Fördjupad granskning nr 20/2023

Regionens hantering av skyddade personuppgifter

Mars 2024
David Leinsköld och Daniel Larsson, EY
Diarienummer: REV 59-2023

region västerbotten

Region Västerbotten

Granskning av regionens hantering av skyddade personuppgifter

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

EY har på uppdrag av revisorerna i Region Västerbotten genomfört en granskning av regionens hantering av skyddade personuppgifter. Granskningen har syftat till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig styrning och kontroll avseende hanteringen av skyddade personuppgifter så att dessa uppgifter inte riskerar att röjas till obehöriga. Vår samlade bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt detta.

Granskningens huvudsakliga iakttagelser är:

- Det finns inga politiskt beslutade styrdokument som är specifikt inriktade på hanteringen av skyddade personuppgifter. Politiskt beslutade styrdokument finns för informationssäkerhets- och dataskyddsarbetet. Dessa kan indirekt beröra hanteringen av skyddade personuppgifter, men området nämns inte uttryckligen i dessa styrdokument.

- Det finns på tjänstepersonsnivå en regionövergripande rutinbeskrivning för hanteringen av patienter med skyddade personuppgifter. Verksamheter som ingått i granskningen har i olika utsträckning beslutat om egna lokala rutinbeskrivningar inom området. De vi har tagit del av kan ytterligare utvecklas för att stärka hanteringen av skyddade personuppgifter.

- Det finns ingen regiongemensam utbildning för hanteringen av skyddade personuppgifter. De verksamheter som har ingått i granskningen har inte heller säkerställt att en tillräcklig kompetensutveckling inom området genomförs.

- Regionstyrelsen och hälso- och sjukvårdsnämnden har inte berört skyddade personuppgifter i sina internkontrollplaner, vare sig som kontrollmoment eller som bevakad risk.

- Det finns ingen egen process för avvikelser gällande skyddade personuppgifter och det genomförs ingen särskild uppföljning av avvikelser avseende skyddade personuppgifter. Det riskerar dels få allvarlig skada för patienten eller medarbetaren vars personuppgifter röjts, dels att erfarenheter från avvikelser inte tillvaratas.

- Regionstyrelsen och hälso- och sjukvårdsnämnden har inte genomfört några uppföljningar inom området.

Utifrån granskningens iakttagelser rekommenderas regionstyrelsen och hälso- och sjukvårdsnämnden att:

- Upprätta ett regionövergripande styrdokument som är specifikt inriktat på hanteringen av skyddade personuppgifter. Ett sådant styrdokument, exempelvis i form av en riktlinje, bör omfatta inriktningen för arbetet av både regionens vårdtagare och dess medarbetare på en strategisk nivå.

- Säkerställa att verksamheterna genomför risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.

- Säkerställa att verksamheterna utifrån ovanstående analys upprättar egna rutiner för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Säkerställ också att verksamheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.

- Säkerställa att verksamheterna genomför obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument och arbetsrutiner regelbundet.

- Säkerställa att verksamheterna genomför kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning 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 mer än fördubblats, från drygt 12 000 personer till knappt 27 000 personer. Den 1 januari 2019 trädde lagändringar i kraft med syfte att öka skyddet för hotade och förföljda personer.

Riksrevisionen konstaterar att regeringen inte har tagit tillräckliga initiativ för att motverka att skyddade personuppgifter röjs (RiR 2024:1). 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 personuppgifter röjts från myndigheter.

Personer med skyddade personuppgifter kan drabbas av mycket allvarliga risker och problem om regioners verksamheter inte har en ändamålsenlig kontroll över uppgifterna. Regioner måste därför ha tydliga rutiner, 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. Riksrevisionen bekräftar den bilden och konstaterar att röjningen bland annat beror på bristande kunskap om skyddade personuppgifter.

Mot bakgrund av detta har revisorerna beslutat att genomföra en fördjupad granskning av Region Västerbottens hantering av skyddade personuppgifter.

2.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig styrning och kontroll av hanteringen av skyddade personuppgifter så att dessa uppgifter inte riskerar att röjas till obehöriga.

I granskningen besvaras följande revisionsfrågor:

- Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt en god kontrollmiljö avseende risken för röjning av skyddade personuppgifter?
- Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att adekvata riskanalyser genomförts på rätt nivå för att minska riskerna för att skyddade personuppgifter röjs?
- Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att ändamålsenliga åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter?
- Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att information om regelverk, riskanalyser och kontroller sprids till medarbetare på ett ändamålsenligt sätt?
- Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?

2.3 Ansvariga nämnder och avgränsningar

Granskningen avser regionstyrelsen och hälso- och sjukvårdsnämnden med målgrupperna anställda och vårdtagare.

2.4 Metod och genomförande

Granskningen har skett genom dokumentstudier och intervjuer med ett urval av 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 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/bolagsstämmor. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning.

I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725) 6 kap. 1 § avseende styrelsens ledande funktion. 6 kap. 6 § om nämndernas ansvar för att bedriva verksamheten på ett ändamålsenligt sätt och med tillräcklig intern kontroll.
- Offentlighets- och sekretesslagen (2009:400).
- Folkbokföringslagen (1991:481).
- Folkbokföringsförordning (1991:749).
- SFS 2018:684 Lag om ändring i folkbokföringslagen (1991:481).
- COSO-modellen för intern kontroll.
- Fullmäktiges beslut och styrdokument inom granskningsområdet.

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, styrprinciper, integritet och etiska värderingar viktiga. Utöver organisationskultur består kontrollmiljön även av styrdokument. En ändamålsenlig kontrollmiljö är avgörande för att minska riskerna vid hantering av skyddade personuppgifter.

3.1 Det saknas ett regionövergripande styrdokument för hanteringen av skyddade personuppgifter

Regionstyrelsen och övriga nämnder är personuppgiftsansvariga inom respektive verksamhetsområde. Varken regionfullmäktige eller regionstyrelsen har beslutat om ett regionövergripande styrdokument som är specifikt inriktade på hantering av skyddade personuppgifter. Hälso- och sjukvårdsnämnden har inte heller beslutat om ett styrdokument specifikt inriktade på hanteringen av skyddade personuppgifter inom nämndens verksamheter.

Frågor som är relevanta för hanteringen av skyddade personuppgifter berörs i regionens informationssäkerhetsarbete. *Informationssäkerhet*[1] är en policy som omfattar Region Västerbottens samtliga ansvarsområden och syftar till att beskriva regionens gemensamma förhållningssätt för en trygg och säker informationsmiljö. Policyn beskriver övergripande regionens inriktning för informationssäkerhetsarbetet vilket samlas under rubrikerna:

- Ansvar och befogenheter är tydliga i vårt säkerhetsarbete.
- Vi förebygger kända risker och minimerar skador vid säkerhetshändelser.
- Informationssäkerhet är integrerat i all vår verksamhet.

Policyn innehåller ingen information om hanteringen av extra skyddsvärda personuppgifter så som skyddade personuppgifter.

