Region Värmland

Region Värmlands revisorer

Granskning av regionens hantering av skyddade personuppgifter – uppföljning

Revisionsrapport nr 13 2025

Ansvarig verksamhet	Revisionskontoret
Kontakt	Emilia Nordin, emilia.nordin@regionvarmland.se tele; 010-831 42 66
Datum	2025-11-20
Diarienummer	Rev/25023
Region Värmland Regionens hus 651 82 Karlstad	

Innehållsförteckning

1. Inledning

Regionens revisorer har ansvar för att genomföra årlig granskning av regionens samtliga verksamheter. Utifrån detta uppdrag och ansvar har regionens revisorer utarbetat dokumentet ”Granskningsstrategi” i vilket de beskrivit de områden som revisorerna främst ska fokusera på under innevarande mandatperiod. Baserad på granskningsstrategin gör revisorerna en årlig riskbedömning och revisionsplan. I ”Revisionsplan 2025” ingår en uppföljning av granskningen av regionens hantering av skyddade personuppgifter från år 2022.

På uppdrag av regionens revisorer granskade EY år 2022 om styrelse och nämnder har säkerställt en tillräcklig intern styrning och kontroll vid hantering av skyddade personuppgifter, för att förhindra att dessa röjs för obehöriga. Granskningen omfattade Regionstyrelsen samt Hälso- och sjukvårdsnämnden, Kollektivtrafiknämnden, Kultur- och bildningsnämnden, Regionala utvecklingsnämnden och Patientnämnden.

Att skydda individer som riskerar att utsättas för brott, hot eller förföljelse och som därmed lever med skyddad identitet är en grundläggande samhällsuppgift. Inom flera av regionens verksamheter hanteras personuppgifter, även uppgifter om regionens egen personal. Det är av yttersta vikt att skyddade personuppgifter hanteras korrekt för att förhindra att dessa röjs, vilket kan medföra allvarliga konsekvenser för den enskilde individen. Felaktig hantering av skyddade personuppgifter kan även medföra ekonomiska påföljder för regionen, såsom skadestånd eller sanktionsavgifter.

Enligt 6 kap. 1 § i Kommunallagen (KL) är det Regionstyrelsens ansvar att leda och samordna förvaltningen av regionens angelägenheter samt att ha uppsikt över de övriga nämndernas verksamhet. Styrelsen ska även följa och beakta de frågor som kan påverka regionens utveckling och ekonomiska ställning, enligt 6 kap. 11 § KL. Vidare, enligt 6 kap. 6 § KL, ansvarar varje nämnd för att verksamheten inom sitt ansvarsområde bedrivs i enlighet med de mål och riktlinjer som fastställts av Regionfullmäktige. Nämnderna ska dessutom säkerställa att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett tillfredsställande sätt.

1.1 Syfte och frågeställningar

Syftet är att följa upp granskningen av regionens hantering av skyddade personuppgifter som genomfördes år 2022.

Den övergripande revisionsfrågan är om och hur Regionstyrelsen och berörda nämnder, vidtagit åtgärder inom de områden som lyftes fram i rekommendationerna i den tidigare granskningsrapporten från 2022

1.2 Avgränsning

Granskningen avser Regionstyrelsen, Hälso- och sjukvårdsnämnden, Kollektivtrafiknämnden, Kultur- och bildningsnämnden, Regionala utvecklingsnämnden samt Patientnämnden.

Granskningen ska ligga till grund för ansvarsprövningen 2025.

1.3 Revisionskriterier

- Folkbokföringslagen (1991:481)
- Offentlighets- och sekretesslagen (2009:400)
- Dataskyddsförordningen (2018:218)
- Patientdatalag (2008:355)
- Skatteverkets vägledning för hantering av skyddade personuppgifter i svensk förvaltning.
- Region Värmlands riktlinjer för skyddade personuppgifter

Granskningen ska även utgå från övriga beslut, interna styrdokument, lagstiftning och föreskrifter som bedöms vara relevanta.

1.4 Ansvarig nämnd

De nämnder som avses att granskas är alla dem vars verksamhet behandlar skyddade personuppgifter. Det gäller i första hand Regionstyrelsen, Hälso- och sjukvårdsnämnden, Kollektivtrafiknämnden, Kultur- och bildningsnämnden, Regionala utvecklingsnämnden samt Patientnämnden.

1.5 Metod

Granskningen har genomförts i form av dokumentstudier och intervjuer.

1.6 Bakgrund – Tidigare granskning från 2022

I samband med EY:s granskning år 2022 redovisades ett antal övergripande iakttagelser kopplade till regionen hantering av skyddade personuppgifter. Granskningen visade att styrelse och nämnder inte i tillräcklig utsträckning har säkerställt en effektiv intern styrning och kontroll inom detta område. Även om det finns riktlinjer, rutiner och anvisningar som överlag bedöms vara utförliga och innehålla nödvändiga beskrivningar, har konsulterna identifierat ett behov av mer verksamhetsspecifika och detaljerade instruktioner baserade på kända riskmoment. Vissa styrande dokument anses dessutom inte vara tillräckligt anpassade efter personalens faktiska behov av stöd i det dagliga arbetet.

