REVISORERNA
Handläggare
Marcus Olofsson

Direkttelefon
010-831 40 41

Datum
2022-06-15
Ert datum

Vår beteckning
Rev/22002
Er beteckning

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

Granskning gällande hantering av skyddade personuppgifter

Region Värmlands revisorer ansvarar för att genomföra årlig granskning av regionens samtliga verksamheter. Utifrån detta uppdrag och ansvar har revisorerna 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 2022” har revisorerna aktualiserat en granskning avseende hantering av skyddade personuppgifter.

Den nu aktuella uppföljande granskningen har genomförts av EY på uppdrag av regionens förtroendevalda revisorer. Syftet har varit att granska om styrelse och nämnder säkerställt en tillräcklig intern styrning och kontroll när det gäller hantering av skyddade personuppgifter så att dessa uppgifter inte riskerar att röjas för obehöriga.

I rapporten redovisar konsulterna bland annat följande sammanfattande iakttagelser:

” Sammantaget görs bedömningen att styrelse och nämnder inte i tillräcklig omfattning säkerställt intern styrning och kontroll. Det finns ett antal riktlinjer, rutiner och anvisningar för hanteringen av personer med skyddade personuppgifter, inklusive medarbetare. Dessa styrande dokument bedöms i huvudsak vara utförliga och omfattar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter. Det finns dock behov av utförligare regionövergripande och verksamhetsspecifika beskrivningar baserat på inventerade riskmoment. Vissa styrande dokument är utformade på ett sätt som inte motsvarar det stöd som personal efterfrågar. De riktlinjer som tillämpas bör enligt vår mening vara fastställda av Regionstyrelse och berörda nämnder, inte som idag av chefsfunktioner, eftersom det kan stå i strid med Regionfullmäktiges beslut om att riktlinjer endast i undantagsfall kan antas av chefer.

Det finns risker av allmän karaktär som gäller hela regionen, exempelvis extern kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelsehanteringen, brister i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare samt tydligare rutiner för hanteringen av medarbetare. Vidare finns verksamhetsspecifika risker som är unika för varje situation.

Vi uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas

Postadress
Region Värmland
Regionens hus
651 82 Karlstad

Besöksadress
Rosenborgsgatan 50

Telefon (växel)
010 831 5000
Telefax

E-postadress
marcus.olofsson@regionvarmland.se
Org.nr
232100-0156

genom obligatoriska utbildningar och informationsspridning då mänskliga faktorn identifierats som stor risk i hanteringen av skyddade personuppgifter.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförd risk- och konsekvensanalys. Regionstyrelsen eller 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 kopplat till hanteringen av skyddade personuppgifter."

Utifrån granskningens iakttagelser rekommenderar vi Regionstyrelsen och granskade nämnder, utifrån sina respektive uppdrag och ansvarsområden, att tillse att det:

- *Genomförs risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov lyfta in bedömda risker i internkontrollplanerna.*
- *Genomförs en översyn av de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter i syfte att säkerställa så Regionstyrelse och nämnder fastställer riktlinjerna.*
- *Genomförs obligatoriska utbildningar/informationsinsatser för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelsehantering, erfarenhetsanalys och i praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.*
- *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.*
- *Genomförs penetrationstester av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång.*
- *Genomförs systematiska loggkontroller i samtliga systemstöd i syfte att säkerställa att obehöriga inte kan få tillgång till skyddade personuppgifter.*
- *Sker uppföljning av incidenter och avvikelser samt att avvikelsehanteringen avseende skyddade personuppgifter stärks.*

Revisorerna översänder härmed rapporten och emotser Regionstyrelsens och berörda nämnders svar med redogörelse för vilka åtgärder styrelsen och nämnderna avser att vidta, senast den 16 november 2022.

Ingela Wretling
ordförande

Kristina Bengtsson Nilsson
vice ordförande