Dokumenten *Struktur för dataskyddsarbete inom Region Västerbotten*[2] och *Informationssäkerhet – förvaltning och drift*[3] beskriver ansvarsfördelningen för regionens dataskydd- och informationssäkerhetsarbete. Hanteringen av skyddade personuppgifter överlappar delvis regionens dataskydd- och informationssäkerhetsarbete, varför denna ansvarsfördelning även har en viss relevans för hanteringen av skyddade personuppgifter. Exempelvis är verksamhetschefen informationsansvarig vilket även har relevans för skyddade personuppgifter.

Roll- och ansvarsfördelningen framgår av tabellen nedan:

[1] Fastställd av regionfullmäktige 2022-02-22 § 18. Giltig fr.o.m. 2022-05-09 t.o.m. 2024-05-09.

[2] Fastställd av regiondirektör. Giltigt fr.o.m. 2022-10-27 t.o.m. 2024-10-27.

[3] Fastställd av regionstyrelsen. Giltig fr.om. 2022-02-11 t.o.m. 2024-02-11.

Roll	Ansvar
Nämnderna i regionen, Personuppgiftsansvarig	Har det yttersta ansvaret för personuppgiftsbehandlingar på nämndens/styrelsens område. Detta innefattar att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med dataskyddsförordningen. Utser även dataskyddsombud. Regionstyrelsen ska därutöver även årligen säkerställa att en årsrapport om informationssäkerhet upprättas samt att det utifrån rapporten vidtas nödvändiga åtgärder.
Dataskyddsombud (DSO)	I Region Västerbotten finns ett dataskyddsombud för samtliga nämnder. DSO kontrollerar och ger råd. DSO rapporterar direkt till den högsta förvaltningsnivån i organisationen beträffande frågor som rör organisationens regelverksefterlevnad genom en årlig granskningsrapport. DSO leder Personuppgiftsnätverket för Personuppgiftshandläggare.
Informationssäkerhets-samordnare (CISO)	Bedriver ett långsiktigt och riskbaserat informationssäkerhetsarbete på en strategisk nivå. Samordnar Region Västerbottens gemensamma informationssäkerhetsarbete.
Regionens högsta ledning[4]	Arbetet med dataskydd och informationssäkerhet enligt styrdokumenten behöver vara tydligt förankrat i ledningen. Regionens ledning ska involvera DSO i frågor som påverkar dataskyddet i Regionen.
Verksamhetschef	Ansvarar för den information som hanteras i sin verksamhet. För information som hanteras i gemensamma IT-system har informationsägaren ansvaret genom att tillse att informationen som tillförs systemet uppfyller informationssäkerhetskraven. Utser en personuppgiftshandläggare för verksamheten. Ansvarar för att det finns rutiner för regelbunden granskning av verksamhetens informationssäkerhet. Rutinerna ska säkerställa att verksamheten uppfyller regionens krav.
Personuppgiftshandläggare	Ska fungera som verksamhetschefens ”*förlängda arm*” i dataskyddsfrågor och vara en tydlig kanal in till det DSO som är utsett på nämndens verksamhetsområde. Utöver att samråda med DSO i dataskyddsfrågor vid enheten ska personuppgiftshandläggaren även: ▸ Ta fram de rutiner som behövs vid enheten i dataskyddsfrågor ▸ Kontakta DSO i frågor som gäller dataskydd och laglighet i behandlingar ▸ Ingå i det närverk som DSO leder ▸ Utreda personuppgiftsincidenter som inträffar på enheten ▸ Bistå verksamheten i att registerförteckna personuppgiftsbehandlingar som verksamheten utför.
Medarbetare	Samtliga anställda inom regionen är informationsanvändare. Varje informationsanvändare ansvarar för att följa fastställda riktlinjer och rutiner samt att genast rapportera avvikelser, incidenter samt risker kopplade till informationssäkerhet och dataskydd.
Objektägare	Ansvarar för att registerförteckna systemet. Ansvarar för att systemet följer GDPR samt att de riskanalyser eller konsekvensbedömningar som behövs har genomförts. Ska också säkerställa att det finns rutiner för att hantera personuppgiftsincidenter gällande systemet.

Vidare beskriver dokumenten två nätverk inom området, nätverket för dataskydd- och informationssäkerhet och personuppgiftsnätverket.

[4] Syftar på regionens tjänstemannaledning.

Nätverket för dataskydd- och informationssäkerhet syftar till att i första hand utgöra en expertgrupp för dataskydd- och informationssäkerhetsfrågor och ska utgöras av representanter från åtminstone följande kompetenser:

- Dataskydd
- Juridik
- IT-säkerhet
- Informationssäkerhet
- Cybersäkerhet

Personuppgiftsnätverket utgörs av alla personuppgiftshandläggare och leds av DSO. Syftet är att utgöra ett forum för dataskyddsfrågor. Hanteringen av skyddade personuppgifter har inte berörts i nätverken men kan enligt intervjuade utgöra stöd om det skulle behövas.

Därutöver finns ett antal riktlinjer/rutiner som indirekt behandlar hanteringen av skyddade personuppgifter. Vi noterar återigen att skyddade personuppgifter inte behandlas specifikt i dokumentationen. Dessa sammanfattas kort nedan.

Riktlinjen *Digital Informationshantering*[5] omfattar hela Region Västerbotten och riktar sig till all personal som arbetar för Region Västerbotten vid hantering av digital information. Syftet med riktlinjen är att säkerställa att Region Västerbotten hanterar information på ett sätt som är lagligt, informationssäkert och som säkerställer bevarande av allmänna handlingar. Av riktlinjen framgår bland annat att känslig information om patienter, ekonomisk information och personalinformation enbart ska hanteras i de system som är avsedda för att hantera dessa uppgifter – exempelvis journalsystem, HR-system och ekonomisystem.

Tröskelanalys avseende dataskydd[6] är en rutinbeskrivning som riktar sig till alla som ska påbörja en ny personuppgiftsbehandling eller göra förändringar i en befintlig personuppgifts-behandling. Rutinbeskrivningen ger stöd för genomförande av tröskelanalys. Rutinbeskrivningen innehåller ett antal frågor som ska besvaras antingen ja eller nej i genomförande av en tröskelanalys.

Konsekvensbedömning avseende dataskydd[7] är en rutinbeskrivning som riktar sig till alla som ska påbörja en ny personuppgiftsbehandling eller göra förändringar i en befintlig personuppgiftsbehandling. Av rutinbeskrivningen framgår syftet med konsekvensbedömningar, ansvar och befogenheter inom området, vad en konsekvensbedömning ska innehålla samt vad en konsekvensbedömning ska resultera i.

Rutinbeskrivningen *Enskildas rättigheter enligt GDPR*[8] syftar till att ge vägledning i hur regionen ska hantera den enskildes rättigheter. Följande ansvar och befogenheter framgår av rutinbeskrivningen:

- Verksamhetschefen ansvarar för att skapa de rutiner som behövs i verksamheten för att säkerställa att den enskildes rättigheter enligt riktlinjen efterlevs.

[5] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2023-02-22 t.o.m. 2025-02-23.

[6] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2023-02-06 t.o.m. 2025-02-06.

[7] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2023-06-15 t.o.m. 2025-06-15.

[8] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2022-03-22 t.o.m. 2024-03-22.

- Varje medarbetare ansvarar för att ta emot den enskildes begäran om utövande av sina rättigheter.
- Regionjurist ansvarar för att fatta beslut om avslag på den enskildes rättigheter.
- DSO ansvarar för vägledning gällande den enskildes rättigheter.

