Kommunrevisorerna granskar

Umeå Energi 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 Energi AB

Granskning av bolagets hantering av skyddade personuppgifter

Umeå kommun

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

Lekmannarevisorerna har gett det sakkunniga biträdet från EY i uppdrag att granska Umeå Energi AB:s hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur styrelse och VD för Umeå Energi 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.

Det pågår en översyn av de övergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen. Då dessa innehåller få skrivningar om hanteringen av skyddade personuppgifter, i kombination med att det inte finns ett beslutat övergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi det inte vara tillräckligt. Vi noterar att det har upprättats vissa verksamhetsnära rutinbeskrivningar för hanteringen av skyddade personuppgifter och tillhörande processer. Rutinbeskrivningar utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att de har utrymme för utveckling. Vi har också identifierat förbättringsområden i hanteringen av skyddade personuppgifter, däribland striktare behörighetsbegränsningar i IT-system och mindre manuell hantering.

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. Vi ser dock positivt på att det har påbörjats en översyn och genomlysning av bolagets informationssäkerhetsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet. I processen har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid.

Arbetsrutinerna introduceras vid nyanställning, och innan årsskiftet 2024 kommer hanteringen av skyddade personuppgifter ingå i bolagets utbildning om GDPR. Det är positivt och en förutsättning för att samtliga medarbetare ska vara införstådda i hanteringen av skyddade personuppgifter specifikt. 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. 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 Umeå Energi AB att:

- Upprätta 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 ändamålsenliga systemstöd för hanteringen 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. 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. Kommunalt ägda bolag 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 Umeå Energi 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 Umeå Energi 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 Energi AB.

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 Umeå Energi AB är personuppgiftsansvarig inom sitt verksamhetsområde

Umeå Energi AB (Umeå Energi) är ett av Umeå kommuns helägda bolag genom moderbolaget Umeå kommunföretag (UKF). Umeå energi är en samhällsaktör som i nära samarbete med andra utvecklar och möjliggör hållbara, tillgängliga och attraktiva energi- och kommunikationslösningar för regionen. Bolaget levererar nät för el och bredband, förnybar el från sol, vind och norrländsk vattenkraft samt fjärrvärme och -kyla.

Enligt bolagets arbetsordning[2] skall styrelsen i första hand äga sig åt övergripande och långsiktiga frågor samt frågor som är av osedvanlig beskaffenhet eller av stor betydelse för bolaget eller koncernen. Vidare ansvarar styrelsen att fortlöpande bedöma hur VD i bolaget respektive koncernens dotterbolag uppfyller sitt ansvar för den löpande förvaltningen. VD ansvarar för den löpande förvaltningen enligt de riktlinjer och anvisningar som styrelsen meddelar. VD eller den VD sätter i sitt ställe är föredragande i styrelsen. Styrelsen har att fatta beslut i alla frågor vilka inte faller inom den löpande förvaltningen samt i de frågor där aktiebolagslagen (2005:551) eller bolagsordningen kräver styrelsens beslut. Styrelsen ska fatta beslut i alla frågor som är av osedvanlig beskaffenhet eller av stor betydelse för bolaget eller koncernens dotterbolag.

Av bolagets delegationsordning[3] framgår att styrelsen ska besluta om att fastslå policys för Umeå Energikoncernen. Koncern VD beslutar om att fastställa säkerhetsorganisation, med vidaredelegerat ansvar till säkerhetschef. Det avser särskilt organisering av bland annat informationssäkerhet vari dataskydd och IT/OT-säkerhet[4] ingår, säkerhetsskydd samt incident- och krishantering. Beslut i löpande säkerhetsskyddsfrågor är delegerat från VD till säkerhetsskyddschef. På delegation från styrelsen ska koncern VD utse och förordna om Dataskyddsombud för respektive koncernbolag, varefter styrelsen ska informeras.

