialtjänsten och andra myndigheter.

Personer med skyddade personuppgifter kan drabbas av mycket allvarliga risker och problem om kommuners verksamheter inte har en ändamålsenlig kontroll över uppgifterna. Kommuner måste därför ha tydliga riktlinjer och kontroller för att hantera skyddade personuppgifter. Det är av väsentlighet att sådana rutiner är välkända bland samtliga medarbetare då i princip samtliga kan komma i kontakt med en person som har skyddade personuppgifter.

Umeå kommuns lekmannarevisorer har i sin riskanalys för 2023 identifierat hanteringen av skyddade personuppgifter som ett angeläget område för fördjupning och beslutat att genomföra en granskning av Vatten och Avfallskompetens i Norr 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 Vatten och Avfallskompetens i Norr AB säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpas. Granskningen avser skyddade personuppgifter för såväl anställd personal som för kunder.

I granskningen besvaras följande revisionsfrågor:

- Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter?
    - Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?
- Har bolaget säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?
- Har bolaget på ett ändamålsenligt sätt analyserat och bedömt risken för att skyddade personuppgifter röjs?

[1] SVT, "Kraftig ökning av skyddade personuppgifter", hämtad 2023-12-05.

- Har den enskilda individens perspektiv beaktats?

- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?
- Har bolaget vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?
- Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter?
    - Hur tillvaratas erfarenhet från avvikelser?

2.3 Ansvarig bolagsstyrelse

Granskningen avser Umeå Vatten och Avfall AB. Det finns ingen anställd personal hos Umeå Vatten och Avfall. Bolaget köper alla personella resurser av det majoritetsägda dotterbolaget Vatten och Avfallskompetens i Norr AB (Vakin) som bedriver verksamheten åt Umeå vatten och Avfall AB, Vindeln Vatten och Avfall AB samt Nordmaling Vatten och Avfall AB. I rapporten hänvisar vi fortsättningsvis till Vakin.

2.4 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer med berörda tjänstepersoner. 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:

- Offentlighets- och sekretesslagen (2009:400)
- Folkbokföringslagen (1991:481)
- Folkbokföringsfördordning (1991:749)
- SFS 2018:695 Lag om ändring i folkbokföringslagen
- 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 samt löpande i rapporten.

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 Vatten och Avfallskompetens i Norr AB är personuppgiftsansvarig inom sitt verksamhetsområde

Umeå Vatten och Avfall AB är ett av Umeå kommuns helägda bolag genom moderbolaget Umeå kommunföretag (UKF). Syftet med bolagets verksamhet är att bedriva verksamhet avseende vattenförsörjning, omhändertagande av avloppsvatten samt kommunal avfallshantering och därmed förenlig verksamhet. Det finns ingen anställd personal hos Umeå Vatten och Avfall. Bolaget köper alla personella resurser av det majoritetsägda dotterbolaget Vatten- och Avfallskompetens i Norr AB (Vakin) som bedriver verksamheten åt Umeå Vatten och Avfall AB, Vindeln Vatten och Avfall AB samt Nordmaling Vatten och Avfall AB.

Av Vakins arbets- och beslutsordning[2] framgår inte om styrelsen eller VD ska ägna sig åt övergripande och långsiktiga frågor samt frågor som är av osedvanlig beskaffenhet eller av stor betydelse för bolaget eller koncernen. Styrelsen ska utöva erforderlig kontroll över hur VD handhar den löpande förvaltningen. Huvudprinciperna för delegationen är att beslut av policykaraktär, beslut som är styrande för bolagets inriktning eller beslut som binder resurser av väsentlig storlek för bolaget är styrelsefrågor medan verkställighetsfrågor eller beslut inom angivna ramar eller upp till angivna beloppsgränser är delegerade till VD.

Styrelsen ska besluta om att fastslå policydokument, upprättade av VD i samråd med ansvarig chef inom det aktuella området. Däremot tydliggörs inte vem som ska fatta beslut om riktlinjer. VD beslutar om IT-strategi som IT-chef upprättar, samt om IT-frågor som omfattar bolagets IT-plattform. Det framgår inte vem som beslutar om att fastställa samt ansvarsfördelning kring säkerhetsorganisation, däribland organisering av informationssäkerhet samt incident- och krishantering. Roll- och ansvarsfördelningen tydliggörs i stället i bolagets riktlinjer för informationssäkerhet, se avsnitt 3.2.

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

Roll- och ansvarsfördelningen för hanteringen av skyddade personuppgifter framgår inte av styrande dokument. Det tydliggörs inte heller av bolagets rutinbeskrivningar.