Vidare har den tidigare granskningen visat på strukturella brister, bland annat att riktlinjer i flera fall fastställs av chefer istället för Regionstyrelsen eller berörda nämnder, vilket strider mot gällande beslut från Regionfullmäktige. På en mer övergripande nivå konstaterades även generella risker som påverkar hela organisationen, exempelvis bristande extern kommunikation med myndighet,

otillräckligt systemstöd, otydlig telefonkontakt med privatpersoner, bristande informationsspridning av styrande dokument, samt avsaknad av rutiner för hantering av medarbetare med skyddade personuppgifter.

Dessutom identifierades verksamhetsspecifika risker och en bristande medvetenhet hos personalen om korrekt hantering av skyddade personuppgifter. Konsulterna bedömer att dessa brister bör åtgärdas genom obligatoriska utbildningsinsatser och förbättrad intern kommunikation, eftersom den mänskliga faktorn utgör en betydande risk.

Vidare konstaterades att någon risk- och konsekvensanalys avseende hantering av skyddade personuppgifter inte har genomförts. Därmed har inte heller tillräckliga kontrollåtgärder införts, och det saknas systematisk uppföljning av avvikelser som rör detta område.

Mot bakgrund av dessa iakttagelser rekommenderas Regionstyrelsen samt berörda nämnder att vidta de åtgärder som framkom i den tidigare granskningen från 2022:

- Genomföra risk- och konsekvensanalyser och inkludera dessa i internkontrollplanerna.
- Säkerställa att riktlinjer fastställs av Regionstyrelsen och nämnderna, i enlighet med beslut från Regionfullmäktige.
- Införa obligatoriska utbildningar för all personal avseende hantering av skyddade personuppgifter och avvikelsehantering.
- Överväga införande av en särskild compliancefunktion för att följa upp efterlevnaden av riktlinjer och rutiner. Compliance handlar om att hålla sig på rätt sida av lagen och se till att allt från dataskydd till arbetsmiljö fungerar som det ska.
- Utföra tester av IT-system och rutiner för att identifiera eventuella sårbarheter.
- Införa systematiska loggkontroller för att motverka obehörig åtkomst till skyddade personuppgifter.
- Förbättra uppföljning och hantering av incidenter samt stärka rutinerna för avvikelsehantering.

2. Granskningens resultat

2.1 Har Regionstyrelsen och de berörda nämnderna vidtagit åtgärder inom de områden som lyftes fram i rekommendationerna i granskningsrapporten från 2022, och i så fall, vilka konkreta insatser har genomförts för att säkerställa förbättring inom dessa områden?

Nedan presenteras granskningens resultat utifrån respektive nämnds ansvarsområde.

2.2 Regionstyrelsen

Regionstyrelsen har vidtagit flera åtgärder för att möta de rekommendationer som lämnades i granskningsrapporten från 2022, främst inom områdena styrning, riskhantering och kompetensutveckling kopplat till hantering av skyddade personuppgifter.

I juni 2023 antog Regionstyrelsen riktlinjen *Skyddade personuppgifter*, som tydliggör ansvarsfördelning, rutiner och kompetenskrav inom området. Riktlinjen fastslår att säker hantering av skyddade personuppgifter förutsätter att berörd personal har god kunskap om gällande sekretessbestämmelser och förståelse för de skyddsåtgärder som sekretessmarkering och skyddad folkbokföring innebär.

Som en del av det fortlöpande informationssäkerhetsarbetet genomförs årliga risk- och konsekvensanalyser inom samtliga verksamhetsområden. Arbetet sker i samband med informationsklassning av den information som hanteras i regionens system och omfattar även personuppgifter och skyddade personuppgifter. Klassningarna utgör ett viktigt underlag för att identifiera skyddsbehov och fastställa lämpliga säkerhetsåtgärder. Resultaten följs upp i årsredovisningen genom indikatorer kopplade till effektmålet *Trygga och nöjda invånare* och resultatmålet *Tillgänglig och säkrad information*. Regionstyrelsen redovisar dessutom fördjupade uppföljningar inom säkerhet och beredskap, inklusive informationssäkerhet, två gånger per år.

Styrningen har stärkts genom att kansliavdelningen fått ett samlat ansvar för den strategiska hanteringen av skyddade personuppgifter. Avdelningen utvecklar riktlinjer, IT-stöd och utbildningsinsatser samt tillhandahåller juridisk rådgivning. En särskild kontaktperson och en jurist med personuppgiftsinriktning har utsetts. Någon formell compliancefunktion har dock ännu inte införts, vilket tidigare rekommenderats. I stället har behovet av informationssäkerhetssamordnare inom varje nämnd lyfts i regionens säkerhetsrapport 2025. Dessa funktioner bedöms bidra till ett mer systematiskt och lokalt förankrat arbete med informationssäkerhet och personuppgiftshantering.

