Granskning Informationssäkerhet - uppföljning och skyddade personuppgifter

Region Västernorrland

December 2023

Ulrike Deppert

Emma Pettersson

Gabriel Axelsson

Helseplan Drottninggatan 97 113 60 Stockholm tel 08-410 408 00 helseplan.se

Innehåll

1. Sammanfattning och slutlig bedömning

Revisorerna i Region Västernorrland har uppdragit åt Helseplan Consulting Group AB (Helseplan) att genomföra en granskning av informationssäkerheten och skyddade personuppgifter samt en uppföljning av tidigare granskning. Syftet har varit att bedöma om tillräckliga åtgärder vidtagits utifrån 2019 års granskning samt om det finns en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter. Granskningen har avsett Regionstyrelsen utifrån sitt övergripande ansvar för regionens informationssäkerhetsarbete. Därtill har granskningen av skyddade personuppgifter även avsett Hälso- och sjukvårdsnämnden som har vårdgivaransvaret för all drift av hälso- och sjukvård och tandvård i egen regi.

Granskningens revisionsfrågor har besvarats genom dokumentstudier samt semistrukturerade intervjuer med förtroendevalda och tjänstepersoner. Granskningen har genomförts mellan juni och december 2023.

Helseplans samlade bedömning är att Regionstyrelsen inte säkerställt en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter och informationssäkerhet. Ett ledningssystem för informationssäkerhet (LIS) har upprättats och en virtuell informationssäkerhetsorganisation har etablerats. Inom ramen för LIS finns styrande dokument som redogör för riktlinjer och rutiner kring informationssäkerhet och skyddade personuppgifter. Däremot har Regionstyrelsen inte utifrån sitt övergripande ansvar för informationssäkerhet säkerställt att det finns strukturer för uppföljning av att rutinerna för skyddade personuppgifter efterlevs.

Helseplan bedömer att tillräckliga åtgärder inte vidtagits utifrån 2019 års granskning. Regionen har upprättat ett LIS på central nivå och en virtuell informationssäkerhetsorganisation har etablerats vilket skapar förutsättningar för regionens fortsatta informationssäkerhetsarbete. Därtill har även en riktlinje för säkerhetsskyddsanalys fastställts. För ett flertal av rekommendationerna bedömer Helseplan att åtgärder delvis vidtagits eller att åtgärder inte vidtagits utifrån rekommendationerna från föregående granskning.

Helseplans samlade bedömning är att Hälso- och sjukvårdsnämnden utifrån sitt vårdgivaransvar inte har säkerställt en tillräcklig intern styrning och kontroll för hanteringen av skyddade personuppgifter i de verksamheter som ingår i nämndens uppdrag. Det finns en regiongemensam rutin för skyddade personuppgifter men däremot saknas styrande dokument för att tillse att det sker en tillräcklig uppföljning av att rutinerna efterlevs. Av granskningen framkommer att det även saknas rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter.

Helseplan rekommenderar Regionstyrelsen:

- att följa upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- att säkerställa och följa upp att en regiongemensam struktur för riskanalyser avseende hanteringen av skyddade personuppgifter upprättas.
- att säkerställa en ändamålsenlig struktur för förankring av styrdokument och rutiner för skyddade personuppgifter inom organisationen.
- att säkerställa en ändamålsenlig uppföljning av personalens kunskap kring gällande regelverk samt att tydliggöra vem som ansvarar för att uppföljning genomförs.
- att säkerställa tillgång till tillräckliga resurser för att regionen ska kunna upprätthålla ett ändamålsenligt arbete avseende informationssäkerhet. Avseende arbetet med skyddade personuppgifter behöver ett tydligt uppdrag och resurser ges till ansvarig enhet.
- att utreda behovet av att göra utbildning i informationssäkerhet och skyddade personuppgifter obligatorisk för berörd personal i syfte att säkerställa tillräcklig kunskap om informationssäkerhet samt hantering av skyddade personuppgifter inom organisationen.
- att säkerställa att alla medarbetare återkommande genomgår relevanta utbildningar med lämpligt intervall för att trygga bestående kunskap över tid.
- att utreda behovet av att erbjuda praktiska utbildningar i hantering av skyddade personuppgifter.
- att säkerställa att riktlinjer för hanteringen av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.
- att säkerställa att riktlinjer för uppföljning och rapportering av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.