3.2 Bolaget har inte beslutat om styrdokument för hanteringen av skyddade personuppgifter

I Umeå kommun finns riktlinjer för informationssäkerhet, som kompletterar kommunfullmäktiges informationssäkerhetspolicy med mer detaljerad information och regler

[2] Fastställd av styrelsen 2022-12-09.

för hur information får hanteras inom kommunen. Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om informationssäkerhetspolicy och riktlinjer för informationssäkerhet inom den egna verksamheten.

Vakin har upprättat bolagsspecifika riktlinjer för informationssäkerhet[3] vars syfte är att konkretisera bolagets informationssäkerhetspolicy. Bolagets informationssäkerhetsarbete syftar till att vidta åtgärder så att bolagets informationstillgångar förblir tillgängliga, riktiga och konfidentiella. Med informationstillgångar avses all information och informationshanterande resurser såsom manuella samt digitaliserade och IT-system. Enligt intervjuade bygger riktlinjerna på Umeå kommuns riktlinjer för informationssäkerhet.

Informationssäkerhet är en del av Vakins ledningssystem för att upprätthålla och bibehålla tjänster och förtroende. Högsta ledningen ska tydligt visa ledarskap och åtagande i fråga om ledningssystemet för informationssäkerhet. Förankringen och medvetandet hos medarbetare är grunden för att lyckas med detta arbete. Det är därför varje chefs ansvar att kommunicera vikten av god informationssäkerhet. Säkerhetschefen ansvarar för det övergripande säkerhetsarbetet inom hela Vakin, vilket även innefattar området informationssäkerhet. Säkerhetschefen ansvarar för att leda och samordna det systematiska säkerhetsarbetet tillsammans med representanter från Vakins olika verksamhetsområden. IT-ansvarig ansvarar för säkerheten i och kring de IT-system som organisationen hanterar och förfogar över och samverkar med säkerhetschefen.

Utöver organisation av informationssäkerhetsarbetet utvecklas ett antal områden i riktlinjerna som indirekt får konsekvenser för bolagets hantering av skyddade personuppgifter, bland annat:

- Riskbedömning och riskbehandling
- Personalsäkerhet
- Hantering av tillgångar
- Styrning av åtkomst
- Kryptering
- Drift- och kommunikationssäkerhet
- Anskaffning, utveckling och underhåll av system
- Leverantörsrelationer
- Informationssäkerhetsincidenter
- Efterlevnad

Det saknas information om hanteringen av skyddade personuppgifter i riktlinjen för informationssäkerhet. Riktlinjen konkretiseras dock ytterligare i underliggande rutiner och instruktioner och rutiner. I rutin för IT-hantering framgår att sekretessklassad information endast ska hanteras i Vakins system om det har en tydlig funktion för sekretessmarkering. Saknas stöd för detta får inte verksamhetssystemet hantera skyddade personuppgifter. Uppgifterna måste då vara fiktiva alternativt strikt hanteras utanför den digitala miljön.

Utöver det finns en verksamhetsnära rutinbeskrivning i form av en instruktion som beskriver den praktiska hanteringen av skyddade personuppgifter. Rutinbeskrivningen har upprättats på

[3] Framgår inte om de är fastställda av styrelsen. Senast reviderade 2023-11-30.

en verksamhetsnära nivå genom ett behov utifrån identifierade brister i arbetssätt av de tjänstepersoner som kommer i kontakt med skyddade personuppgifter. Den har inte upprättats utifrån genomförd riskanalys eller på uppdrag av styrelse eller VD. Den är således inte fastställda av vare sig styrelsen eller VD.

Intervjuade framhåller att styrelsen lämpligen inte bör besluta om ett styrdokument som rör skyddade personuppgifter, bland annat med hänvisning till bolagets styrmodell där styrelsen endast fattar beslut om övergripande policydokument. I och med att bolaget hanterar en liten mängd kunder med skyddade personuppgifter anser intervjuade det inte vara nödvändigt med en enskild policy för den hanteringen, då det i stället ryms inom ramen för det övriga informationssäkerhetsarbetet. Intervjuade uppger att det inte heller finns ett behov att upprätta en övergripande riktlinje, fastställd av VD, för att tydliggöra och styra arbetet med skyddade personuppgifter med samma anledning som ovan. Enligt intervjuade finns därför redan en god intern kontroll över hanteringen av skyddade personuppgifter.