Utbildningsinsatserna har utvecklats. För medarbetare inom hälso- och sjukvården finns obligatorisk utbildning i hantering av skyddade personuppgifter. En mer generell, icke sektorsspecifik utbildning har tagits fram och erbjuds sedan 2023. Utvärderingar visar positiva effekter, men spridningen inom organisationen behöver öka. Regionstyrelsen planerar därför mer uppsökande utbildningsinsatser, särskilt inom HR och telefonväxel, där behovet är störst. Utbildningarna har även bidragit till att brister i rutiner identifierats, bland annat i hanteringen av skyddade personuppgifter för regionens egna medarbetare och arbetssökande, vilket nu är föremål för särskild utveckling.

Avvikelsehantering sker genom det befintliga systemet AHA, där incidenter kring informationssäkerhet, inklusive personuppgifter och skyddade personuppgifter, rapporteras och följs upp. Ett utvecklingsarbete pågår för att införa en särskild kategori för skyddade personuppgifter i systemet, vilket möjliggör mer effektiv uppföljning och statistik. Utbildningsinsatserna omfattar även rutiner för rapportering av personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY).

Loggkontroller genomförs främst inom vårdens system, men även i andra system som innehåller skyddsvärda personuppgifter, såsom Platina och Heroma. Regionstyrelsen ser över rutinerna för årliga loggkontroller för att säkerställa en korrekt hantering i samtliga system.

Frågan om penetrationstester av IT-system har ännu inte hanterats på övergripande nivå. I nuläget ansvarar respektive systemägare för att säkerställa att systemen uppfyller gällande säkerhetskrav. Det pågående arbetet med informationsklassning förväntas på sikt ge ett bättre underlag för att avgöra i vilka system penetrationstester bör genomföras.

Sammanfattningsvis har Regionstyrelsen tagit flera steg för att stärka styrningen, riskhanteringen och kompetensen inom området skyddade personuppgifter. Arbetet är dock inte fullt ut genomfört, särskilt vad gäller etableringen av en samlad compliancefunktion och införandet av regelbundna penetrationstester. Den fortsatta utvecklingen av informationsklassning, utbildning och loggkontroller bedöms vara centrala delar i regionens förbättringsarbete.

2.3 Hälso- och sjukvårdsnämnden

Hälso- och sjukvårdsnämnden har under de senaste åren intensifierat arbetet med informationssäkerhet, särskilt inom risk- och konsekvensanalyser kopplade till hantering av personuppgifter och skyddade personuppgifter. Arbetet har i hög grad byggts upp kring regionens gemensamma process för informationsklassning, som omfattar all information inom verksamheten.

Informationsklassningen innebär att varje verksamhet bedömer konsekvenserna av bristande skydd för konfidentialitet, riktighet och tillgänglighet, och fastställer lämpliga skyddsåtgärder. Detta arbete har ökat medvetenheten om risker vid otillräckligt skydd och bidrar till framtagande av risk- och konsekvensanalyser samt åtgärdsplaner.

Klassningen följs upp som indikator i Regionstyrelsens interna ramfördelning under effektmålet *Trygga och nöjda invånare* och resultatmålet *Tillgänglig och säkrad information*. Dessutom genomför Hälso- och sjukvårdsnämnden årliga riskanalyser som utgör underlag för internkontrollplanen, där nya risker som identifieras genom informationsklassningen inkluderas.

Sedan nämnden antog riktlinjen *Skyddade personuppgifter inom hälso- och sjukvården (HSN 2024)* har arbetet intensifierats ytterligare. Riktlinjen syftar till att säkerställa en enhetlig och rättssäker hantering av skyddade personuppgifter inom Region Värmlands hälso- och sjukvård. Uppföljning och tillämpning sker genom informationsklassningen, via regionens avvikelsehanteringssystem AHA samt genom regelbundna dialoger mellan verksamheter, informationssäkerhetssamordnare, dataskyddsombud och personal i samband med utbildnings- och kompetensinsatser.

Ett utvecklingsområde som identifierats är behovet av att kunna särskilja avvikelser som specifikt rör skyddade personuppgifter i avvikelsesystemet, för att möjliggöra enklare uppföljning och trendanalys. En sådan förbättring bedöms kunna stärka det förebyggande arbetet.

Inom hälso- och sjukvården finns obligatoriska utbildningar i hantering av skyddade personuppgifter, kompletterade av mer generella utbildningar med ett övergripande perspektiv. Dessa utbildningar har lett till att brister i rutiner identifierats och hanterats, exempelvis inom hantering av skyddade personuppgifter för medarbetare och arbetssökande. En utvärdering visar dock att utbildningarna ännu inte når ut tillräckligt brett. Mer uppsökande insatser planeras därför, särskilt inom HR och telefonväxel.

Någon särskild compliancefunktion finns ännu inte, men behovet av informationssäkerhetssamordnare på nämndnivå lyfts i regionens säkerhetsrapport 2025. I större verksamheter kan flera samordnare bli aktuella för att stärka stödet inom informationsklassning, riskanalys, incidenthantering, upphandling och utbildning. På regionnivå finns en kontaktperson och en jurist med särskild inriktning mot personuppgifter som samordnar utbildning och rådgivning. Tillsammans med dataskyddsombud och informationssäkerhetssamordnare bedöms dessa funktioner kunna utveckla ett mer strategiskt arbete framöver.