Personuppgiftsansvaret följer kommunkoncernens ansvarsfördelning; varje nämnd/styrelse är personuppgiftsansvarig för de personuppgifter som behandlas inom sitt verksamhetsområde. Det innebär att Umeå Energis 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. På bolagets intranät finns en intern arbetsrutin som riktar sig till bolagets samtliga medarbetare vid namn ”FAQ – Vem gör vad när det gäller skyddad identitet”. Den beskriver detaljerade sammanhang när bolagets medarbetare kommer i kontakt med kunder

[2] Fastställd av styrelsen 2023-02-23.

[3] Fastställd av styrelsen 2023-05-25.

[4] Operational Technology (OT) är ett begrepp som innefattar alla de delsystem som behövs för att styra och övervaka en fysisk process, exempelvis ett kraftverk eller en fabrik.

som har skyddade personuppgifter, och vem i form av en specifik person, de ska kontakta för vidare hantering.

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 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.

I Umeå Energi finns en säkerhetspolicy[5] som klargör att bolagets verksamhet är säkerhetskänslig, vilket ställer höga krav på bolagets säkerhetsarbete. Säkerhetsarbetet omfattar såväl lagstadgade krav på bland annat informationssäkerhet, dataskydd och säkerhetsskydd. Av policyn framgår att bolaget definierar säkerhetsarbetet som ett viktigt bidrag till affärs- och verksamhetsnyttan genom att vägledning av säkerhetsrisker bör ingå som en del i affärsmässiga beslut. Bolaget ämnar bibehålla en god kultur gällande säkerhetsarbetet bland annat genom att:

- Bedriva säkerhetsarbete systematiskt och proaktivt med ambitionen att ständigt bli bättre och öka medvetenheten och kompetensen i hela organisationen.
- Hantera säkerhetsarbete och säkerhetsrelaterade frågor så långt det är möjligt som en naturlig och integrerad del i allt verksamheten gör i sitt dagliga arbete.
- Arbete övergripande med riskhantering för att på så vis kunna identifiera relevanta säkerhetsbrister och förbättringsmöjligheter.
- Erbjuda riktade utbildningsinsatser för att säkerställa och utveckla kompetensen inom säkerhetsområdet.

Ett av fyra områden policyn omfattar är arbetet inom IT- och informationssäkerhet, cybersäkerhet och dataskydd. Av policyn framgår att bolaget skyddar informationstillgångar, kommunikationslösningar, IT/OT-infrastruktur samt IT/OT-lösningar från obehörig åtkomst, påverkan samt attacker och hot. Bolaget upprättar en hög cyberförmåga och säkerställer verksamhetsinformationens tillgänglighet, spårbarhet, autenticitet och konfidentialitet. Varje medarbetare och andra som arbetar inom bolagets verksamhet ansvarar för tillämpningen av säkerhetsarbetet inom det egna ansvars- och arbetsområdet. En ny säkerhetspolicy ska behandlas av styrelsen i december 2023.

Därutöver finns en IT-användarpolicy som beskrivs vara en del av bolagets informationssäkerhetsarbete. Policyn är dock föråldrad och inaktuell, varför den ska ersättas med nya riktlinjer inom ramen för pågående översyn av riktlinjer inom området. Enligt intervjuade kommer de riktlinjer som gäller för information med höga skyddskrav, däribland skyddade personuppgifter, vara markerade med fet stil i de nya riktlinjerna.

Inom ramen för pågående översyn av upprättade riktlinjer inom informationssäkerhetsområdet ska även nya riktlinjer för informationshantering upprättas. Intervjuade påpekar att information om detta dock redan finns på intranätet, liksom information om offentlighet och sekretess. Informationsförvaltning, det vill säga ett

[5] Fastställd av styrelsen 2022-11-24.

samlingsbegrepp för hantering av information som inkluderar allt från arkivering till processer för informationssäkerhet, ingår i bolagets kvalitetspolicy. En ny policy ska också den behandlas av styrelsen i december 2023.