Helseplan rekommenderar Hälso- och sjukvårdsnämnden:

- att följa upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- att i dialog med Regionstyrelsen verka för att nödvändiga dokument tas fram.
- att när dokumenten är beslutade säkerställa att dessa implementeras i verksamheten inom nämndens ansvarsområde.

2. Inledning

2.1. Bakgrund

Revisorerna granskade år 2019 regionens informationssäkerhet. Syftet med granskningen var att bedöma om Regionstyrelsen hade tillsett att informationssäkerheten var tillräcklig. I granskningen ingick en uppföljning av 2017 års granskning av IT-säkerheten. Den sammanfattande bedömning som gjordes utifrån 2019 års granskning var att Regionstyrelsen inte hade säkerställt att ändamålsenliga åtgärder hade vidtagits med anledning av 2017 års granskning samt att Regionstyrelsen inte hade säkerställt en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten. Bedömningen baserades på avsaknad av ett gediget ledningssystem för informationssäkerhet och tillhörande organisatorisk struktur och dokumentation, avsaknad av regelbundna rapporteringsrutiner avseende informationssäkerhetsarbetet samt brister i regionens uppföljning och vidtagande av ändamålsenliga åtgärder som följd av iakttagelserna från 2017 års granskning.

Regionen behöver i övrigt kunna hantera skyddade personuppgifter, som är ett samlingsbegrepp för åtgärder som används för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Enligt uppgifter från Jämställdhetsmyndigheten lever i Sverige cirka 15 000 kvinnor och 10 000 män med skyddade personuppgifter. Revisorerna har bedömt att det finns en risk för att inte tillräckliga åtgärder har vidtagits utifrån föregående granskning. Revisorerna har även bedömt att det föreligger en risk för bristande rutiner för hantering av skyddade personuppgifter.

2.2. Syfte och avgränsningar

Syftet med granskningen är att bedöma om tillräckliga åtgärder vidtagits utifrån 2019 års granskning samt om det finns en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter.

Granskningen avser Regionstyrelsen utifrån sitt övergripande ansvar för regionens informationssäkerhetsarbete.

Granskningen av skyddade personuppgifter avser även Hälso- och sjukvårdsnämnden som har vårdgivaransvaret för all drift av hälso- och sjukvård och tandvård i egen regi. Nämnden ansvarar för att verksamheten inom nämndens ansvarsområde bedrivs i enlighet med anvisningar och direktiv från Regionstyrelsen.

2.3. Revisionsfrågor

Granskningen ger svar på följande revisionsfrågor:

- Har tillräckliga åtgärder vidtagits med anledning av de rekommendationer som lämnades i 2019 års revisionsrapport?
- Har ändamålsenliga styrdokument upprättats för hantering av skyddade personuppgifter?
- Utgår hanteringen av skyddade personuppgifter från riskanalyser?
- Är styrdokument och rutiner för hantering av skyddade personuppgifter förankrade i organisationen?
- Har tillräcklig kunskap om gällande regelverk säkerställts för berörd personal?
- Har det tillsetts att det sker en tillräcklig uppföljning av att rutinerna för hantering av skyddade personuppgifter efterlevs?
- Finns ändamålsenliga rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter och efterlevs de?
- Finns det kompetens och kapacitet för att arbeta med informationssäkerhet och skyddade personuppgifter?
- Erbjuds berörd personal teoretiska och/eller praktiska utbildningar i informationssäkerhet och skyddade personuppgifter?

