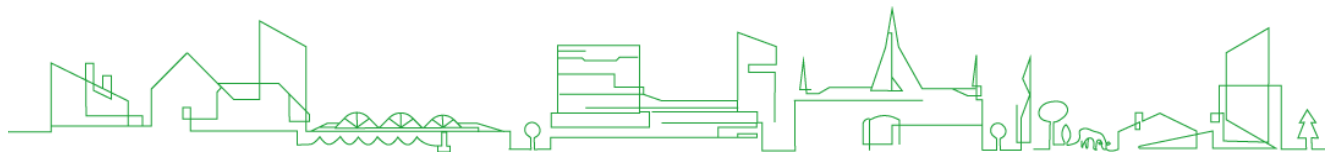


Kommunrevisionen granskar

Uppföljande granskning: Hantering av skyddade personuppgifter,
2025



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

Uppföljande granskning: Hantering av skyddade personuppgifter

Umeå kommun



The better the question. The better the answer.
The better the world works.



Shape the future
with confidence

Innehåll

Sammanfattning.....	2
1. Inledning.....	3
1.1. Bakgrund.....	3
1.2. Syfte och revisionsfrågor	3
1.3. Metod och avgränsning	3
1.4. Revisionskriterier	4
2. Granskningsresultat	5
2.1. Behandling av den tidigare granskningen	5
2.2. Åtgärder utifrån tidigare granskning.....	5
2.3. Åtgärderna i förhållande till rekommendationerna	8
3. Samlad bedömning	11
<i>Bilaga 1: Källförteckning</i>	<i>12</i>
<i>Bilaga 3: Umeå Vatten och Avfallskompetens i Norr AB: Granskning av bolagets hantering av skyddade personuppgifter</i>	<i>12</i>
<i>Bilaga 4: Umeå Energi AB: Granskning av bolagets hantering av skyddade personuppgifter</i>	<i>12</i>

Sammanfattning

Vår granskning visar också att bolagen har behandlat ärendet (revisionsrapporten) på ett sammanträde och att bolagsstyrelserna har gett förvaltningarna i uppdrag att åtgärda konstaterade brister. Åtgärderna har däremot inte följts upp och återrappporterats.

EY har på uppdrag av lekmannarevisorerna i Umeå Energi AB samt Umeå vatten och avfallskompetens AB genomfört en uppföljande granskning av kommunens hantering av skyddade personuppgifter. Lekmannarevisorerna granskade kommunens hantering av skyddade personuppgifter år 2023. Granskningen har utgått från tidigare revision och de rekommendationer som då lämnades. Syftet har varit att bedöma om bolagen har vidtagit ändamålsenliga åtgärder och om dessa åtgärder är tillräckliga för att säkerställa ett gott skydd av personuppgifter.

Vår sammanfattande bedömning är att Umeå Energi AB samt Umeå vatten och avfallskompetens AB **har** vidtagit ändamålsenliga åtgärder med utgångspunkt från revisionens tidigare granskning och rekommendationer.

Granskningen visar att båda bolagen har behandlat frågan om skyddade personuppgifter i sina styrelser och gett förvaltningarna i uppdrag att åtgärda identifierade brister. Åtgärder har vidtagits, men uppföljning och återrappportering till styrelserna har inte skett i tillräcklig utsträckning.

När det gäller de specifika rekommendationerna har bolagen bland annat:

- Tagit fram eller reviderat styrdokument och rutiner för hantering av skyddade personuppgifter.
- Inkluderat hanteringen av skyddade personuppgifter i utbildningsmaterial och genomfört årliga utbildningar i dataskydd och informationssäkerhet.
- Genomfört konsekvensbedömningar, bland annat enligt GDPR för att identifiera risker och vidta nödvändiga åtgärder.
- Säkerställt att avvikelser och incidenter som rör skyddade personuppgifter kan följas upp genom befintliga processer för personuppgiftsincidenter.

Samtidigt konstateras att vissa rekommendationer ännu inte är helt omhändertagna, exempelvis att området inte har inkluderats i internkontrollplanerna och att vissa riktlinjer ännu inte är formellt fastställda. För Vakin sker hanteringen av skyddade personuppgifter manuellt och i mycket begränsad omfattning.