Vidare beskrivs vilka rättigheter den enskilde har enligt dataskyddsförordningen som exempelvis rätten att få bli raderad.

Riktlinjen *Informationssäkerhet – Användare*[9] innehåller information om hanteringen av skyddade personuppgifter. Den riktar sig till alla personal i regionen och omfattar alla informationstillgångar. Syftet med riktlinjen är att säkerställa att regionens informationstillgångar skyddas så att:

- Endast behöriga personer får ta del av dem (konfidentialitet).
- Alltid finns när regionen behöver dem (tillgänglighet).
- Tillgångarna är korrekta, inte manipulerade eller förstörda (riktighet och spårbarhet).

Av riktlinjen framgår ett antal regler avseende informationssäkerhet. Alla försändelser ska sändas till patientens aktuella bokföringsdress och det ska finnas särskilda rutiner vid kontakt med patienter som har skyddade personuppgifter.

Regionen har ett antal ytterligare rutinbeskrivningar och riktlinjer för informationssäkerhet.

3.2 Skyddade personuppgifter ska hanteras utifrån särskilda rutiner

Som vi tidigare konstaterat finns inga politiskt beslutade styrande dokument i regionen som är specifikt inriktade på hanteringen av personer med skyddade personuppgifter. Rutinbeskrivningen *Vårdsystem – Patienter med skyddade personuppgifter, sekretesskydd*[10] är en övergripande rutinbeskrivning som riktar sig till all personal inom Region Västerbotten som kommer i kontakt med patienter med skyddade personuppgifter. Syftet är att uppnå hög patientsäkerhet och undvika att patientens skyddade personuppgifter röjs.

Av rutinbeskrivningen framgår bland annat information om personer med skyddade personuppgifter och hur dessa ska kontaktas genom Skatteverkets förmedlingstjänst. Därutöver framgår information om vilka uppgifter som ska föras in i vårdsystem samt ett särskilt tillvägagångssätt för personer som har skyddade personuppgifter och inte anser sig kunna besöka vården om de inte får vara totalt anonyma.

Rutinbeskrivningen utgör grunden för regionens hantering av personer med skyddade personuppgifter. Rutinbeskrivningen har inte upprättats utifrån genomförd riskanalys eller på uppdrag av regionstyrelsen eller hälso- och sjukvårdsnämnden. Vi noterar därtill att det saknas information om hur vårdtagare med skyddade personuppgifter ska kontakta regionen på hemsidan.

Enheten för Juridik och säkerhet samt relevanta objektsägare för en diskussion om att vidareutveckla den övergripande styrningen av hanteringen av skyddade personuppgifter. Det finns enligt intervjuade ett behov av tydligare regiongemensamma förhållningsätt avseende behörighetsstyrning, loggkontroller och

[9] Fastställd av regionstyrelsen. Giltig fr.o.m. 2022-02-11 t.o.m. 2024-02-11.

[10] Fastställd av CMIO medicinskt informationsansvarig överläkare, objektägare vårdsystem. Giltig fr.o.m. 2023-01-01 t.o.m. 2024-12-31.

andra liknande frågor. Det är inte beslutat vilket format en sådan styrning skulle ta – om den skulle beslutas av regionfullmäktige eller regionstyrelsen och vilken detaljnivå informationen i ett sådant styrdokument skulle ha. Den övergripande styrningen har inte förtydligats ytterligare.

Det övergripande stödet för hanteringen av informationssäkerhet och dataskydd hanteras av enheten Juridik och säkerhet inom regionstyrelsens förvaltning. Det involverar även stöd för hanteringen av skyddade personuppgifter. Verksamhetschefer ansvarar för hanteringen av skyddade personuppgifter inom sina respektive verksamheter i egenskap av informationsägare. Objektägare ansvarar för att systemstöden som används i respektive verksamhet har ett ändamålsenligt stöd för hanteringen av skyddade personuppgifter. Dataskyddsombudet stöttar verksamheterna avseende dataskyddsfrågor vilket kan inkludera hanteringen av skyddade personuppgifter. Därutöver har personuppgiftshandläggarna en roll i att stödja på lokal nivå i arbetet med hanteringen av skyddade personuppgifter.

Av den regiongemensamma rutinbeskrivningen framgår att verksamhetschef på respektive enhet är ansvarig för lokala rutiner i verksamheter. Regionens olika verksamheter har i många fall upprättat rutinbeskrivningar för hanteringen av skyddade personuppgifter. De innehåller verksamhetsspecifik information om hanteringen av patienter och medarbetare som har skyddade personuppgifter. De kan exempelvis bestå av detaljerad information om kommunicering med vårdtagare som har skyddade personuppgifter, hantering av skyddade personuppgifter i regionens journalsystem eller hur annan administration av skyddade personuppgifter ska hanteras. Vissa rutinbeskrivningar är mindre detaljerade.

Vi noterar att ingen av de rutinbeskrivningar vi har tagit del av har upprättats utifrån genomförd riskanalys eller på uppdrag av hälso- och sjukvårdsnämnden. Vi noterar också att vissa verksamheter inte har upprättat lokala rutiner. Intervjuade uppger i dessa fall att den regiongemensamma rutinen upplevs vara tillräcklig för hanteringen av skyddade personuppgifter.

3.3 Det finns behov av ytterligare kompetensutveckling

Regionen har inga interna utbildningar eller andra kompetenshöjande insatser som specifikt avser hanteringen av skyddade personuppgifter.

Av *Informationssäkerhet – förvaltning och drift*[11] framgår att all personal ska ha regelbunden utbildning i informationssäkerhet och i de informationssystem som de ska använda i sin tjänsteutövning. Av *Informationssäkerhet – Användare*[12] framgår att nyanställd i samband med anställning ska få kunskap om informationssäkerhet och sin roll i informationssäkerhetsarbetet. Nyanställda ska få utbildning i informationssäkerhet och i de informationssystem som de ska använda i sin tjänsteutövning.

Enheten för Juridik och säkerhet har genomfört utbildningar avseende informationssäkerhet. Det finns en regiongemensam grundutbildning inom informationssäkerhet samt en mikroutbildning avseende IT-säkerhet som är obligatorisk för alla medarbetare. Utbildningarna fokuserar på att stärka medarbetarnas säkerhetsmedvetenhet och påverka deras beteende. Skyddade personuppgifter har inte behandlats specifikt i dessa utbildningar.

Dataskyddsombudet har även genomfört utbildningar för personer med särskilt ansvar för personuppgifter samt personuppgiftshandläggare – dessa har dock inte specifikt avsett skyddade personuppgifter. Under

[11] Fastställt av regionstyrelsen. Giltig fr.o.m. 2022-02-11 t.o.m. 2024-02-11.

[12] Fastställt av regionstyrelsen. Giltig fr.o.m. 2022-02-11 t.o.m. 2024-02-11.

intervjuer lyfts att en regiongemensam och övergripande utbildning för hanteringen av skyddade personuppgifter skulle behöva vara allmänt hållen då många medarbetare inte behöver hantera skyddade personuppgifter i sin yrkesutövning. Intervjuade hänvisar också till den inbyggda medvetenheten av säker hantering av personuppgifter i allmänhet till följd av den starka sekretessen som finns bland regionens medarbetare då det minskar risken för röjning av skyddade personuppgifter.