Enligt uppgift är en målsättning i framtagandet av de nya riktlinjerna att säkerställa en säker hantering av skyddade personuppgifter samt tydliggöra struktur för uppföljning av det förbättrande arbetet.

Därutöver finns bolagets integritetspolicy tillgänglig på hemsidan. I den finns riktad information till bolagets kunder hur deras personuppgifter behandlas. Däribland finns information om hur en kund eller framtida kund med skyddade personuppgifter ska kontakta bolaget för att dess uppgifter ska hanteras säkert. Av informationen framgår bland annat att en kund med skyddade personuppgifter inte kan vara anonym och utföra en tjänst som kräver inloggning eller identifiering, exempelvis i tjänsten "Mina sidor". I stället ska kunden vända sig till bolagets kundservice för personlig service. Då bolaget har särskilda säkerhetsrutiner för hantering av skyddade personuppgifter är det därför viktigt att kunden alltid uppger att denne har skyddade personuppgifter vid kontakt med bolaget så att rutinerna följs. Om kunden vill lämna en synpunkt eller kontakta bolaget anonymt ska inga personliga uppgifter, i till exempel ett e-postmeddelande, finnas med eftersom bolaget registrerar uppgifterna och blir en offentlig handling.

I integritetspolicyn finns också information hur bolaget hanterar personuppgifter vid rekrytering. Av informationen framgår att personer med skyddade personuppgifter inte ska använda bolagets rekryteringssystem för att ansöka om ett jobb, utan i stället kontakta en utpekad person. I övrigt saknas riktlinjer för hantering av skyddade personuppgifter i bolagets HR-processer.

Utöver det finns flera verksamhetsnära rutinbeskrivningar som beskriver den praktiska hanteringen av skyddade personuppgifter. Rutinbeskrivningarna har upprättats på en verksamhetsnära nivå genom ett behov utifrån identifierade brister i arbetssätt av de tjänstepersoner som kommer i kontakt med skyddade personuppgifter. De har inte upprättats utifrån genomförd riskanalys eller på uppdrag av styrelse eller VD. Dessa 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 VD har ett utökat ansvar enligt bolagets arbets- och delegationsordning och att frågans beskaffenhet är för verksamhetsnära.

Samtidigt uppger intervjuade att det finns ett behov, i samband med pågående översyn av styrdokument inom informationssäkerhetsområdet, att upprätta en övergripande riktlinje för att tydliggöra och styra arbetet med skyddade personuppgifter. Detta i kombination med verksamhetsnära rutiner/instruktioner som beskriver praktiska detaljer kring hanteringen av skyddade personuppgifter. En sådan övergripande riktlinje skulle fastställas av VD.

3.3 Det finns behov av ytterligare kompetensutveckling

Nya medarbetare inom avdelning kundservice introduceras alltid till bolagets arbetsrutiner gällande hantering av skyddade personuppgifter. Därutöver finns en obligatorisk GDPR-utbildning för samtliga anställda, där det från och med december 2023 finns ett avsnitt om hanteringen av skyddade personuppgifter. Det har inte funnits tidigare.

Det saknas dock 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 beskriver dels att arbetet med att sprida

rutinerna 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. Framför allt framhävs behovet av att stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn.

3.4 Bedömning

Vår bedömning är att det saknas ändamålsenliga styrande dokument för hantering av skyddade personuppgifter. Det pågår en översyn av de övergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen. Då dessa innehåller få skrivningar om hanteringen av skyddade personuppgifter, i kombination med att det inte finns ett beslutat övergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi det inte vara tillräckligt. Vi noterar att det har upprättats vissa verksamhetsnära rutinbeskrivningar för hanteringen av skyddade personuppgifter och tillhörande processer. Rutinbeskrivningar utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter och vår bedömning är att de har utrymme för utveckling. 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 riktlinje fastställd av styrelse eller VD.