För bedömningar kopplat till respektive revisionsfråga, samt de rekommendationer vi lämnar med anledning av resultatet av denna granskning, se avsnitt 3.

1. Inledning

1.1. Bakgrund

En viktig del i revisionsarbetet är att de rekommendationer som ges tas om hand av berörda bolag. Det innebär att de områden där revisionen ser behov av förbättring får uppmärksamhet och åtgärdas, så att verksamheten kan utvecklas på ett positivt sätt.

Kommunens revisorer granskade under år 2023 kommunens hantering av skyddade personuppgifter. Granskningen omfattade kommunstyrelsen, gymnasie- och vuxenutbildningsnämnden, för- och grundskolenämnden, individ- och familjenämnden, fritidsnämnden samt kulturnämnden. Den sammanfattande bedömning var att kommunstyrelsen och de granskade nämnderna inte på ett tillräckligt sätt säkerställt att skyddade personuppgifter inte röjs till obehöriga, samt att de tillämpade rutiner inte var ändamålsenliga. Granskningen omfattade även Umeå Energi AB samt Umeå vatten och avfallskompetens AB, där bedömningen blev den samma.

I revisionens tidigare granskningar riktades ett antal rekommendationer till kommunstyrelse, nämnder och bolagsstyrelser. Se tabellen i avsnitt 2.2 *Åtgärder utifrån tidigare granskning* för en sammanställning utifrån respektive granskningsobjekt i primärkommunen.

Med anledning av vikten av att skyddade personuppgifter hanteras på ett ändamålsenligt sätt samt iakttagelser och bedömningar från tidigare granskning har revisorerna beslutat att genomföra en uppföljande granskning.

1.2. Syfte och revisionsfrågor

Syftet med den uppföljande granskningen är att bedöma om Umeå Energi AB samt Umeå vatten och avfallskompetens AB har vidtagit ändamålsenliga åtgärder med utgångspunkt från revisionens tidigare granskning och rekommendationer.

Granskningen ska besvara följande *revisionsfrågor*:

- ▶ Har åtgärder vidtagits utifrån revisionens tidigare granskning?
- ▶ Har åtgärderna medfört att rekommendationerna har omhändertagits i tillräcklig utsträckning?

1.3. Metod och avgränsning

Granskningen omfattar Umeå Energi AB samt Umeå vatten och avfallskompetens AB (härefter Vakins). Granskningen avgränsas till att följa upp de rekommendationer som lämnats i granskningen. I granskningen ingår bland annat att kartlägga om:

- ▶ Berörda bolag har behandlat ärendet (revisionsrapporten) på ett sammanträde?

- ▶ Berörda bolag har gett förvaltningarna i uppdrag att åtgärda konstaterade brister?
- ▶ Åtgärderna har följts upp och återrapporterats till berörda bolag?

Uppföljningen har genomförts genom dokumentanalys och skriftliga frågor till respektive förvaltning.

Vi använder följande bedömningsskala för bedömning utifrån revisionsfrågorna:

1.4. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. I denna granskning utgörs revisionskriterierna av revisionskriterier och rekommendationer från tidigare granskning.

2. Granskningsresultat

2.1. Behandling av den tidigare granskningen

Utifrån protokollsgranskning kan vi konstatera följande gällande bolagens behandling av den tidigare granskningen:

Bolag	Behandling av tidigare granskning	Beslut i samband med behandling	Uppföljning av åtgärder i yttrande
Vakin	2024-03-15 § 4, pt. 4:6 (Vakin)	Styrelsen beslutade att godkänna yttrande enligt VD:s förslag.	Styrelsen i Vakin har enligt uppgift tagit del av en uppföljning av åtgärderna. Vi har ej mottagit underlag som styrker detta
Umeå Energi AB	2024-02-29 § 29 2024-03-21 § 44	Styrelsen tog emot granskningen som information (februari) och beslutade att VD ska återkomma med en handlingsplan vid mötet i mars. Handlingsplan presenteras i styrelse och styrelsen gav styrelseordförande och VD ansvar att besvara rapportens rekommendationer (mars).	Uppföljning av Umeå Energi handlingsplan avses presenteras för styrelsen efter denna granskning.