Verksamhetschefer ansvarar för utbildningar avseende rutiner inom sina verksamheter och objektägare ansvarar för utbildningar avseende specifika systemstöd. Det är ovanligt med utbildningar som fokuserar på skyddade personuppgifter. Vissa verksamheter har utbildningar som specifikt avser skyddade personuppgifter med fokus på journalföring och det ingår i vissa utbildningar för nyanställda.

Förankringen av nya rutiner avseende skyddade personuppgifter såväl som andra områden sker till stor del i olika forum. Det finns exempelvis forum för verksamhetschefer och för objektsägare där eventuella nya rutiner avseende skyddade personuppgifter kan meddelas och förankras. Hanteringen av skyddade personuppgifter kan vid behov diskuteras på arbetsplatsträffar och i liknande forum. Detta beskrivs också som en central del av förankringen av nya rutiner. Rutiner för skyddade personuppgifter ingår dock inte i något årshjul inom de intervjuades olika verksamheter.

3.4 Bedömning

Vår bedömning är att det saknas ändamålsenliga styrande dokument för hantering av skyddade personuppgifter. Det finns regionövergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen, men då dessa saknar skrivningar om hanteringen av skyddade personuppgifter i kombination med att det inte finns ett beslutat regionövergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi det inte vara tillräckligt.

Det finns en regiongemensam rutinbeskrivning. Denna har inte beslutats politiskt och beskriver i huvudsak det praktiska tillvägagångssättet för hanteringen av vårdtagare med skyddade personuppgifter. Vi gör bedömningen att avsaknaden av ett styrande dokument som anger den övergripande inriktningen på arbetet med hanteringen av personer med skyddade personuppgifter 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 policy fastställd av regionfullmäktige eller som en riktlinje fastställd av regionstyrelsen.

Ansvaret för hanteringen av skyddade personuppgifter är till stor del decentraliserat. Verksamhetschefer ansvarar för att sina respektive verksamheter hanterar skyddade personuppgifter på ett tillräckligt sätt. Då området är verksamhetsnära bedömer vi att det är rimligt att verksamheterna i stor utsträckning utformar sina egna rutiner. Samtidigt finns det en risk att arbetet kan bli personberoende, särskilt med hänsyn till avsaknaden av regionövergripande styrande dokument. Vi noterar att vissa verksamheter inte har några egna rutinbeskrivningar för hanteringen av skyddade personuppgifter, utan endast utgår från den regiongemensamma rutinbeskrivningen. Verksamheternas egna rutinbeskrivningar har också ett varierande innehåll – vissa är relativt utförliga men andra är mycket begränsade. Vissa verksamheter har ett antal olika rutinbeskrivningar, vilket kan innebära en risk för förvirring och motsägelse.

Utöver rutinförankring genom interna diskussioner genomförs inte någon övergripande och systematisk kompetensutveckling specifikt för hanteringen av skyddade personuppgifter. Enheten för juridik och säkerhet har genomfört regionövergripande utbildningar inom informationssäkerhet men dessa omfattar inte skyddade personuppgifter. Även andra riktade utbildningar har genomförts, exempelvis har

dataskyddsombudet genomfört utbildningar om personuppgiftshantering för personuppgiftshandläggare men dessa har inte heller omfattat skyddare personuppgifter specifikt. Verksamheterna har inte heller genomfört några egna utbildningar som specifikt avser hanteringen av skyddade personuppgifter.

Baserat på den begränsade kompetensutvecklingen som finns och utvecklingsområdena i styrdokument och rutinbeskrivningarna bedömer vi att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt att information om regelverk, riskanalyser och kontroller sprids till medarbetare på ett ändamålsenligt sätt. 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. Vår bedömning är att det är väsentligt att samtliga medarbetare får åtminstone övergripande utbildningsinsatser med mer riktad kompetensutveckling för medarbetare som i större utsträckning hanterar skyddade personuppgifter.

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 internkontrollarbetet

Hanteringen av skyddade personuppgifter ingår inte som kontrollmoment i regionstyrelsens eller hälso- och sjukvårdsnämndens tillsynsplaner för internkontroll 2023 eller 2024. Området ingår inte heller som en bevakad risk i någon av tillsynsplanerna. Anledningen till detta är att riskerna för röjning av skyddade personuppgifter inte har bedömts vara tillräckligt sannolikt. Intervjuade menar att riskerna inom området framför allt avser specifika verksamheter och att riskerna därmed i huvudsak bör hanteras vid riskanalyser för enskilda objekt och verksamheter.

En övergripande riskanalys genomförs varje år för informationssäkerhetsarbetet kopplat till dataskyddsombudets tillsynsplan. Denna berör inte skyddade personuppgifter specifikt men intervjuade betonar att ett stärkt arbete inom informationssäkerhet och hantering av dataskyddsförordningen även gynnar hanteringen av skyddade personuppgifter. Dataskyddsombudets tillsynsplan beslutas dock inte av styrelse eller nämnder.

Verksamheterna har inte heller genomfört några riskanalyser kring hanteringen av skyddade personuppgifter. Rutiner har i många fall upprättats utifrån identifierade behov och inte utifrån genomförda riskanalyser. Intervjuade uppger dock att verksamheterna genomför informella eller mer riktade riskanalyser för det löpande arbetet. Detta kan exempelvis innefatta att perspektivet skyddade personuppgifter ingår i hanteringen av risker kopplat till utrop av patienters namn i väntrummet på psykiatrisk klinik.

4.2 Bedömning

Vi bedömer det vara en brist att regionstyrelsen och hälso- och sjukvårdsnämnden inte har analyserat risken för att skyddade personuppgifter röjs i internkontrollarbetet. Området ingår inte i regionstyrelsens eller hälso- och sjukvårdsnämndens tillsynsplaner för internkontroll för 2023 eller 2024. Vi noterar också att området inte heller ingår som en bevakad risk. Då konsekvenserna av att skyddade personuppgifter röjs kan vara mycket allvarliga, både för den drabbade och för regionen i stort, gör vi bedömningen att detta område löpande bör bevakas i regionstyrelsens och hälso- och sjukvårdsnämndens formella internkontrollarbete.

Verksamheterna genomför i olika sammanhang informella riskanalyser. Med hänsyn till de allvarliga konsekvenser som en röjning av skyddade personuppgifter kan få ser vi dock att hela processen kring hanteringen av skyddade personuppgifter åtminstone bör utvärderas i risk- och väsentlighetsanalysen. Detta kan också stärka regionstyrelsens och hälso- och sjukvårdsnämnden insyn och uppföljning inom området.

5. Kontrollaktiviteter – Rutiner och arbetssätt inom regionstyrelsens och hälso- och sjukvårdsnämndens verksamhetsområden

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 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 med skyddade personuppgifter. Gemensamt är att aktiviteterna syftar till att reducera risker.