Granskningen har genomförts i enlighet med God revisionssed i kommunal verksamhet samt med beaktning av de rekommendationer och vägledningar som utarbetats av Sveriges Kommunala Yrkesrevisorer (SKYREV).

2.4. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar. Dessa har bland annat varit:

- Kommunallagen (2017:725) 6 kap 6 §, 11 kap 1 §
- Hälso- och sjukvårdslagen (2017:30) 3-5 kap och 7 kap
- Dataskyddsförordningen (GDPR)
- Reglemente för regionstyrelsen, hälso- och sjukvårdsnämnden och regionala utvecklingsnämnden 2023-2026
- Offentlighets- och sekretesslagen (2009:400)

2.5. Metod

2.5.1. Dokumentgranskning

Revisionen har inbegripit granskning av dels relevanta styrande, dels relevanta redovisande dokument. Detta har inkluderat befintliga styrdokument, riktlinjer och arbetsbeskrivningar för informationssäkerhet samt hantering av personuppgifter. Granskningen har tagit del av Regionstyrelsens svar på tidigare genomförda granskningar avseende Region Västernorrlands arbete med informationssäkerhet. Därtill har även redovisande dokument som protokoll och patientsäkerhetsberättelse granskats. En förteckning över granskade dokument finns i *bilaga 1*.

2.5.2. Intervjuer

För att få en god uppfattning och ett tillräckligt underlag från de granskade verksamheterna har Helseplan intervjuat ett urval av personer som är relevanta utifrån granskningens syfte. Bland de politiska förtroendevalda har representanter för Regionstyrelsen och presidiet i Hälso- och sjukvårdsnämnden intervjuats. I förvaltningen har regiondirektören, HR-direktör och samordningsdirektör intervjuats. Även ansvariga tjänstepersoner, som verksamhetschef Regionledningsförvaltningens kansli och informationssäkerhetsstrateg har intervjuats för att få information om hur arbetet med informationssäkerhet och skyddade personuppgifter implementerats och efterlevs.

Totalt har 17 intervjuer genomförts. Samtliga intervjuade har erbjudits möjlighet att sakgranska rapporten. En förteckning över intervjuade funktioner finns i *bilaga 2*.

2.6. Projektorganisation

Från Helseplan har Ulrike Deppert varit projektledare och Emma Pettersson seniorkonsult. Gabriel Axelsson har varit expert och Pär Ahlborg har varit kvalitetsgranskare. Granskningen genomfördes mellan juni och december 2023.

3. Bakgrund

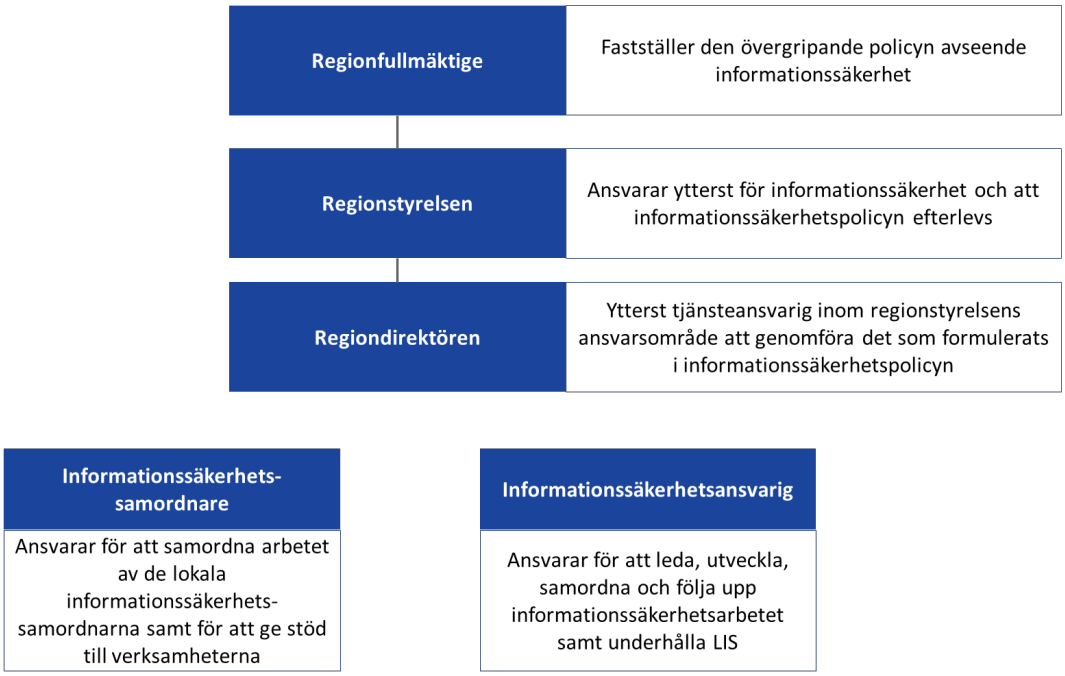
3.1. Ledningssystemet för informationssäkerhet (LIS)