När det gäller teknisk säkerhet ansvarar respektive systemägare för att systemen uppfyller krav på skyddsnivå och informationssäkerhet. De pågående informationsklassningarna kommer på sikt att ge ett bättre underlag för att avgöra vilka system som behöver penetrationstester. Samtliga IT-system som innehåller skyddsvärda personuppgifter omfattas av krav på loggkontroller.

För vårdsystemet *Cosmic* genomförs regelbundna loggranskningar av loggranskningsgruppen vid Utveckling och användarstöd patientjournal, för att säkerställa att endast behörig personal har åtkomst. Verksamhetschefen ansvarar för att loggkontroller och eventuella utredningar genomförs, med stöd av informationssäkerhetssamordnare och HR vid behov. Loggkontroller planeras även i

administrativa system som *Platina* och *Heroma*, där skyddade personuppgifter förekommer i begränsad omfattning.

Avvikelsehanteringen sker i det gemensamma systemet AHA, där diskussion pågår om att införa ”skyddade personuppgifter” som särskild kategori för att underlätta statistik och analys. Utbildningarna om skyddade personuppgifter inkluderar även moment om rapportering av incidenter till Integritetsskyddsmyndigheten (IMY).

Sammanfattningsvis har Hälso- och sjukvårdsnämnden tagit tydliga steg mot ett mer strukturerat arbetssätt för hantering av skyddade personuppgifter. Informationsklassningen har skapat förutsättningar för bättre skydd och riskhantering, men utvecklingsbehov kvarstår gällande uppföljning av incidenter, bredare utbildningsinsatser och införandet av tydliga informationssäkerhetsroller inom verksamheten.

2.4 Kollektivtrafiknämnden

Kollektivtrafiknämnden bedriver ett omfattande arbete med informationssäkerhet och hantering av personuppgifter, inklusive skyddade personuppgifter. Under de senaste åren har nämnden, i likhet med övriga delar av Region Värmland, påbörjat ett systematiskt arbete med informationsklassning av all information som hanteras inom verksamheten. Syftet är att bedöma skyddsbehovet för informationens konfidentialitet, riktighet och tillgänglighet samt att identifiera och analysera risker.

Informationsklassningen omfattar all information som kollektivtrafiken hanterar, även personuppgifter och skyddade personuppgifter och inkluderar risk- och konsekvensanalyser samt framtagande av åtgärdsplaner. Arbetet sker i samverkan mellan verksamheten, Region-IT och förvaltningsledare inom enheten Trafiknära teknik, där det även finns en särskilt utsedd person med ansvar för informationssäkerhetsutveckling.

I internkontrollplanen har nämnden under de senaste åren prioriterat olika risker kopplade till digitalisering. År 2023 låg särskilt fokus på hantering av personuppgifter, inklusive skyddade personuppgifter, medan de följande åren har haft tyngdpunkt på tillgänglighet och aktualitet i system. Eftersom personuppgifter endast hanteras i begränsad del av verksamheten, främst inom skoltrafik, färdtjänst, sjukresor och kundärenden, bedöms risknivån vara koncentrerad till vissa system och funktioner.

Arbetet med att identifiera, analysera och följa upp risker kopplade till skyddade personuppgifter sker dels genom den pågående informationsklassningen, dels genom regionens gemensamma avvikelsehanteringssystem. Incidenter som rör informationssäkerhet, inklusive personuppgifter, registreras och följs upp. Det finns dock önskemål om att avvikelser som rör skyddade personuppgifter ska kunna särskiljas tydligare i systemet för att möjliggöra bättre analys och uppföljning.

Kollektivtrafiken arbetar inom ramen för en förvaltningsmodell där frågor om informationssäkerhet, personuppgifter och systemhantering hanteras i ett

förvaltningsråd. Där sker samordning mellan enheten Trafiknära teknik och övriga delar av verksamheten. Säkerhetsarbetet omfattar tekniska och organisatoriska åtgärder såsom brandväggar, kryptering, behörighetsbegränsningar och utbildningar.

När det gäller utbildning finns ännu inga obligatoriska krav inom kollektivtrafikens verksamhetsområde. Däremot har regionen under de senaste åren tagit fram utbildningar som behandlar skyddade personuppgifter på ett mer generellt plan, utanför vårdverksamheten. Kollektivtrafiken planerar att, i samverkan med regionens utbildningsfunktion, anpassa utbildningsinsatser för de medarbetare som hanterar personuppgifter. Målsättningen är att alla relevanta grupper ska kunna genomföra digital utbildning under 2026, med hänsyn till verksamhetens drift dygnet runt.

Någon särskild compliancefunktion finns inte inom kollektivtrafiken, men verksamheten har ett etablerat samarbete med dataskyddsombud och informationssäkerhetssamordnare. I regionens säkerhetsrapport 2025 har behovet av särskilda informationssäkerhetssamordnare per nämnd lyfts som en utvecklingspunkt. En sådan funktion bedöms kunna stärka det strategiska arbetet kring informationssäkerhet, inklusive skyddade personuppgifter.