5.1 Det pågår ett arbete med att informationsklassa regionens system

Rutinbeskrivningen *Anskaffning, utveckling och förändring av informationssystem*[13] vänder sig till anställda inom regionen som ska driva och genomföra ett utvecklings- eller förändringsarbete kopplat till informationssystem i projekt/uppdrag och objektorganisationer. Syftet med rutinbeskrivningen är att skapa en tydlighet och standardisering av utvecklings- och förändringsarbeten avseende informationssystem. Av rutinbeskrivningen framgår att:

- Objektägaren ansvarar för säkerheten i respektive systemstöd och att de skyddsåtgärder som behövs vidtas. Informationssäkerhetsklassning utgör stöd för detta.
- Informationsägare ansvarar för informationssäkerheten för information som informationsägaren är ägare för och att de berörda informationstillgångarna är informationssäkerhetsklassade.
- Behovsägaren ansvarar vid anskaffning av nytt informationssystem för att informationssäkerhetsklassning genomförs.
- Projektägaren ansvarar för att informationssäkerhet integreras i projektledningen för att säkerställa att informationssäkerhetsrisker som rör projektet och dess leveranser beaktas, bedöms och hanteras under projektets livscykel.

Vidare framgår anledningar till att informationssäkerhetsklassning är användbart, vad som ska klassas, samt när och hur klassning ska genomföras. Region Västerbotten använder verktyget KLASSA[14] för att genomföra informationssäkerhetsklassningar. Objektspecialist för KLASSA kan bidra med stöd och vägledning för informationssäkerhetsklassning.

Därutöver framgår av rutinbeskrivningen att införandet av nyanskaffat informationssystem, förändringar av informationssystem och utveckling av informationssystem ska planeras och föregås av riskanalyser av berörda informationstillgångar.
Miniriskmetoden[15] finns som stöd för riskanalysen. Informationssäkerhetssamordnare finns som stöd och vägledning kring informationssäkerhetsrisker.

[13] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2023-09-10 t.o.m. 2025-09-10

[14] För att förenkla kommuners och regioners genomförande av informationsklassningen har SKR tagit fram verktyget KLASSA. KLASSA består av tre delar: informationsklassning, handlingsplan och upphandlingskrav.

[15] Miniriskmetoden är en metod för att identifiera och prioritera risker inom projekt.

Arbetet med informationsklassning av regionens system pågår. Informationsklassning genomförs inför alla nyanskaffningar men vissa befintliga system har ännu inte informationsklassats. I samband med informationsklassning upprättas handlingsplaner där skyddade personuppgifter ingår som ett särskilt område. Enheten för juridik och säkerhet stöttar i arbetet med informationsklassning och objektägaren ansvarar för att den genomförs. Intervjuade uppger att informationsklassning när den är utförd också ska kunna användas som grund för exempelvis kravställning i nya upphandlingar.

Merparten av systemstöd som hanterar personuppgifter innehåller möjlighet till särmarkering. Det finns äldre system som inte gör det och i dessa hanteras inte skyddade personuppgifter.

5.2 Behandling av skyddade personuppgifter i regionens IT- och verksamhetssystem samt tillhörande processer

Grunden för hanteringen av skyddade personuppgifter i regionens system och tillhörande processer är den regiongemensamma rutinbeskrivningen (se avsnitt 3.2). Den innehåller information om exempelvis hantering av kontaktuppgifter, kontaktvägar, bokning och dokumentation. Intervjuade inom verksamheterna beskriver att rutinbeskrivningen till stora delar beskriver hur de arbetar avseende personer med skyddade personuppgifter. Detta medför att exempelvis journaler för personer med skyddade personuppgifter inte är behörighetsbegränsade men att kontaktuppgifter inte ska förvaras i journaler. Det finns en funktion i systemet som dagligen rensar journaler för personer med skyddade personuppgifter från eventuella kontaktuppgifter som har förts in. Vissa verksamheter för i stället pappersjournaler specifikt för patienter med skyddade personuppgifter. Dessa förvaras i låsta kassaskåp vilket ställer stora krav på en säker hantering.

Vissa intervjuade menar att en mer framträdande övergripande styrning, i form av exempelvis ett politiskt beslutat dokument, skulle vara gynnsamt för hanteringen av skyddade personuppgifter. Som exempel anges att det skulle ge tydligare instruktioner avseende om skyddade personuppgifter ska hanteras av ett fåtal eller om det är bättre att personer med skyddade personuppgifter hanteras i en ordinarie verksamheten med särskilda rutiner.

Av *Informationssäkerhet – Förvaltning och drift* framgår att systemägare ansvarar för rutin för loggkontroll. Av rutinen ska det framgå på vilket sätt och hur ofta loggarna ska granskas, vem som ska utföra granskningen, vad som är att betraktas som en överträdelse samt hur överträdelser ska hanteras. Det finns en regiongemensam rutinbeskrivning för loggkontroller *NCS Cross – Loggkontroller*[16] på regionens intranät. Rutinbeskrivningen beskriver tillvägagångsättet för att genomföra loggkontroller, samt hur granskningsresultat ska omhändertas. Av dokumentet framgår också att verksamhetschefer på respektive enhet ansvarar för att det finns lokala rutiner för loggkontroller och att dessa följs. Enligt dokumentet ska loggkontroller genomföras varje kalendermånad där ”ett antal” användare med läsbehörighet på vårdenheten slumpmässigt väljs ut. Närsjukvårdsområde Skellefteå har en rutinbeskrivning för loggkontroll *NCS cross Loggkontroll – lokal rutin*[17]. Loggkontroll sker varje månad och utförs av lokalt systemansvarig. Avdelningschef granskar loggkontrollerna. Loggkontrollerna genomförs inte specifikt avseende personer med skyddade personuppgifter utan görs utifrån ett slumpmässigt urval. Därutöver kan loggkontroller även komma att genomföras på förekommen anledning. Övriga verksamheter av de som ingått i granskningen har inte en specifik rutinbeskrivning för loggkontroller.

[16] Det framgår inte av dokumentet om det har fastställts och i sådana fall av vem. CMIO medicinskt informationsansvarig överläkare, objektägare vårdsystem står som dokumentansvarig. Giltigt fr.o.m. 2018-08-17 tills vidare.

[17] Fastställd av avdelningschef. Giltig fr.o.m. 2021-07-19 tills vidare.

Verksamheterna genomför i regel systematiska loggkontroller. Dessa genomförs i varierande former men vanligast förekommande är att en loggkontroll genomförs månatligen på ett slumpmässigt urval av loggar samt på förekommen anledning vid exempelvis misstanke om oegentligheter. Ingen verksamhet genomför loggkontroller specifikt avseende personer med skyddade personuppgifter.

I övrigt ger intervjuade en relativt enhällig bild av vilka rutiner, tillvägagångssätt och processer som gäller inom verksamheterna. Många arbetssätt härstammar från ett allmänt sekretessperspektiv och personuppgifter ska aldrig lämnas ut till utomstående oavsett om det rör skyddade personuppgifter eller ej. Arbetsrutinen är att motringa vid telefonkontakt med andra myndigheter. Åtgärder vidtas även i form av att bland annat undvika namn eller personuppgifter vid utrop i väntrum. Fax används i vissa verksamheter, särskilt i kontakt med exempelvis polisen och i vissa fall kommuner. Samtliga verksamheter som använder fax har som rutin att ringa för att bekräfta att faxat underlag mottagits och omhändertagits – men det finns en osäkerhet kring efterlevnaden av denna rutin. Samtliga verksamheter har rutinen att personuppgifter inte ska skickas med e-post men regionen har system som möjliggör krypterade mejl. Om personuppgifter behöver skickas till annan myndighet används i huvudsak telefon.