Trots avsaknaden av övergripande styrdokument inom området bedömer vi avdelningarna 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 med tanke på dess osedvanliga beskaffenhet.

Arbetsrutinerna introduceras vid nyanställning, och innan årsskiftet 2024 kommer hanteringen av skyddade personuppgifter ingå i bolagets utbildning om GDPR. Vi bedömer att den kompetensutveckling som finns just nu inte är tillräcklig, men ser positivt på att skyddade personuppgifter ska inkluderas i bolagets utbildning om GDPR. I och med de identifierade utvecklingsområdena i styrdokument och rutinbeskrivningarna, bedömer vi dock att det vid granskningens tidpunkt 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. Det finns dock risker som tangerar frågor kopplade till hanteringen av skyddade personuppgifter. 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, uppger intervjuade.

Utifrån genomförd riskhantering identifierades tre aktiviteter i 2023 års internkontrollplan som även fanns med i 2022 års internkontrollplan, och som indirekt har bäring på granskningsområdet:

- Fortsätta arbetet med de styrande dokumenten – slutföra genomgång av befintliga dokument gällande koppling av riktlinjer till policys
- Ramverk för intern kontroll – utred och ta fram förslag i syfte att skapa struktur
- Riskhanteringsprocess – vidareutveckla riskvärdering av bolagets risker

Enligt intervjuade utgör områdena en del av den tidigare beskrivna pågående översyn av internkontrollprocessen som inkluderar organisation, styrning och uppföljning som pågått i tre till fyra år. Mycket har förbättrats sedan dess, men samtidigt kvarstår arbete. Exempelvis uttrycks bland intervjuade ett behov att skapa en tydligare spårbarhet mellan övergripande policys och arbetsnära rutiner inom informationssäkerhetsområdet.

Bland de intervjuade finns en samlad bild att risken för röjning av skyddade personuppgifter därutöver diskuteras internt inom de olika enheterna, och att riskanalyser genomförs kontinuerligt i det dagliga arbetet, dock inte inom ramen för internkontrollarbetet. 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. Därutöver ska kravställning alltid ske utifrån bedömning av informationens skyddsvärde vid anskaffning av nya IT-stöd; upphandling, hyra samt egen utveckling. Framtagandet av vissa rutinbeskrivningar har därutöver föregåtts av en informell risk- och väsentlighetsanalys. Det finns dock enligt intervjuade ett behov att hantera skyddade personuppgifter specifikt inom den formella internkontrollprocessen.

4.2 Bedömning

Vi ser positivt på att det har påbörjats en översyn och genomlysning av bolagets informationssäkerhetsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet. I processen har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid. Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har dock 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 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.

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

Allmänt gäller att skyddade personuppgifter ska hanteras mycket varsamt, i enlighet med särskild rutin, och av särskilt utsedda handläggare.

Sedan ett halvår tillbaka finns möjligheten att automatiskt få information att en kund har skyddade personuppgifter, exempelvis via uppdatering av adressuppgifter via statens person- och adressregister (SPAR) och via kreditupplysningsföretaget Creditsafe, som i sin tur uppdateras mot Skatteverkets uppgifter. Det sker en gång per vecka. Innan dess fick bolaget förlita sig på att kunden med skyddade personuppgifter själv hörde av sig och informerade, vilket ansågs vara en brist.