2.2. Åtgärder utifrån tidigare granskning

I revisionens tidigare granskning riktades ett antal rekommendationer. Se nedanstående tabell för en sammanställning:

Se nedanstående tabell för en sammanställning utifrån respektive granskat bolag:

Rekommendation	Riktad till
Upprätta risk- och konsekvensanalyser specifikt avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.	Umeå Energi AB, UMEVA/Vakin
Upprätta och anta ett styrdokument av övergripande karaktär för hanteringen av skyddade personuppgifter. Riktlinjen bör	Umeå Energi AB, UMEVA/Vakin

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.	Umeå Energi AB, UMEVA/Vakin
Säkerställa ändamålsenliga systemstöd för hanteringen av skyddade personuppgifter.	Umeå Energi AB
Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.	Umeå Energi AB, UMEVA/Vakin

I kommande avsnitt redogör vi i tabellform för vilka åtgärder respektive granskningsobjekt har vidtagit utifrån de lämnade rekommendationerna. I den högra kolumnen finns våra iakttagelser kopplat till respektive svar/åtgärd inom ramen för den uppföljande granskningen. I den högra kolumnen finns också iakttagelser kopplat till uppföljande frågor till respektive granskningsobjekt.

2.2.1. Vakin

Vakins kommentarer och åtgärder enligt yttrande	EY:s iakttagelser 2025
Bolaget hanterar ett fåtal skyddade personuppgifter och har därigenom inte sett ett behov av att införskaffa eller anpassa befintliga IT-stöd för att hantera denna typ av information. Hantering av skyddade personuppgifter sker manuellt på papper, med inlåsning för säkerhetsskydd med godkänt säkerhetsskåp, samt att tre personer har tillgång till uppgifterna. Dessa är utbildade i vad som gäller samt har tystnadsplikt. De bedömer att den manuella hanteringen är säker eftersom endast ett fåtal individer är involverade i den direkta hanteringen. Det framgår att anpassade datastöd medför att fler medarbetare kommer i kontakt med känslig information utöver de som har ansvar för hanteringen, samt att det medför en risk under nuvarande säkerhetsläge att IT-stöd utsätts för intrång och att känslig information röjs. Det	

framgår att den nuvarande hanteringen därmed är anpassad efter behov och inte står i strid med gällande lagstiftning i området.	
Bolaget avser att förtydliga personuppgiftshantering, inklusive skyddade personuppgifter, med ett eget kapitel i deras styrande dokument för informationssäkerhet och informationshantering.	Vi har erhållit reviderade riktlinjer (2025-10-21) för informationssäkerhet. Riktlinjen inkluderar behandling av skyddade personuppgifter. Det framgår inte om/när styrelsen fattade beslut om riktlinjen.
Bolaget ska uppdatera och fastställa en verksamhetsnära rutinbeskrivning för den praktiska hanteringen av skyddade personuppgifter.	Vi har erhållit en reviderad instruktion (2025-10-08) vilket beskriver hanteringen av kunder med skyddade personuppgifter.
Bolaget ska inkludera hanteringen av skyddade personuppgifter, likt övriga informationssäkerhetsfrågor, i internkontrollplaner.	Företrädare från Vakinn framhåller att bolaget inte har inkluderat hanteringen av skyddade personuppgifter i internkontrollplan för 2025, men att de implementerar ISO 27001 ¹ i verksamhetssystem under hösten 2025.
Bolaget ska säkerställa att de medarbetare som hanterar, eller kommer att hantera skyddade personuppgifter, inom ramen för sitt arbete får den kompetensutveckling som krävs för uppgiften.	Vi har i granskningen inte erhållit underlag som styrker att bolaget har säkerställt att medarbetare har fått kompetensutveckling i området.