5.3 Hantering av skyddade personuppgifter i regionens HR-processer

Av *Informationssäkerhet – förvaltning och drift* framgår att vid rekrytering får endast sådana personuppgifter som är nödvändiga för rekryteringen behandlas. Det är möjligt att markera en person som anonym i systemstödet som används för rekrytering.

För hantering av anställda med skyddade personuppgifter finns *Rutin för hantering av anställda eller liknande med skyddade personuppgifter*[18]. Detta är en regiongemensam[19] rutin som gäller för alla regionens verksamheter och samtliga anställda, konsulter, studenter, förtroendevalda och övergripande uppdragstagare som verkar eller har verkat i regionens verksamheter. Av rutinen framgår att person med skyddad identitet ansvarar för att informera närmaste chef och uppvisa Skatteverkets beslut om skyddade personuppgifter samt ta ställning till om att vara synlig i HSA-katalog[20]. Detta innefattar både om en person med skyddade personuppgifter anställs och om en anställd får skyddade personuppgifter. Personens närmaste chef ansvarar för att informera personen med skyddad identitet om hur och i vilka system regionen hanterar personuppgifter samt informera HR-systemförvaltning och HSA-förvaltning via beställning i webfacit[21]. Vidare framgår bland att:

- Kretsen av personer som har behörighet att ta del av skyddade personuppgifter ska begränsas så mycket som möjligt.
- När en person fått skyddade personuppgifter döljs dennes uppgifter i HSA-katalogen. Vill personen ha sina uppgifter synliga i katalogen ska denne uttryckligen meddela det till HSA-förvaltningen.

[18] Dokumentet är inte daterat och det framgår inte vem som har beslutat om rutinen. I dokumentet hänvisas till Västerbottens Läns Landsting, vilket tyder på att dokumentet är upprättat innan 2019.

[19] I dokumentet kallat landstinget.

[20] Nationell katalog för hälso- och sjukvårdsaktörer.

[21] Webfacit har upphört och ersatts av serviceportalen, där motsvarande ärenden kan skapas.

Rutinen beskriver därutöver bland annat hur personer med skyddade personuppgifter ska hanteras i regionens HR-system. I rutinen uppges att namn loggas i samtliga vårdsystem och att om en patient begär loggutdrag måste regionen lämna logguppgifter där anställdas namn syns.
Rutinen *Hantering av person med Skyddad identitet HR system*[22] innehåller information om hanteringen av personer med skyddade personuppgifter i regionens HR-system Personec P.

Möjligheten att komma åt uppgifter om en anställd med skyddade personuppgifter i regionens HR-system är begränsad till den anställdes chef samt en begränsad mängd personer inom regionens HR-avdelning. Intervjuade uppger att en chef måste genomgå en utbildning om dess ansvar i personalfrågor för att få behörighet i HR-systemet. Denna utbildning inkluderar bland annat förhållningssätt kring anonymitetsfrågor.

Anställningsavtal hanteras på papper och förvaras inlåsta i kassaskåp. Ett begränsat antal medarbetare har tillgång till nycklarna. Alla personuppgifter undantaget personnummer tas bort från anställningsavtal med personer med skyddade personuppgifter.

Verksamhetschef beslutar i samråd med den anställde som har skyddade personuppgifter vilka rutiner som ska gälla för den anställde i det ordinarie arbetet. Det finns inga regiongemensamma regler eller beslutade förhållningssätt för detta.

5.4 Bedömning

Vår sammantagna bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt att ändamålsenliga åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter. Verksamhetscheferna har enligt regionens ansvarsfördelning ett stort ansvar för att de egna verksamheterna vidtar de åtgärder som krävs för att säkerställa en god hantering av skyddade personuppgifter. Risken för att skyddade personuppgifter avslöjas minskas genom olika arbetsrutiner i verksamheterna. Dessa har beslutats av verksamhetscheferna, inte av regionstyrelsen och hälso- och sjukvårdsnämnden. Vår bedömning är att det är positivt att verksamhetschefer har beslutat om rutinbeskrivningar och bidrar till att minska risken för röjning av skyddade personuppgifter men att detta inte är tillräckligt för att bedöma att regionstyrelsen och hälso- och sjukvårdsnämnden har säkerställt att åtgärder vidtagits. Avsaknaden av övergripande politisk styrning bedömer vi vara en stor brist i arbetet med hanteringen av skyddade personuppgifter.

Vi är positiva till att det finns loggkontroller, men gör bedömningen att rutinerna för dessa kan utvecklas. Vi noterar att det finns olika förhållningssätt till loggkontroller inom verksamheterna, vissa genomför loggkontroller mer frekvent än andra. Ingen verksamhet genomför loggkontroller som specifikt avser personer med skyddade personuppgifter – loggkontroller sker slumpmässigt månatligen samt på förekommen anledning. Vår bedömning är att, givet de möjliga konsekvenserna av att obehöriga tar del av uppgifter om personer med skyddade personuppgifter, regionstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa att verksamheterna genomför systematiska loggkontroller som specifikt avser personer med skyddade personuppgifter.

Vi ser vidare förbättringspotential avseende bland annat användning av fax. Vissa verksamheter måste använda fax på grund av krav från extern myndighet. I dessa fall gör vi bedömningen att det är väsentligt att telefonrutiner finns för att bekräfta att rätt personer har mottagit faxet. I övrigt gör vi bedömningen att

[22] Senast reviderad 2023-11-01. Rutinen följer inte samma mall som övriga rutiner i regionen.

användandet av fax bör minimeras. Vi gör bedömningen att regionen bör utforska möjligheten att nyttja säker och krypterad e-post om information om personer med skyddade personuppgifter behöver skickas snabbt och inte kan kommuniceras via telefon.

Vissa arbetsrutiner som har upprättats av verksamhetschefer är mycket sparsamma och täcker inte nödvändigtvis in alla relevanta risker och arbetssätt avseende personer med skyddade personuppgifter. Vår bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa att verksamheterna har ändamålsenliga arbetsrutiner, exempelvis genom att tydliggöra i politiskt beslutade övergripande styrande dokument hur verksamheterna ska förhålla sig till personer med skyddade personuppgifter.

Vi noterar att regionen har ett pågående arbete med att informationsklassa sina systemstöd. Vår bedömning är att detta bidrar till att stärka kontrollmiljön, även för hanteringen av skyddade personuppgifter. Vi bedömer att det är viktigt att detta arbete slutförs skyndsamt.

6. Uppföljning och kontroll

Övervakande aktiviteter har till ändamål att utvärdera och följa upp kontrollen i organisationen. Tillsynen bör ske kontinuerligt med kontroller och utvärdering. Tillsyn kan till exempel bestå av internrevision, självutvärdering, oberoende externa utredningar och genom att löpande föra statistik och aktiviteter till ändamål att utvärdera och följa upp kontrollen i organisationen och analysera den egna verksamheten.