Bolaget använder flera IT-system som hanterar kunduppgifter. Kunder med skyddade personuppgifter tilldelas ett alias utan personnummer och adressuppgifter. De riktiga uppgifterna skrivs ut på papper, och hanteras manuellt på säker plats. Enligt intervjuade finns en brist i systemen eftersom det saknas tekniska möjligheter att begränsa behörigheten till kunder med skyddade personuppgifter. Med andra ord saknas möjligheten att tekniskt styra behörigheten till en viss handläggare. I stället har bolaget valt att utse ett begränsat antal handläggare som hanterar skyddade personuppgifter manuellt. En annan brist med systemet är att kundnummer, som även framgår hos de med skyddade personuppgifter, är kopplad till en tillhörande anläggning med en lägesadress. Enligt intervjuade finns andra system som kan begränsa även den informationen. Det kan därför, enligt intervjuade, finnas skäl att upphandla ett nytt kundinformationssystem, där bolaget som kravställare och upphandlare har möjlighet att ställa krav på en mer ändamålsenlig hantering av skyddade personuppgifter. Arbetet kommer initieras under 2024.

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. Loggarna kan komma att lämnas ut till myndigheter vid behov. Administratörer har rätt att övervaka användaren utan att meddela denne om det finns misstanke om brott eller policyöverträdelser. Loggning har dock inte skett med anledning av att upptäcka brister i hanteringen av skyddade personuppgifter. 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.

I och med att en kund med skyddade personuppgifter inte har möjlighet att använda "Mina sidor" sker kommunicering med en kund via telefon eller post. Post skickas med

rekommenderat brev via Skatteverkets förmedlingstjänst, däribland fakturor till vissa kunder. Intervjuade uppfattar det vara en brist då det innebär en ökad risk att de skyddade personuppgifterna röjs, exempelvis av Posten. I dagsläget finns inget annat alternativ tillgängligt.

För överföring av känslig information till extern part finns en upprättad rutin. Kundgruppen skyddade personuppgifter omfattas dock inte av denna rutin. Det finns ett system för krypterad e-post som används vid filöverföring av dokumentation innehållandes känslig information. Kommunikation via e-post ska aldrig tillämpas vid hantering av skyddade personuppgifter. 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 framställs dock som en risk, då det krävs mycket av den enskilda handläggaren, att undvika avslöja något. Vid ett flertal tillfällen har personer ringt och varit påstridiga att tillskansa sig uppgifter om andra kunder.

Som kommunalt bolag omfattas Umeå Energi 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 respektive avdelning 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. Alla sekretesskyddade uppgifter ska maskeras före utlämnandet.

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 respektive enhet 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.

Vi bedömer det finns risker att samtliga system inte har en funktion för sekretessmarkering, då det medför risker att hantera skyddade personuppgifter utanför systemet. Detta då manuell hantering av skyddade personuppgifter ställer höga krav på noggrannhet och riskmedvetenhet samt ökar risken för felhantering orsakad av den mänskliga faktorn.

Därutöver saknas möjligheten att tekniskt styra och begränsa behörigheten bland anställda på bolaget till kunder med skyddade personuppgifter. Vi bedömer det finns betydande risker att det inte finns strikta behörighetsbegränsningar till sekretessbelagda ärenden, både i och utanför systemen. Detta då vi bedömer det vara angeläget att minimera antalet personer som hanterar skyddade personuppgifter.

Umeå Energi har inte gjort loggkontroller för att upptäcka suspekta användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser kopplat till risken för röjning av skyddade personuppgifter. Vi bedömer att bolaget årligen bör genomföra systematisk anomalianalys av loggar – att avvikande beteendemönster i verksamhetssystemen uppmärksammas automatiskt och därefter analyseras – med anledning av risken för röjning av skyddade personuppgifter. Detta särskilt med anledning av att det saknas begränsad behörighetstilldelning.

Bolaget har därtill inte övervakat och granskat verksamhetssystem som hanterar skyddade personuppgifter för att upptäcka sårbarheter och brister, däribland genom så kallade penetrationstester. Penetrationstester kan användas på många sätt för att identifiera brister vid hantering av skyddade personuppgifter, däribland säkerheten i IT-systemen och de arbetsrutiner som finns beskrivna i respektive förvaltnings rutinbeskrivningar. Vi bedömer det vara angeläget att rutiner för penetrationstester implementeras.