2.2.2. Umeå Energi AB

Åtgärder enligt fastställd handlingsplan	EY:s iakttagelser 2025
En övergripande riktlinje ska tas fram och fastställas.	Enligt företrädare från Umeå Energi ska en riktlinje för hantering av skyddade personuppgifter, fastställas. Vi har erhållit ett utkast till riktlinje. Företrädare uppger att beslut om riktlinjen ska ske i december 2025.
En konsekvensbedömning ska genomföras för kund och HR-processer som ska resultera i en dokumenterad bedömning av riskerna samt vilka åtgärder som behövs för att minimera riskerna och på så vis ska uppfylla GDPR artikel 35.	Vi har erhållit underlag till konsekvensbedömning vilket innehåller en introduktion om det praktiska tillvägagångssättet samt mallar för personuppgiftsbehandling, kartläggningsinformationsflöde, konsekvensbedömning samt åtgärder.
Hantering av skyddade personuppgifter ingår i en utbildning som medarbetare ska genomföra gällande dataskydd och informationssäkerhet årligen.	Vi har erhållit underlag som styrker att hantering av skyddade personuppgifter ingår i utbildningsmaterial.

¹ ISO 27001 är en internationell standard för informationssäkerhet

Ändamålsenliga systemstöd för hanteringen av skyddade personuppgifter ska införas. Genom konsekvensbedömningen ska bolaget identifiera i vilka system det saknas stöd för hanteringen samt ta fram rekommendationer för att förbättra systemstödet.	Enligt företrädare från Umeå Energi, behandlas inte skyddade personuppgifter inte i systemstöd.
Bolaget ska säkerställa möjligheten till att systematiskt följa upp avvikelser gällande skyddade personuppgifter via processen för anmälan av personuppgiftsincidenter, och särskilt där skyddade personuppgifter förekommer.	Enligt företrädare från Umeå Energi, finns möjligheten att systematiskt följa upp avvikelser gällande skyddade personuppgifter via processen för anmälan av personuppgiftsincidenter där skyddade personuppgifter är en särskild kategori av registrerade.

2.2.3. Bedömning

Revisionsfråga: Har åtgärder vidtagits utifrån revisionens tidigare granskning?

Bedömning:

Vi bedömer att Umeå Energi och Vakin **har** vidtagit åtgärder utifrån revisionens tidigare granskning. Vi grundar vår bedömning på att bolaget har vidtagit ett antal åtgärder och på ett tydligt sätt motiverat orsaker till att åtgärder inte har vidtagits kopplat till vissa av de brister som identifierades i revisionens tidigare granskning.

2.3. Åtgärderna i förhållande till rekommendationerna

2.3.1. Iakttagelser

Rekommendation	Riktad till	EY:s kommentarer
Upprätta risk- och konsekvensanalyser specifikt avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.	Umeå Energi AB	Inget av bolagen har inkluderat området i internkontrollplaner. Rekommendationen bedöms som ej omhändertagen.
	Vakin	Inget av bolagen har inkluderat området i internkontrollplaner. Rekommendationen bedöms som ej omhändertagen.

Upprätta och anta ett styrdokument av övergripande karaktär för hanteringen av skyddade personuppgifter. Riktlinjen bör tydliggöras genom verksamhetsnära rutiner/instruktioner.	Umeå Energi AB,	Umeå Energi har vidtagit åtgärder genom att upprätta en riktlinje avseende hanteringen av skyddade personuppgifter, denna är däremot inte fastställd. Rekommendationen bedöms som omhändertagen.
	Vakin	Bolaget har förtydligat personuppgiftshanteringen, inklusive skyddade personuppgifter i en reviderad riktlinje för informationssäkerhet samt en rutinbeskrivning. Rekommendationen bedöms som omhändertagen.
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.	Umeå Energi AB	Skyddade personuppgifter ingår i en utbildning medarbetare ska genomföra gällande dataskydd och informationssäkerhet årligen. Vi har erhållit underlag som styrker att hanteringen av skyddade personuppgifter ingår i utbildningsmaterial. Rekommendationen bedöms därför som omhändertagen.
	Vakin	Utbildning i GDPR sker årligen genom digitala dataskyddsutbildningar. Utöver detta informeras kundservicemedarbetare i hanteringen enligt den bifogade instruktionen om de skulle få in uppgifter som behöver hanteras. Ovanstående har inte kunnat bekräftas genom underlag. Rekommendationen bedöms dock sammantaget som omhändertagen.
Säkerställa ändamålsenliga systemstöd för hanteringen av skyddade personuppgifter	Umeå Energi AB	Bolaget har analyserat befintliga systemstöd och konstaterat att inga personuppgifter hanteras i systemstöd.