6.1 Det görs inga egenkontroller av följsamhet till rutiner och regelverk

Många intervjuade beskriver att det är svårt att avgöra hur god efterlevnaden är kring rutiner för en säker hantering av personer med skyddade personuppgifter. Verksamheterna som har ingått i granskningen har inte genomfört en enkätundersökning eller liknande bland medarbetarna för att undersöka kunskapsnivån om hanteringen av skyddade personuppgifter, om de vet var arbetsrutinerna finns, om arbetsrutinerna saknar nödvändig information eller liknande. En enhet har till följd av att denna granskning skulle genomföras gjort en uppföljning bland medarbetarna. Resultatet visade att många medarbetare inte känner sig trygga i hanteringen av skyddade personuppgifter, däribland finns bristande kännedom om rutinen som finns i verksamheten.

I och med att skyddade personuppgifter inte har hanterats i regionstyrelsens eller hälso- och sjukvårdsnämndens internkontrollarbete sker ingen uppföljning till styrelsen och nämnden. Vi noterar att skyddade personuppgifter inte berörts i något protokoll under 2023 och intervjuade påtalar att styrelsen och nämnden inte ställt frågor om hanteringen av skyddade personuppgifter.

Dataskyddsombudets årsrapport 2022[23] innehåller uppföljning av dataskyddsombudets tillsyn enligt dataskyddsförordningen. Denna berör inte specifikt skyddade personuppgifter men aspekter av dataskyddsarbetet som även har relevans för hanteringen av skyddade personuppgifter. Exempelvis innehåller årsrapporten information om hur många personuppgiftshandläggare det finns inom regionstyrelsen och de olika nämndernas verksamheter, om dessa har deltagit i utbildningar samt information om antal personuppgiftsincidenter som har registrerats under året.

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

Rapportering och utredning av personuppgiftsincidenter[24] är en instruktion som riktar sig till samtliga anställda som misstänker, observerar eller får kännedom om händelse som riskerar säker behandling av personuppgifter. Av instruktionen framgår att personuppgiftsincident ska dokumenteras och anmälas till Integritetskyddsmyndigheten (IMY) inom 72 timmar. Vidare framgår att verksamheten också kan behöva informera de registrerade till exempel om det finns risk för id-stöld eller bedrägeri. Därutöver framgår ansvar och befogenheter.

Verksamhetschef eller avdelningschef ansvarar för att:

- Alla medarbetare informeras om hur incidenter ska rapporteras och utredas på enheten. Nya medarbetare och studenter ska informeras, information ska ske minst en gång per år både skriftligt och muntligt.

[23] Regionstyrelsen besvarar 2023-03-07 § 49. HSN informerad 2023-02-15 § 38.

[24] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2022-03-22 t.o.m. 2024-03-22

- Vidta omedelbara åtgärder vid upptäckten av incident.
- Det finns rutiner som behövs för att personuppgiftsincidenter anmäls och utreds på enheten.
- Ta ställning till om en anmälas till IMY ska göras samt i förekommande fall informera de registrerade.
- Utse personuppgiftshandläggare.

Personuppgiftshandläggare ansvarar för att:

- Starta utredningen av en inrapporterad personuppgiftsincident.
- Vid misstanke om en allvarlig personuppgiftsincident omedelbart kontakta verksamhetschefen/avdelningschef.
- Lämna över ej avslutade personuppgiftsincidenter vid byte av personuppgiftshandläggare.
- Meddela de verksamheter som drabbats av en personuppgiftsincident som upptäckts inom den egna verksamheten.

DSO ansvarar för att:

- Ge råd och stöd till verksamhetschefer och personuppgiftshandläggare.

Alla medarbetare ansvarar för att:

- Rapportera personuppgiftsincidenter som observeras eller kommer denne till kännedom.

I instruktionen definieras begreppet personuppgiftsincident där det även framgår exempel på personuppgiftsincidenter. Vidare definieras allvarliga personuppgiftsincidenter särskilt. Detta begrepp exemplifieras också. I instruktionen betonas att allvarliga incidenter ska rapporteras till IMY inom 72 timmar samt att de registrerade utan dröjsmål ska informeras om incidenten om det är sannolikt att incidenten leder till en hög risk för fysiska personers rättigheter och friheter. Det framgår av instruktionen vilken information som ska lämnas till de registrerade vid incident. Av instruktionen framgår inte någon särskild information om incidenter avseende skyddade personuppgifter. Vi noterar att en allvarlig incident således inte exemplifieras av en röjning av skyddade personuppgifter. Regionen har också en *Mall – för utredning av personuppgiftsincidenter*[25]. För varje rubrik och underrubrik framgår information om vad rubriken ska innehålla. Den innehåller inte heller information om skyddade personuppgifter.

Dataskyddsombud utbildar handläggare om hanteringen av personuppgiftsincidenter. Detta avser inte skyddade personuppgifter specifikt utan personuppgifter generellt.

Det har förekommit att dataskyddsombudet fått frågor avseende skyddade personuppgifter och personuppgiftsincidenter och då betonat vikten av skyndsamhet och återkoppling till drabbade.

I regionens avvikelsehanteringssystem går inte att särskilja en incident som avser skyddade personuppgifter från andra personuppgiftsincidenter. Av *Dataskyddsombudets årsrapport 2022* framgår att 21 personuppgiftsincidenter rapporterades under 2022. Viss uppföljning av antalet incidenter som avser skyddade personuppgifter är möjlig men kräver en betydande manuell handpåläggning och det sker ingen systematisk uppföljning av avvikelser inom detta område. Det har inte rapporterats någon avvikelse avseende skyddade personuppgifter i regionen.

[25] Fastställd av enhetschef juridik och säkerhet. Giltig fr.o.m. 2023-06-07 t.o.m. 2025-06-07

6.3 Bedömning

Vi bedömer att det inte finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. I regionen finns en central process för hanteringen av personuppgiftsincidenter och avvikelser avseende skyddade personuppgifter hanteras i denna process. 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. Då incidenter avseende skyddade personuppgifter inte på något sätt särskiljs från övriga personuppgiftsincidenter är vår bedömning även att det endast finns begränsade förutsättningar för uppföljning inom området, vilket riskerar få konsekvensen att erfarenheter från avvikelser inte tillvaratas och allvarlig skada för patienten eller medarbetaren vars personuppgifter röjts.

Ingen av verksamheterna som har omfattats av granskningen har genomfört några egna kontroller avseende följsamhet till rutiner och regelverk avseende skyddade personuppgifter, undantaget en enkät som genomförts med anledning av denna granskning. Regionstyrelsen och hälso- och sjukvårdsnämnden har inte heller genomfört några särskilda uppföljningar avseende hanteringen av skyddade personuppgifter. Vår sammantagna bedömning utifrån den begränsade möjligheten till uppföljningen av iakttagelser, avsaknaden av egenkontroller samt att regionstyrelsen och hälso- och sjukvårdsnämnden inte beslutat om några styrande dokument är att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad.