3.3 Det finns behov av ytterligare kompetensutveckling

Varje chef ansvarar för att informera medarbetare om nya och uppdaterade riktlinjer. Varje medarbetare har eget ansvar att följa riktlinjerna, däribland instruktionen för skyddad identitet. Det saknas dock en obligatorisk utbildning om hanteringen av skyddade personuppgifter. Det saknas därför ett utpekat ansvar för att medarbetarna har goda kunskaper om hanteringen av skyddade personuppgifter, bolagets sekretessbestämmelser samt för att kunskapsnivån bibehålls över tid genom utbildningar. Intervjuade har inte identifierat ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt, och att så bör ske årligen. De som hanterar skyddade personuppgifter uppges ha tillräcklig kunskap.

3.4 Bedömning

Vår bedömning är att det saknas ändamålsenliga styrande dokument för hantering av skyddade personuppgifter. Det finns styrande dokument för arbetet med informationssäkerhet, men då dessa innehåller få skrivningar om hanteringen av skyddade personuppgifter, i kombination med att det inte finns ett beslutat styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi det inte vara tillräckligt. Vi noterar att det har upprättats en verksamhetsnära rutinbeskrivning i form av en instruktion för hanteringen av skyddade personuppgifter och tillhörande processer. Instruktionen utgör ett värdefullt stöd i sammanhanget, men vi noterar att den endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter, och vår bedömning är att den har utrymme för utveckling. 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 verksamhetsnivå 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/riktlinje fastställd av styrelse/VD. Detta trots den begränsade mängd kunder med skyddade personuppgifter som hanteras.

Trots avsaknaden av övergripande styrdokument inom området bedömer vi enheterna vara medvetna om att de ska bedriva ett eget arbete med att säkerställa trygg hantering av skyddade personuppgifter. Vi noterar att varken styrelse eller VD har genomfört någon särskild uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter.

Med hänsyn till avsaknaden av övergripande styrdokument bedömer vi att det skulle finnas ett värde i att styrelsen stärker uppföljningen och kontroll inom området.

Vi bedömer att den kompetensutveckling som finns inte fullt är tillräcklig. I kombination med utvecklingsområdena i styrdokument och rutinbeskrivningen, bedömer vi att det inte finns ett tillräckligt stöd till medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter. Då fel orsakat av den mänskliga faktorn är den största risken för röjning av skyddade personuppgifter, bedömer vi det vara särskilt angeläget att stärka kontrollmiljön inom området.

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 bolagets internkontrollarbete

Risker för röjning av skyddade personuppgifter har inte ingått i bolagets internkontrollplaner. Av intervju har framkommit att röjningen av skyddade personuppgifter inte har betraktats som en tillräckligt allvarlig risk för att inkluderas i riskanalysen. Om ett flertal incidenter skulle inträffa skulle också riskanalysen se annorlunda ut.

Bland de intervjuade finns en samlad bild att risken för röjning av skyddade personuppgifter fångas upp i bolagets systematiska informationssäkerhetsarbete genom riskbedömning och riskbehandling. Bolaget ska regelbundet identifiera hot för att undvika informationssäkerhetsrisker. Riskbedömningar kan exempelvis ske vid anskaffning av varor eller tjänster vilket inkluderar upphandling av nya IT-system, samt vid informationsklassning av processer som delvis omfattar hanteringen av skyddade personuppgifter. Bland annat sker bedömning av risker löpande och i varje enskilt fall av de handläggare som hanterar skyddade personuppgifter, i dialog med den enskilde som har skyddade personuppgifter.

4.2 Bedömning

Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har inte upprättats inom ramen för bolagets systematiska internkontrollarbete, vilket vi bedömer är en brist. Med hänsyn till de allvarliga konsekvenser som en röjning av skyddade personuppgifter kan få ser vi att hela processen kring hanteringen av skyddade personuppgifter åtminstone bör utvärderas i risk- och väsentlighetsanalys. Detta kan också stärka styrelsens insyn och uppföljning inom området.

Vi bedömer att säkerhetsfrågor kopplade till skyddade personuppgifter delvis har analyserats och trygghetsskapande åtgärder vidtagits. Bedömningen bygger på de risk- och skyddsbedömningar avseende potentiella säkerhetsrisker som görs i anslutning till hantering av kunder med skyddade personuppgifter, bland annat av verksamhetssystem och genom kartläggning av potentiella risker. Därigenom beaktas den enskilda individens perspektiv även om vi bedömer att arbetet kan stärkas.

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 risker.