Avseende penetrationstester ansvarar respektive systemägare för att säkerställa att systemen uppfyller gällande krav på informationssäkerhet. Inom kollektivtrafiken har penetrationstester genomförts för systemet Triplex, som tidigare hanterade känsliga personuppgifter. Identifierade åtgärder har genomförts och erfarenheterna används vid implementeringen av det nya systemet We, som ersätter Triplex under 2025. Penetrationstester planeras även framöver för andra systemgrupper.

När det gäller loggkontroller följer kollektivtrafiken samma krav som övriga verksamheter inom Region Värmland – det vill säga att loggkontroller genomförs i system där skyddsvärda personuppgifter hanteras. Den pågående informationsklassningen ska tydliggöra vilka system som omfattas av krav på loggkontroll samt fastställa kontrollfrekvens. Endast ett fåtal medarbetare har tillgång till dessa system, vilket bidrar till ökad säkerhet.

Arbetet med avvikelsehantering följer regionens gemensamma rutiner. Kollektivtrafiken uppmuntrar aktivt medarbetare att rapportera alla typer av incidenter för att stärka lärande och förebyggande arbete. Det förs dialog om att införa en särskild kategori för skyddade personuppgifter i avvikelsesystemet AHA, vilket skulle underlätta uppföljning och analys av trender. I den digitala utbildningen om skyddade personuppgifter ingår även moment om rapportering av incidenter och personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY).

Sammanfattningsvis har Kollektivtrafiknämnden under de senaste åren utvecklat ett mer strukturerat arbete kring informationssäkerhet och personuppgiftshantering. Den pågående informationsklassningen kommer att ge ett tydligare underlag för riskbedömning och styrning framöver. Områden som fortsatt kräver utveckling är implementering av utbildningsinsatser, tydligare uppföljning av avvikelser samt förstärkt lokal funktion för informationssäkerhet.

2.5 Kultur- och bildningsnämnden

Kultur- och bildningsnämnden i Region Värmland har vidtagit flera åtgärder utifrån de utvecklingsområden som lyftes fram i revisionsrapporten från 2022. Revisorerna betonade särskilt behovet av tydligare risk- och konsekvensanalyser, en stärkt intern styrning och kontroll, utbildningsinsatser för personal samt utvecklade rutiner och uppföljningsmekanismer.

För att möta dessa rekommendationer har nämnden integrerat hantering av skyddade personuppgifter i sitt systematiska internkontrollarbete. I internkontrollplanen för 2023 identifierades risken *”Verksamhetens informationstillgångar ges inte ett tillräckligt skydd*”. Som åtgärd beslutades att regionens riktlinjer för skyddade personuppgifter skulle spridas till folkhögskolorna och att berörd personal skulle erbjudas utbildning, med uppföljning i tertialrapport 2. Detta har lett till en mer systematiserad riskhantering och stärkt kunskapen hos personalen.

I internkontrollrapporten för 2023 redovisades att de planerade kontrollmomenten hade genomförts och att rutinerna för informationssäkerhet hade stärkts. Även avvikelserapporteringen hade utvecklats, vilket förbättrade möjligheterna att följa upp risker kring skyddade personuppgifter.

Vidare har nämnden säkerställt en långsiktig inriktning genom att i internkontrollplanen för 2024 fortsatt prioritera riskerna kring informationssäkerhet som en central kontrollpunkt. Detta skapar förutsättningar för kontinuerlig uppföljning och förbättring av området.

Utbildningsinsatserna har utgjort en viktig del av åtgärdsarbetet. Personal som hanterar skyddade personuppgifter erbjuds återkommande utbildningar och information, och regionens riktlinjer har spridits till berörda delar av Kultur- och bildningsverksamheten för att säkerställa en enhetlig tillämpning.

Sammanfattningsvis har Kultur- och bildningsnämnden vidtagit flera konkreta åtgärder i enlighet med revisorernas rekommendationer. Genom att stärka riskhanteringen, utveckla utbildningsinsatser, förbättra rutiner och följa upp arbetet inom ramen för internkontrollplanerna 2023 och 2024, har nämnden omsatt identifierade förbättringsområden från 2022 i praktiska insatser. Arbetet är emellertid långsiktigt och kommer att behöva vidareutvecklas för att säkerställa en hållbar och säker hantering av skyddade personuppgifter över tid.

2.6 Regionala utvecklingsnämnden

Regionala utvecklingsnämnden har i sin verksamhet inte haft någon hantering av skyddade personuppgifter. Varken inom företagsstöd eller projektstöd har det inkommit ansökningar från aktörer med skyddade personuppgifter, och sannolikheten bedöms som låg att sådana ärenden uppkommer framöver. Trots detta finns rutiner

på plats för att säkerställa en korrekt hantering om sådana uppgifter skulle förekomma.

Verksamheten använder systemet NYPS[1], som tillhandahålls av Tillväxtverket och används både av företagsstöd och beredningen inom regional utveckling. Systemet är direkt kopplat till Skatteverkets register, vilket innebär att eventuella ärenden som innehåller skyddade personuppgifter automatiskt får skydd i systemet. Dessutom omfattas företagsstödsärenden av sekretess, vilket ytterligare säkerställer att känsliga uppgifter inte exponeras.