7. Svar på revisionsfrågor

Fråga	Svar
Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt en god kontrollmiljö avseende risken för röjning av skyddade personuppgifter?	Nej. Det saknas en ändamålsenlig politisk styrning inom området. Det finns inga politiskt beslutade styrande dokument som specifikt handlar om hantering av skyddade personuppgifter. Den finns en regiongemensam rutinbeskrivning som inte är politiskt beslutat och rutinbeskrivningar på lokal nivå som har fastställts av verksamhetschefer. Därutöver saknas utbildningar om skyddade personuppgifter.
Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att information om regelverk, riskanalyser och kontroller sprids till medarbetare på ett ändamålsenligt sätt?	Nej. Det finns inga regiongemensamma utbildningar avseende hanteringen av skyddade personuppgifter. Enheten för juridik och säkerhet har genomfört regionövergripande utbildningar inom informationssäkerhet, men dessa omfattar inte skyddade personuppgifter. Regionstyrelsen och hälso- och sjukvårdsnämnden har därför inte säkerställt att information om regelverk, riskanalyser och kontroller sprids till medarbetare på ett ändamålsenligt sätt.
Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att adekvata riskanalyser genomförts på rätt nivå för att minska riskerna för att skyddade personuppgifter röjs?	Nej. Området ingår inte i regionstyrelsens eller hälso- och sjukvårdsnämndens tillsynsplaner för internkontroll för 2023 eller 2024. Vi noterar också att området inte heller ingår som en bevakad risk. Under arbetet med granskningen har vi heller inte funnit riskanalyser på tjänstepersonsnivå med inriktning på hantering av skyddade identiteter.
Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt att ändamålsenliga åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter?	Nej. Verksamhetscheferna har enligt regionens ansvarsfördelning ett stort ansvar för att de egna verksamheterna vidtar de åtgärder som krävs för att säkerställa en god hantering av skyddade personuppgifter. Risken för att skyddade personuppgifter avslöjas minimeras genom olika arbetsrutiner i verksamheterna. Dessa har beslutats av verksamhetscheferna – regionstyrelsen och hälso- och sjukvårdsnämnden har inte beslutat om några egna styrande dokument eller kontroller.
Har regionstyrelsen och hälso- och sjukvårdsnämnden säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Nej. I regionen finns en central process för hanteringen av personuppgiftsincidenter och avvikelser avseende skyddade personuppgifter hanteras i denna process. Av upprättade riktlinjer och rutiner för personuppgiftsincidenter framgår inte någon särskild information om skyddade personuppgifter. Det finns därför begränsade förutsättningar för uppföljning inom området, vilket riskerar få konsekvensen att erfarenheter från avvikelser inte tillvaratas och allvarlig skada för patienten eller medarbetaren vars personuppgifter röjts. Ingen av verksamheterna som har omfattats av granskningen har genomfört några egna kontroller avseende följsamhet till rutiner och regelverk avseende skyddade personuppgifter, undantaget en enkät som genomförts med anledning av denna granskning. Regionstyrelsen och hälso- och sjukvårdsnämnden har inte heller genomfört några särskilda uppföljningar avseende hanteringen av skyddade personuppgifter.

Stockholm den 25 mars 2024

David Leinsköld
Verksamhetsrevisor, EY

Daniel Larsson
Verksamhetsrevisor, EY

Bilaga 1. Källförteckning

Intervjuade funktioner

- Informationssäkerhetssmordnare
- Enhetschef, enheten för juridik och säkerhet
- Regionjurist och dataskyddsombud
- Verksamhetschef, psykiatriska kliniken Umeå
- Verksamhetsutvecklare, primärvårdsområde syd
- Kanslichef
- Registrator
- Regionarkivarie
- Objektägare, HR-system
- Verksamhetschef, löneenheten
- Chefsläkare
- Biträdande verksamhetschef, psykiatriska kliniken Skellefteå
- Verksamhetschef, psykiatriska kliniken Södra Lappland
- Verksamhetschef, medicinskt centrum Lycksele lasarett
- Områdeschef, folktandvården
- Avdelningschef
- Objektspecialist, T4
- Tandvårdsstrateg

Granskad dokumentation

- Dataskyddsombudets årsrapport 2022
- Tillsynsplan för intern kontroll 2023, regionstyrelsen
- Tillsynsplan för intern kontroll 2024, regionstyrelsen
- Tillsynsplan för intern kontroll 2023, hälso- och sjukvårdsnämnden
- Tillsynsplan för intern kontroll 2024, hälso- och sjukvårdsnämnden
- Hantering av person med Skyddad identitet HR system
- Rutin för hantering av anställda eller liknande med skyddade personuppgifter
- Ändringshantering och test
- Anskaffning, utveckling och förändring av informationssystem
- Användarklienter
- Vårdsystem – Patienter med skyddade personuppgifter, sekretesskyddad
- Utveckling, kod och arkitektur
- Tröskelanalys avseende dataskydd
- Struktur för dataskyddsarbete inom Region Västerbotten
- Rapportering och utredning av personuppgiftsincidenter
- Objektsarkitektur-OA Modell för Objektstyrning Region Västerbotten
- Nätverkssäkerhet
- Åtkomsträttigheter och säker autentisering
- Mall för utredning av personuppgiftincident
- Loggning, övervakning och synkronisering av tid
- Kryptering, redundans, radering och läckage
- Konsekvensbedömning avseende dataskydd
- Konfiguration, tekniska sårbarheter och webbfiltrering
- Informationssäkerhet

- Informationssäkerhet – tekniska säkerhetsåtgärder
- Informationssäkerhet – användare
- Informationssäkerhet – förvaltning och drift
- Enskildas rättigheter enligt GDPR
- Digital informationshantering
- Vårdprogram Våld i nära relationer Västerbottens läns landsting 2015
- Interna flöden slutenvård – pågående och nya patienter som blir inlagda
- NCS cross Loggkontroll – lokal rutin
- Våld i nära relationer, hedersrelaterat våld och sexuellt våld
- Rapportering och uppföljning av händelser i samverkan mellan primärvård, sluten vård, kommunens hälso- och sjukvård och socialtjänst
- Brevkontakt till person med skyddade personuppgifter
- Kontaktuppgifter för patienter med skyddade personuppgifter, lokal rutin[26]
- Identifiering, bemötande, stöd och behandling till våldsutsatta vuxna
- Instruktion för hjälpmedel till person med skyddad identitet
- Hantering av skyddade personuppgifter, lokal rutin[27]

[26] Psykiatrisk klinik Skellefteå

[27] Psykiatrisk klinik Södra Lappland

Bilaga 2. Revisionskriterier

COSO-modellen 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.

Kommunallagen (2017:725)

Det är enligt 6 kap. 1 § styrelsens uppgift att leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders och eventuella gemensamma nämnder. Regionstyrelsen ska, enligt 6 kap. 2 §, uppmärksammat följa de frågor som kan inverka på regionens utveckling och ekonomiska ställning.

Kommunallagens 6 kap. 6 § anger att nämnderna var och en inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som beslutats av regionfullmäktige samt de föreskrifter som gäller för verksamheten. Nämnderna ska även tillse att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Bilaga 3. Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. Mellan åren 2011 och 2023 har antalet personer med skyddade personuppgifter mer än fördubblats, från drygt 12 000 personer till knappt 27 000 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 0,26 procent av befolkningen och matematiskt motsvarar det ca 723 invånare och knappt 25 anställda i Region Västerbotten. Siffrorna är inte exakta 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[28] intervjuas 86 kvinnor och 15 barn om deras erfarenheter. 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).

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

[28] *Skyddade personuppgifter – oskyddade personer* (Jämställdhetsmyndigheten 2022:10).

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 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.