5.1 Behandling av skyddade personuppgifter i bolagets IT- och verksamhetssystem samt tillhörande processer

Bolaget använder flera IT-system som hanterar kunduppgifter. Kunder med skyddade personuppgifter hanteras i ett kärnsystem, genom att tilldelas ett alias utan personnummer och adressuppgifter. De riktiga uppgifterna skrivs ut på papper, och förvaras inlåsta i ett kassaskåp som ett begränsat antal personer har tillgång till. I respektive system hanteras således inte skyddade personuppgifter, då de inte kan krypteras och markeras med en varningstriangel eller liknande, utan får ett alias. Det saknas därutöver tekniska möjligheter att i systemen begränsa behörigheten till kunder med skyddade personuppgifter, det vill säga tekniskt styra behörigheten till en viss handläggare. Det kräver således manuell hantering av skyddade personuppgifter och de hanteras strikt utanför den digitala miljön enligt skrivelsen i rutin för IT-hantering. Enligt intervjuade är dock nuvarande hantering säker, och upplever inte brister i nuvarande systemstöd. Detta främst med tanke på fåtalet kunder med skyddade personuppgifter de kommer i kontakt med. Det finns därför, enligt intervjuade, inte själ att upphandla ett nytt kundinformationssystem, där bolaget som kravställare och upphandlare har möjlighet att ställa krav på en mer ändamålsenlig hantering av skyddade personuppgifter.

All användning av IT och internet loggas för att i efterhand kunna utreda incidenter. Stickprov kan göras i känsliga system för att se om användare har använt systemen utan lov. Loggarna används även för att effektivisera IT-produktionen samt för att spåra fel och brister. Loggning har dock inte skett med anledning av att upptäcka brister i hanteringen av skyddade personuppgifter, detta enligt intervjuade då skyddade personuppgifter endast hanteras utanför de digitala miljöerna. Bolaget genomför penetrationstester, det vill säga skanning av sårbarheter med automatiska verktyg för att upptäcka brister och svagheter i systemen. Dock inte med anledning av risken för röjning av skyddade personuppgifter med samma anledning som ovan.

Kommunicering med kunder som har skyddade personuppgifter sker via telefon eller post. Post skickas med rekommenderat brev via Skatteverkets förmedlingstjänst, däribland fakturor till vissa kunder. Känslig och sekretessklassad information, exempelvis skyddade personuppgifter, får inte hanteras i mejl. Dokument som skannas skickas ofta med mejl från skannern till mottagarens e-postadress. Skanning av dokument som innehåller känslig eller sekretessklassad information ska ske via verktyget ’Säker skanning’. Om mejl inkommer som innehåller känslig eller sekretessklassad information ska denna genast flyttas till annan lagringsform. Chatt är för en del medarbetare ett vanligt och viktigt sätt att kommunicera internt inom kommunenkoncernen och till vissa grupper av externa parter. Känslig information eller information som klassificerats med sekretess får inte hanteras i chatt. Det finns inte ett

system för krypterad e-post. Enligt intervjuade finns en stor medvetenhet bland bolagets anställda att inte lämna ut uppgifter om kunder till privatpersoner eller andra myndigheter via e-post eller vid telefonsamtal.

Det saknas riktlinjer för hantering av skyddade personuppgifter i bolagets HR-processer. Enligt intervjuade har det inte funnits ett behov av en sådan särskild rutin då ingen med skyddade personuppgifter har sökt en tjänst inom bolaget.

5.2 Bedömning

Vår bedömning är att styrelse och VD inte har vidtagit tillräckliga åtgärder för att minska risken för röjning av skyddade personuppgifter. Vi noterar dock att enheten kundservice har vidtagit ett antal olika åtgärder, även om vi också bedömer att det samtidigt finns utrymme för förbättringar som presenteras nedan. Vi bedömer det vara särskilt angeläget att styrelsen och VD följer upp vidtagna åtgärder.

Det finns brister i nuvarande systemstöd. Dels saknas en tydlig funktion för sekretessmarkering, vilket resulterar i strikt manuell hantering av de skyddade personuppgifterna. Detta är i linje med rutin för IT-hantering, men vi bedömer det finns risker att systemstöden inte har en funktion för sekretessmarkering, då det medför risker att hantera skyddade personuppgifter utanför systemet. Detta då manuell hantering av skyddade personuppgifter ställer exceptionella krav på noggrannhet och riskmedvetenhet samt ökar risken för felhantering orsakad av den mänskliga faktorn.

6. Avvikelsehantering

6.1 Det går inte att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter

Samtliga personuppgiftsincidenter rörande skyddade personuppgifter rapporteras som personuppgifts- eller säkerhetsincidenter. I nuvarande arbetsrutin för hanteringen av skyddade personuppgifter saknas information om incidenthantering. Av bolagets användarhandbok IT framgår att IT-ansvarig och/eller säkerhetschef ska kontaktas omgående om pågående eller inträffad informationssäkerhetsincident. Det går inte att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter vid en incidentrapportering. Ingen incident har rapporterats som rör bolagets hantering av skyddade personuppgifter.