6. Avvikelsehantering

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

Samtliga personuppgiftsincidenter rörande skyddade personuppgifter rapporteras enligt bolagets rutin för personuppgifts- eller säkerhetsincidenter. I dessa saknas dock information om hanteringen av skyddade personuppgifter. Det går inte heller att särmarkera personuppgiftsincidenter som rör hanteringen av skyddade personuppgifter vid en incidentrapportering, vilket försvårar uppföljningen. Intervjuade beskriver det som ett utvecklingsarbete att inkludera information om skyddade personuppgifter i en ny övergripande riktlinje för hanteringen av skyddade personuppgifter.

Ingen incident har rapporterats som rör bolagets hantering av skyddade personuppgifter. Allmänt rapporteras få personuppgiftsincidenter, vilket enligt intervjuade 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. Orsaken är dock inte utredd och fastställd. Samtidigt finns bland de intervjuade en tilltro till att en eventuell röjning eller incident kopplat till skyddade personuppgifter skulle anmälas och hanteras skyndsamt.

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. I bolaget finns en process för hanteringen av personuppgiftsincidenter samt informationssäkerhetsavvikelser och avvikelser avseende skyddade personuppgifter hanteras i dessa processer. Av upprättade riktlinjer och rutiner för personuppgiftsincidenter framgår inte någon särskild information om 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.

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 pågår en översyn av de övergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men styrelse och VD har inte beslutat om något styrande dokument för hantering av skyddade personuppgifter specifikt. Det har dock upprättats arbetsrutiner utifrån det egna upplevda behovet av de som hanterar skyddade personuppgifter. Dessa utgör ett värdefullt stöd i sammanhanget, men vi noterar att de endast delvis speglar det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter. Arbetsrutinerna introduceras vid nyanställning. I övrigt diskuteras skyddade personuppgifter i huvudsak på förekommen anledning, exempelvis vid avvikelse. I dessa sammanhang förankras, och vid behov, stärks arbetsrutinerna.
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 från styrelse eller VD. Det har dock påbörjats en översyn och genomlysning av bolagets informationssäkerhetsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Ja. Innan årsskiftet 2024 kommer hanteringen av skyddade personuppgifter ingå i bolagets utbildning om GDPR.
Har bolaget på ett ändamålsenligt sätt analyserat och bedömt risken för att skyddade personuppgifter röjs? o *Har den enskilda individens perspektiv beaktats?*	Nej. Inom ramen för genomlysningen av bolagets informationssäkerhetsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid. Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har dock 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 av skyddade personuppgifter och följs detta upp av berörda nämnder?	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 arbetsrutiner medför ett antal gynnsamma åtgärder, men det finns brister. I granskningen framgår potentiella förbättringsområden, där avsaknaden av ett ändamålsenligt systemstöd är en framträdande brist.
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
- Tf. HR-chef
- Chef kund och kommunikation
- Chef process och betalning
- Koordinator kund och fakturering
- Handläggare fakturering

Granskad dokumentation

- Bolagsordning Umeå Energi Aktiebolag (KF 2021-09-27)
- Arbetsordning för styrelsen i Umeå Energi AB (2023-02-23)
- Delegationsordning Umeå Energi AB (UE-2023-0057-140)
- VD-instruktion Umeå Energi AB (UE-2023-0164-130)
- Säkerhetspolicy (UE-2022-0856-130)
- Umeå Energi – Förslag till beslut Internkontrollplan 2023, Uppföljning av plan 2022
- Umeå Energi – Identifierade risker inför 2023, uppföljning av genomförda under 2022 (2023-01-26)
- Rutin vid begäran om utlämnande av allmän handling enligt offentlighetsprincipen
- Intern rutin vid hantering av kunder med Skyddade personuppgifter (”Skyddad identitet”)
- FAQ – Vem gör vad när det gäller skyddad identitet!

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[6] 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).

[6] *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[7] 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.

[7] 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 Umeå Energi AB.