Risk- och konsekvensanalyser genomförs årligen i samband med framtagandet av internkontrollplanen. Arbetet följer COSO-modellen och omfattar en systematisk identifiering och värdering av risker. Eftersom skyddade personuppgifter aldrig hanterats inom verksamheten har detta inte bedömts utgöra en aktuell risk, och har därför inte inkluderats i internkontrollplanen. Om förutsättningarna skulle förändras finns rutiner på plats för att ompröva riskbedömningen och vid behov lyfta frågan i den ordinarie riskhanteringsprocessen.

När det gäller styrning och uppföljning av frågor kopplade till skyddade personuppgifter hänvisar nämnden till Regionstyrelsens övergripande riktlinje från juni 2023, Skyddade personuppgifter. Regional utveckling omfattas därmed av de regiongemensamma rutinerna för identifiering, analys och uppföljning av risker inom området. I enlighet med riktlinjen ansvarar kansliavdelningen under Regionstyrelsen för det strategiska arbetet, inklusive uppföljning, utbildning och juridiskt stöd.

Ingen särskild compliancefunktion finns inom Regionala utvecklingsnämnden, då denna fråga hanteras centralt på regionsnivå. Nämnden planerar dock att som ny rutin årligen gå igenom de rutiner som gäller för hantering av skyddade personuppgifter i NYPS-systemet, samt att se över behörigheter för de medarbetare som kan komma i kontakt med sådana uppgifter. Syftet är att säkerställa att rutiner och systemfunktioner fungerar som avsett och att eventuella manuella registreringar hanteras på ett korrekt sätt.

Någon obligatorisk utbildning i hantering av skyddade personuppgifter har ännu inte införts inom verksamheten, eftersom hantering av sådana uppgifter inte förekommer. Nämnden förhåller sig dock till Regionstyrelsens riktlinje och kan vid behov inkludera utbildningsmoment om området i framtida kompetensinsatser

Avseende penetrationstester och loggkontroller ansvarar Tillväxtverket som systemägare för NYPS för dessa säkerhetsåtgärder. Regionala utvecklingsnämnden har därmed inte något direkt ansvar eller möjlighet att genomföra egna tester i systemet, men följer de säkerhetsrutiner och krav som fastställs av systemägaren.

[1] Nyps är ett centralt ärendehanteringssystem som används av regioner, länsstyrelser och myndigheter i Sverige för att hantera och administrera regionalt utvecklingsstöd. Systemet har tagits fram och tillhandahålls av Tillväxtverket för att säkerställa att processerna följer nationella och EU-regler. Användare kan via Nyps söka medel, hantera ärenden, följa upp insatser och få tillgång till relevant statistik och analysverktyg

Inga avvikelser eller incidenter kopplade till hantering av skyddade personuppgifter har identifierats inom verksamheten. Eftersom sådana uppgifter hittills inte förekommit, har det inte funnits behov av särskilda rapporterings- eller uppföljningsåtgärder. Om skyddade personuppgifter skulle hanteras i framtiden finns dock systemstöd och sekretessrutiner som omedelbart skyddar uppgifterna och möjliggör avvikelsehantering vid behov.

Sammanfattningsvis bedöms Regionala utvecklingsnämnden ha tillräckliga rutiner och systemskydd för att kunna hantera skyddade personuppgifter om det skulle bli aktuellt, även om området idag inte utgör en praktisk fråga inom verksamheten.

2.7 Patientnämnden

Patientnämnden har utvecklat sitt arbete med hantering av skyddade personuppgifter i linje med Region Värmlands riktlinje Skyddade personuppgifter (antagen den 20 juni 2023). Nämnden har tagit fram en särskild rutin, *Skyddade personuppgifter* (RUT 23577), som reglerar hur ärenden som innehåller skyddade personuppgifter ska hanteras.

Inför framtagandet och vid varje revidering av rutinen har riskbedömningar genomförts för varje steg i ärendehanteringen, vilket utgör ett dokumenterat underlag till rutinen. Rutinen ses regelbundet över och uppdateras vid behov, i samverkan mellan enhetschef och systemstödsansvarig för det system som används, Platina. För att säkerställa korrekt hantering märks därför alla handlingar som innehåller skyddade personuppgifter med benämningen SKYDDAD. Märkningen möjliggör spårbarhet, säker hantering och underlättar vid gallring.

Patientnämndens ärenden omfattas av förstärkt sekretess och kan endast ses av ett begränsat antal personer inom patientnämndsenheten, systemstödenheten och registraturen. Vid gallring följer särskilda rutiner som innebär att känsliga uppgifter och originaldokument tas bort innan handlingar eventuellt överlämnas till Värmlandsarkiv.

Inför framtagandet av internkontrollplanen för 2026 kommer en särskild riskbedömning att genomföras gällande hantering av skyddade personuppgifter. Om risknivån bedöms som betydande kommer frågan att inkluderas i internkontrollplanen för uppföljning.