6.2 Bedömning

Vi bedömer att det inte finns ett ändamålsenligt 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. Det bör även inkluderas i styrande dokumentation som rör hanteringen av skyddade personuppgifter. Då incidenter avseende skyddade personuppgifter inte på något sätt särskiljs från övriga personuppgiftsincidenter är vår bedömning även att det finns begränsade förutsättningar för uppföljning inom området, vilket riskerar få konsekvensen att erfarenheter från avvikelser inte tillvaratas.

7. Svar på revisionsfrågor

Fråga	Svar
Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter? o *Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?*	Nej. Det finns styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men styrelse eller VD har inte beslutat om något styrande dokument för hantering av skyddade personuppgifter specifikt. Det har upprättats en arbetsrutin utifrån det egna upplevda behovet av de som hanterar skyddade personuppgifter. Den utgör ett värdefullt stöd i sammanhanget, men vi noterar att den endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter. Varje chef ansvarar för att informera medarbetare om nya och uppdaterade riktlinjer. Styrande dokument publiceras i verksamhetssystemet och är tillgängliga för samtliga medarbetare.
Har bolaget säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Nej. Det finns inga styrdokument inom området, men de medarbetare som hanterar skyddade personuppgifter är medvetna om att de ska bedriva ett eget arbete med skyddade personuppgifter. Styrelse eller VD har inte 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 av styrelse eller VD.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Med hänvisning till den begränsade mängd kunder med skyddade personuppgifter genomförs ingen utbildning eller övrig kompetensutveckling kring hanteringen av skyddade personuppgifter. Utbildningar i säkerhetsskydd, informationssäkerhet och GDPR genomförs regelbundet. Skyddade personuppgifter kommer eventuellt inkluderas i någon utbildning 2024.
Har bolaget på ett ändamålsenligt sätt analyserat och bedömt risken för att skyddade personuppgifter röjs? o *Har den enskilda individens perspektiv beaktats?*	Nej. Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har inte upprättats inom ramen för bolagets systematiska internkontrollarbete. Ja. Genom de risk- och skyddsbedömningar avseende potentiella säkerhetsrisker som görs i anslutning till hantering av kunder med skyddade personuppgifter, bland annat av verksamhetssystem och genom kartläggning av potentiella risker, beaktas den enskilde individens perspektiv.
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygg-hetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?	Delvis. Styrelse eller VD har inte själva genomfört några analyser inom området. De har inte heller tillsett att säkerhetsfrågor analyseras och åtgärder vidtas av enheterna. Däremot görs individuella risk- och skyddsbedömningar avseende potentiella säkerhetsrisker på enhetsnivå i anslutning till hantering av kunder med skyddade personuppgifter.
Har bolaget vidtagit ändamålsenliga åtgärder för att minska risken för röjning	Nej. Varken styrelse eller VD 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. Dessa

av skyddade personuppgifter och följs detta upp av berörda nämnder?	arbetsrutiner medför ett antal gynnsamma åtgärder, men det finns brister.
Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter? o *Hur tillvaratas erfarenhet från avvikelser?*	Nej. Bolaget har en dokumenterad process för hanteringen av personuppgiftsincidenter. 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. Se ovan.

Stockholm den 14 december 2023

David Leinsköld
Verksamhetsrevisor, EY

Bilaga 1 Källförteckning

Intervjuade funktioner

- VD
- Chef HR/Lön
- Chef kund och kommunikation/Sektionschef kundservice
- IT-chef
- Reskontraansvarig
- Säkerhetschef

Granskad dokumentation

- Bolagsordning för Umeå Vatten och Avfall Aktiebolag (KS-2013/01190)
- Bolagsordning för VAKIN – Vatten och avfallskompetens i Norr AB (KS-2015/00447)
- Arbets- och beslutsordning för Vatten- och avfallskompetens i norr AB (2022-12-09)
- Instruktion BFUS, Skyddad identitet – Utskick, upplägg, borttag (2023-08-07)
- Riktlinjer för informationssäkerhet (2022-10-06)
- Användarhandbok IT – Rutin för IT-hantering Vakin (2022-10-06)

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[4] intervjuas 86 kvinnor och 15 barn om deras erfarenheter där 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).

[4] *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[5] 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.

[5] 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 Umeå kommun gör över Vatten och avfallskompetens i Norr AB (Vakin).