		Rekommendationen bedöms därför som omhändertagen.
Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.	Umeå Energi AB,	Uppföljning av avvikelser gällande skyddade personuppgifter sker via processen för anmälan av personuppgiftsincidenter som är implementerad genom befintlig process. Rekommendationen bedöms som omhändertagen.
	Vakin	Vakin hanterar enligt intervjuade få skyddade personuppgifter och alla skyddade personuppgifter fysiskt och manuellt. Uppföljning av avvikelser bedöms därför kunna ske på förekommen anledning. Rekommendationen bedöms därför som ej tillämplig.

2.3.2. Bedömning

Revisionsfråga: Har åtgärderna medfört att rekommendationerna har omhändertagits i tillräcklig utsträckning?

Bedömning:

Vi bedömer att Umeå Energi AB och Vakin **har** vidtagit åtgärder som medfört att rekommendationerna har omhändertagits i tillräcklig utsträckning. Vi grundar vår bedömning på att bolaget har vidtagit ett antal åtgärder utifrån tidigare identifierade brister.

3. Samlad bedömning

Vår sammanfattande bedömning är att Umeå Energi AB samt Umeå vatten och avfallskompetens AB **har** vidtagit ändamålsenliga åtgärder med utgångspunkt från revisionens tidigare granskning och rekommendationer. Vår sammanfattande bedömning grundar sig på nedanstående:

Bolag	Har åtgärder vidtagits utifrån revisionens tidigare granskning?	Har åtgärderna medfört att rekommendationerna har omhändertagits i tillräcklig utsträckning?
Umeå Energi AB	Ja	Ja
VAKIN	Ja	Ja

Vi rekommenderar bolagsstyrelserna i Umeå Energi och Vakinn att:

- ▶ Besluta om riktlinjerna som behandlar skyddade personuppgifter
- ▶ Säkerställa att vidtagna åtgärder, bland annat de som vidtagits utifrån genomförda granskningar, återspeglar, återrapporteras
- ▶ Överväga att genomföra riskanalyser avseende hantering av skyddade personuppgifter

Umeå november 2025

Jonna Aimoson
Verksamhetsrevisor

Max Stenman
Certifierad kommunal yrkesrevisor

Johan Perols
Certifierad kommunal yrkesrevisor

Bilaga 1: Källförteckning

Dokument:

- ▶ Umeå Energi AB styrelseprotokoll 2024-02-29
- ▶ Umeå Energi AB styrelseprotokoll 2024-03-21
- ▶ Umeå Energi AB Handlingsplan - hantering skyddade personuppgifter
- ▶ Umeå Energi AB Konsekvensbedömning - hantering skyddade personuppgifter
- ▶ Umeå Energi AB - Riktlinjer hantering av skyddade personuppgifter [utkast]
- ▶ Vatten och Avfallskompetens i Norr AB (VAKIN) styrelseprotokoll 2024-04-15
 - ▶ Bildspel till styrelsemöte 2024-03-15
- ▶ VAKIN tjänsteskrivelse 2024-03-05
- ▶ VAKIN Riktlinjer för informationssäkert (reviderad 2025-10-21)
- ▶ VAKIN Riktlinje för informationshantering (reviderad 2024-08-27)
- ▶ VAKIN Instruktion skyddade personuppgifter (reviderad 2025-10-08)

Bilaga 3: Umeå Vatten och Avfallskompetens i Norr AB: Granskning av bolagets hantering av skyddade personuppgifter

Bilaga 4: Umeå Energi AB: Granskning av bolagets hantering av skyddade personuppgifter