Ledningssystemet för informationssäkerhet (LIS)[1] är baserat på ramverket ISO/IEC 27002 och styr Region Västernorrlands hantering av information och ska säkerställa att den hanteras med den informationssäkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Med ledning avses verksamhetschef för den verksamhet som hen ansvarar för. Verksamhetschef är som regel även informationsägare. I styrningen omfattas att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra informationssäkerheten i verksamhetens informationshantering enligt *riktlinje Informationssäkerhet* (2020).

3.2. Roller och ansvar inom informationssäkerhet

I Region Västernorrland innehas det övergripande informationssäkerhetsansvaret av Regionfullmäktige, Regionstyrelsen, regiondirektören, informationssäkerhetsansvarig och informationssäkerhetssamordnare, vilket framgår av *riktlinje Informationssäkerhet, organisation av* (2020). *Figur 1* beskriver rollerna för det övergripande informationssäkerhetsansvaret i regionen.

[1] Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. *Riktlinje för Säkerhetsskydd i Region Västernorrland* (2021)



Figur 1 - Roller för det övergripande informationssäkerhetsansvaret i Region Västernorrland. Källa: riktlinje Informationssäkerhet, organisation av (2020).

Regionfullmäktige fastställer den övergripande policyn avseende informationssäkerhet för regionen. Regionstyrelsen ansvarar ytterst för dataskydd och informationssäkerhetsarbetet inom regionen, vilket framgår av *Reglemente för regionstyrelsen, hälso- och sjukvårdsnämnden och regionala utvecklingsnämnden 2023-2026*. Styrelsen ansvarar därutöver för att policyn avseende informationssäkerhet som Regionfullmäktige fastställt efterlevs.

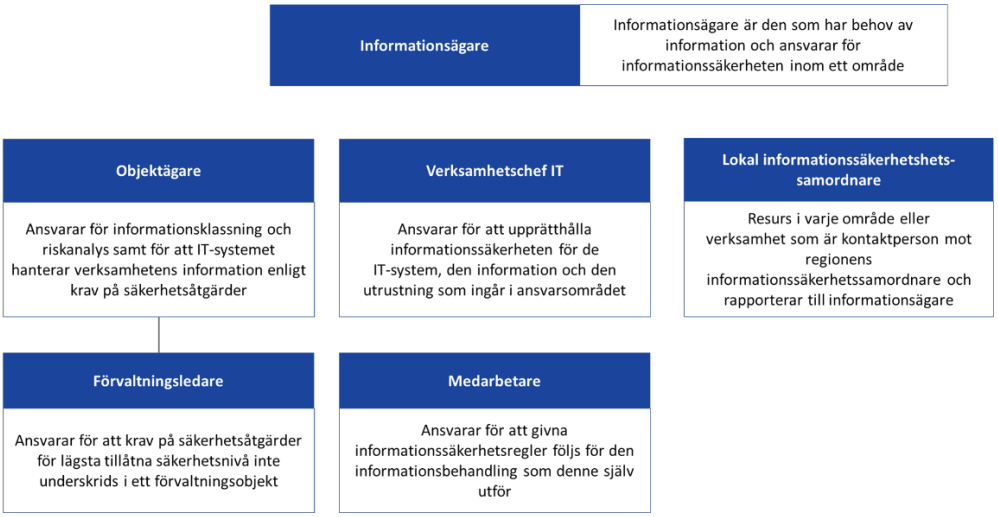
Av *riktlinjen* framgår vidare att det yttersta tjänsteansvaret för att genomföra det som formuleras i informationssäkerhetspolicyn ligger på regiondirektören. Ansvaret omfattar att säkerställa att LIS innehåller de styrdokument som verksamheten kräver och förutsättningar att genomföra det som styrdokumenten anger.