Arbetet med styrning och uppföljning av skyddade personuppgifter utgår från Regionstyrelsens riktlinje. Den lokala rutinen (RUT 23577) konkretiserar hur riktlinjen tillämpas inom patientnämndens verksamhet.

När det gäller utbildning finns för närvarande ingen obligatorisk utbildning för personalen i hantering av skyddade personuppgifter. Samtliga handläggare arbetar dock regelbundet med inkommande klagomålsärenden där sådana uppgifter kan förekomma, och enheten överväger att införa krav på genomgång av relevant utbildning framöver för att säkerställa enhetlig kunskapsnivå.

Patientnämnden har inte någon egen compliancefunktion, och kännedom om den regionövergripande funktionen har tidigare varit begränsad. Ansvar för uppföljning av en sådan funktion ligger i nuläget på Regionstyrelsen.

Frågor om penetrationstester och loggkontroller bedöms inte vara aktuella inom patientnämndens verksamhetsområde, eftersom dessa frågor hanteras på regionövergripande nivå

Avvikelsehantering sker enligt regionens gemensamma rutiner. Det finns ingen separat hantering för avvikelser kopplade specifikt till personuppgifter, utan sådana ärenden hanteras inom ramen för det ordinarie avvikelsesystemet.

Sammanfattningsvis har Patientnämnden stärkt sin hantering av skyddade personuppgifter genom att införa en dokumenterad rutin och genomföra riskbedömningar kopplade till ärendeprocessen. Arbetet präglas av hög sekretess och tydliga ansvarsgränser, men fortsatt utveckling bedöms nödvändig inom områden som utbildning och systematisk uppföljning av risker i internkontrollplanen.

3. Sammanfattande bedömning

Regionens revisorer har under 2025 följt upp den granskning som EY genomförde 2022 av hur Region Värmland hanterar skyddade personuppgifter. Syftet har varit att bedöma om Regionstyrelsen och berörda nämnder har vidtagit åtgärder utifrån de tidigare rekommendationerna, för att stärka intern styrning och kontroll samt säkerställa en trygg och korrekt hantering av skyddade personuppgifter.

Övergripande resultat
Sedan 2022 har regionen tagit flera viktiga steg för att förbättra hanteringen av skyddade personuppgifter, särskilt inom styrning, riskhantering och kompetensutveckling. En ny regionövergripande riktlinje, Skyddade personuppgifter (antagen 2023), reglerar ansvar, rutiner och kompetenskrav. Arbetet med informationsklassning och risk- och konsekvensanalyser har stärkts i samtliga verksamheter och utgör numera en del av regionens systematiska informationssäkerhetsarbete. Samtidigt kvarstår utvecklingsbehov, särskilt vad gäller utbildning, uppföljning och tekniska säkerhetsåtgärder.

Regionstyrelsen
Regionstyrelsen har förstärkt styrningen genom nya riktlinjer, utökade riskanalyser och årliga uppföljningar. En särskild kontaktperson och jurist har utsetts, men någon formell compliancefunktion saknas ännu. Obligatoriska utbildningar har införts, men deltagandet behöver breddas. Loggkontroller och incidenthantering har förbättrats, medan penetrationstester fortfarande hanteras på systemnivå.

Hälso- och sjukvårdsnämnden
Nämnden har infört en egen riktlinje (2024) och arbetar systematiskt med informationsklassning, riskanalyser och internkontroll. Utbildningsinsatser har prioriterats, och loggkontroller genomförs regelbundet i vårdsystemen. Utmaningar kvarstår i form av behov av fler informationssäkerhetsroller och förbättrad uppföljning av avvikelser.

Kollektivtrafiknämnden
Nämnden har utvecklat sitt informationssäkerhetsarbete genom risk- och konsekvensanalyser samt förvaltningssamverkan mellan teknik- och verksamhetssidan. Personuppgifter hanteras främst inom färdtjänst och sjukresor. Penetrationstester har genomförts för vissa system. Behov finns av stärkt uppföljning och lokal informationssäkerhetsfunktion.

Kultur- och bildningsnämnden
Nämnden har integrerat hanteringen av skyddade personuppgifter i internkontrollarbetet. Risker kopplade till informationssäkerhet har följts upp 2023–2024, och personalen har fått utbildning. Rutiner och avvikelsehantering har förbättrats, men arbetet behöver fortsatt utvecklas långsiktigt.

Regionala utvecklingsnämnden

Nämnden hanterar i nuläget inga skyddade personuppgifter. Systemet NYPS, som används för stödärenden, har inbyggt skydd kopplat till Skatteverkets register. Rutiner finns om behov skulle uppstå, men området är inte en aktiv risk. Nämnden planerar årliga genomgångar av behörigheter och rutiner.

Patientnämnden

Nämnden har infört en särskild rutin (RUT 23577) för hantering av skyddade personuppgifter, med märkning och strikt åtkomstbegränsning i systemet Platina. Riskbedömningar genomförs inför varje revidering. Utbildning är ännu inte obligatorisk men planeras införas. Uppföljning och systematisk riskhantering behöver stärkas framöver.

