Handläggare
Lotta Carlborg

Datum
2022-12-13

Diarienummer
RUN/220243

Ert Datum
2022-06-15

Er beteckning
Rev/22002

Revisorerna

Svar på revisionsrapport gällande hantering av skyddade personuppgifter

Regionala utvecklingsnämnden vill avge följande svar på rubricerad revisionsrapport.

Revisorerna bedömer sammanfattningsvis att regionstyrelsen och granskade nämnder inte i tillräcklig omfattning säkerställt intern styrning och kontroll vid hantering av skyddade personuppgifter. Även om det finns ett antal styrande dokument som i huvudsak bedöms utförliga, behövs utförligare, regionövergripande och verksamhetsspecifika beskrivningar baserade på inventerade riskmoment. Riktlinjerna bör enligt revisorerna vara fastställda av regionstyrelse och nämnder – inte som idag av chefsfunktioner.

Det finns enligt revisorerna risker av allmän karaktär som gäller hela Region Värmland, exempelvis extern kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelsehanteringen, brister i informationsspridning av styrande dokument till medarbetare samt rutiner för hantering av medarbetare med skyddade personuppgifter. Vidare finns verksamhetsspecifika risker som är unika för varje situation.

Revisorerna uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas genom obligatoriska utbildningar, eftersom den mänskliga faktorn identifierats som en stor risk i sammanhanget.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförd risk- och konsekvensanalys. Regionstyrelsen och granskade nämnder har därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Avvikelser systematiseras och aggregeras inte för att åtgärda brister vid hantering av skyddade personuppgifter.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att, utifrån sitt ansvarsområde, tillse att det genomförs risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov lyfta in bedömda risker i internkontrollplanen.

Enligt Region Värmlands övergripande riktlinje för skyddade personuppgifter ska hälso- och sjukvården, kollektivtrafiken, kultur- och bildning, HR-avdelningen samt patientnämndens verksamhet göra en egen riskbedömning av de skyddade personuppgifter som behandlas; motsvarande gäller skyddade personuppgifter avseende förtroendevalda. Eftersom Regional utveckling enligt Region Värmlands övergripande riktlinje inte bedömts vara i behov av en egen riskbedömning, har en sådan inte genomförts.

I samband med granskningen av regionala utvecklingsnämnden gjordes en utredning av hur skyddade personuppgifter hanteras inom Regional utveckling. Det hanteras väldigt få personuppgifter inom verksamheten eftersom det sällan förekommer kontakt med enskilda personer. Däremot är kontakter med organisationer och företag vanliga, även om personuppgifter är mycket ovanliga även i dessa fall. Av utredningen framkom att det inte fanns någon erfarenhet alls av situationer inom verksamheten där det förekommit skyddade personuppgifter. Kunskapen om hantering av skyddade personuppgifter behöver dock stärkas inom verksamheten, om det någon gång skulle uppstå en situation där skyddade personuppgifter förekommer. Att göra en riskbedömning i samband med upprättande av interkontrollplan 2023 skulle kunna vara ett sätt att aktualisera frågan, men eftersom riskbedömningen görs utifrån en bedömning av *både* konsekvens och sannolikhet riskerar frågan om skyddade personuppgifter att nedprioriteras i interkontrollplanen på grund av extremt låg sannolikhet.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det genomförs en översyn av de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter i syfte att säkerställa att styrelse och nämnder fastställer riktlinjerna.

Regionstyrelsen ansvarar för strategiska frågor om informationssäkerhet samt för gemensam struktur och samordning av regionens ledningssystem. Mot bakgrund av detta bör regionstyrelsen ombesörja att de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter säkerställer att styrelse och nämnder fastställer riktlinjerna. Regionala utvecklingsnämnden har, med anledning av den obefintliga förekomsten av skyddade personuppgifter i verksamheten, inga nämndspecifika riktlinjer utan följer de regionövergripande riktlinjerna.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det genomförs obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelsehantering, erfarenhetsanalys och i praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.

Enligt Region Värmlands övergripande riktlinje för skyddade personuppgifter ska de medarbetare som hanterar sådana uppgifter årligen erbjudas internutbildning i dessa frågor. Kansliavdelningen ansvarar för utbildningen. Eftersom en säker hantering av skyddade personuppgifter kräver att medarbetarna har goda kunskaper om regelverket, bör utbildningen bli obligatorisk för personal som hanterar skyddade personuppgifter. Regionala utvecklingsnämnden anser att medarbetare inom Regional utveckling, som eventuellt skulle kunna komma i kontakt med skyddade personuppgifter, ska erbjudas denna utbildning för att höja kunskapsnivån inom verksamheten.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det övervägs att inrätta ”compliancefunktion/-er”, det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp. Detta för att hanteringen av skyddade personuppgifter ska vara prioriterat i regionens verksamheter.

Enligt Region Värmlands övergripande riktlinje för skyddade personuppgifter ska kansliavdelningen, som lyder under regionstyrelsen, utse en medarbetare med uppgift att följa upp att Region Värmland arbetar strategiskt med hantering av skyddade personuppgifter i enlighet med kraven i riktlinjen angående IT-stöd, utbildning och riktlinjer inom verksamheterna. Detta är en regionövergripande funktion som ombesörjs av regionstyrelsen, och således inte en fråga för regionala utvecklingsnämnden.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det genomförs penetrationstester av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång.

Det är regionstyrelsen som ansvarig nämnd för IT-frågor som ska överväga i vilken utsträckning penetrationstester av IT-system och rutiner bör genomföras, och är således inte en fråga för regionala utvecklingsnämnden.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det genomförs systematiska loggkontroller i samtliga systemstöd i syfte att säkerställa att obehöriga inte kan få tillgång till skyddade personuppgifter.

Systematiska loggkontroller kan inte säkerställa att obehöriga inte får tillgång till skyddade personuppgifter men bidrar till att sådana incidenter uppdagas och har också en avhållande effekt på personal som annars kan frestas ta del av personuppgifter utöver sin befogenhet. Inom hälso- och sjukvården finns lagkrav att vårdgivaren ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt patientuppgifter i systemen (4 kap. 3 § patientdatalagen). Regionstyrelsen

ska utreda vilka systemstöd som ska prioriteras för genomförande av sådana loggkontroller i övrigt, och regionala utvecklingsnämnden avvaktar denna utredning.

Revisorerna rekommenderar regionstyrelsen och granskade nämnder att tillse att det sker uppföljning av incidenter och avvikelser samt att avvikelsehanteringen avseende skyddade personuppgifter stärks.

Medarbetarna i verksamheten Regional utveckling ska få utbildning i hur avvikelser rapporteras på korrekt sätt i Region Värmlands system för avvikelsehantering. På grund av den hittills obefintliga förekomsten av skyddade personuppgifter i verksamheten är det dock inte troligt att underlåtenhet att göra avvikelserapportering är orsaken till att det inte rapporterats några incidenter från Regional utveckling.

Regionala utvecklingsnämnden

Stina Höök
Ordförande regionala utvecklingsnämnden

Eleonore Åkerlund
Regional utvecklingsdirektör