Samlad bedömning

Revisorernas samlade bedömning är att Region Värmland i huvudsak har vidtagit relevanta och ändamålsenliga åtgärder utifrån de rekommendationer som lämnades i granskningsrapporten 2022. Arbetet med styrning, riskhantering och kompetensutveckling har stärkts, särskilt genom införandet av den regionövergripande riktlinjen *Skyddade personuppgifter.* Vidare har det stärkts genom ett mer systematiskt arbete med informationsklassning, risk- och konsekvensanalyser och utbildningsinsatser.

Samtidigt kvarstår vissa utvecklingsbehov:

- Införandet av en samlad compliancefunktion.
- Breddad utbildning för samtliga berörda medarbetare.
- Förbättrad uppföljning av incidenter och avvikelser.
- Fortsatt utveckling av tekniska säkerhetsåtgärder, såsom penetrationstester.

Revisorerna bedömer sammanfattningsvis att Region Värmland har tagit tydliga och viktiga steg mot en mer enhetlig och säker hantering av skyddade personuppgifter. För att fullt ut säkerställa en långsiktigt hållbar intern styrning och kontroll inom området krävs dock att de identifierade utvecklingsbehoven prioriteras och följs upp i det fortsatta förbättringsarbetet.

Revisionsfråga	Bedömning
Har Regionstyrelsen och de berörda nämnderna vidtagit åtgärder inom de områden som lyftes fram i rekommendationerna i granskningsrapporten från 2022, och i så fall, vilka konkreta insatser har genomförts för att säkerställa förbättring inom dessa områden?	Samtliga nämnder har vidtagit åtgärder utifrån rekommendationerna i 2022 års granskning. Regionstyrelsen och Hälso- och sjukvårdsnämnden har i allt väsentligt genomfört förbättringar genom nya riktlinjer, riskhantering och utbildningsinsatser. Kollektivtrafiknämnden, Kultur- och bildningsnämnden samt Patientnämnden har delvis genomfört åtgärder men behöver stärka uppföljning, utbildning och lokala informationssäkerhetsfunktioner. Enligt uppgift hanterar Regionala utvecklingsnämnden i nuläget inga skyddade personuppgifter, men har rutiner för korrekt hantering vid behov. Sammantaget har arbetet utvecklats i rätt riktning, men fortsatt fokus krävs på uppföljning, ansvarsfördelning och kompetensspridning inom informationssäkerhet.

4. Källor

- Reglemente för samtliga nämnder.
- Regionstyrelsens riktlinje *Skyddade personuppgifter* (antagen juni 2023).
- Regionens säkerhetsrapport 2025.
- Regionens avvikelsehanteringssystem (AHA).
- Årsredovisning för samtliga nämnder.
- Patientnämndens rutin RUT 23577 – Skyddade personuppgifter
- Tidigare revisionsrapport från 2022.

5. Bilaga

Som underlag för informationsinhämtningen har ett frågeformulär skickats till samtliga nämnder. Svaren har inkommit från respektive nämnds ansvariga tjänsteperson.

1. Risk- och konsekvensanalyser

- Hur har nämnden säkerställt att risk- och konsekvensanalyser för skyddade personuppgifter nu genomförs systematiskt och dokumenterat?
- Kan ni ge exempel på hur risker lyfts in i internkontrollplanen?

2. Styrande dokument

- 20 juni 2023 antog Regionstyrelsen riktlinjen Skyddade personuppgifter. På vilket sätt arbetar ni idag med att identifiera, analysera och följa upp risker kopplade till skyddade personuppgifter?

3. Obligatoriska utbildningar

- Vilka grupper omfattas idag av obligatorisk utbildning i hantering av skyddade personuppgifter, och hur följer ni upp att de genomförs?

4. Compliancefunktion

- Hur fungerar den funktion som utsetts för att följa upp hanteringen av skyddade personuppgifter, och överväger ni att utveckla den vidare?

5. Penetrationstester

- Har ni genomfört eller planerat penetrationstester av era system sedan granskningen, och hur har resultaten i så fall använts?

6. Loggkontroller

- Utöver vårdens system, vilka andra system har prioriterats för loggkontroller, och hur ofta genomförs dessa?

7. Avvikelsehantering

Hur har ni arbetat för att stärka rapportering och uppföljning av avvikelser som rör skyddade personuppgifter.

Revisionen är ett demokratiskt kontrollinstrument som på uppdrag av fullmäktige ska granska styrelsens och nämndernas verksamhet samt presentera en revisionsberättelse. I Kommunallagen fastslås att revisorerna bland annat ska granska:

- Om verksamheten sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt.

- Om räkenskaperna är rättvisande, samt

- Om nämndernas interna kontroll är tillräcklig.

Vidare genomför revisorerna fördjupade granskningar inom områden där det finns betydande risker som kan medföra allvarliga konsekvenser.

Region Värmlands revisorsgrupp består av sju revisorer som utses av Regionfullmäktige. Revisionen biträds av sakkunniga vid regionens egna revisionskontor samt av upphandlade revisionsbyråer.

Information om revisionen och revisionsrapporter hittar du här: Revision - Region Värmland (regionvarmland.se)

Region Värmland