Informationssäkerhetsansvarig, som vid tidpunkten för granskningen även är informationssäkerhetsstrateg, har enligt *riktlinjen* ansvar för att leda, utveckla, samordna och följa upp arbetet med informationssäkerhet, ta fram och underhålla LIS, genomföra omvärldsbevakning samt inhämta information om informationssäkerhetsläget i regionen. Informationssäkerhetsansvarig ska stötta ledning och verksamhetschefer och rollen har inget formellt juridiskt ansvar för informationssäkerheten.

Informationssäkerhetssamordnaren ansvarar för att samordna arbetet av de lokala informationssäkerhetssamordnarna som finns i respektive område eller verksamhet.

Informationssäkerhetssamordnaren ska därtill stödja verksamheterna vid genomförande av informationsklassning, riskanalys och identifiering av säkerhetsåtgärder, vilket framgår av *riktlinjen*.

Riktlinjen redogör även för roller med informationssäkerhetsansvar i verksamheten. *Figur 2* beskriver roller och ansvar för informationssäkerhet i verksamheten.



Figur 2 - Roller och ansvar för informationssäkerhet i verksamheten. Källa: riktlinje Informationssäkerhet, organisation av (2020).

Informationsägare kan vara en förvaltningschef eller verksamhetschef. Denna ska säkerställa en tillräcklig konfidentialitet, riktighet, tillgänglighet och spårbarhet till information i förhållande till informationshanteringens behov och gällande lagkrav i verksamheten. Det är även informationsägaren som beslutar om skyddsnivå, krav på säkerhetsåtgärder och vilka risker som måste hanteras samt vilka risker som är acceptabla inom ägarens respektive område.

Det finns lokala informationssäkerhetssamordnare som är en resurs i varje område eller verksamhet och som är kontaktperson mot regionens informationssäkerhets-samordnare och rapporterar till informationsägare. Av *riktlinjen* framgår att det är dennes ansvar att i sin verksamhet sprida kunskap om LIS och gällande riktlinjer. Därtill finns det objektägare som bland annat ansvarar för genomförande av informationsklassning och riskanalys samt för att IT-systemen hanterar informationen i verksamheten enligt krav på säkerhetsåtgärder. Därutöver finns även förvaltningsledare för ett förvaltningsobjekt med ansvar för att krav på säkerhetsåtgärder för lägsta tillåtna säkerhetsnivå inte underskrids samt verksamhetschef IT med ansvar för att upprätthålla informationssäkerheten för de IT-system och den information och utrustning som ingår i området.

Varje enskild medarbetare har ansvar för att informationssäkerhetsregler följs för den informationssäkerhetsbehandling som denne utför. *Riktlinjen* beskriver att medarbetaren ska rapportera informationssäkerhetsbrister, funktionsfel och brister enligt fastställda rutiner. Brister i fastställda rutiner kan rapporteras till handläggare av dokumentet. Vid behov av IT-support vid IT-problem och IT-incidenter kontaktas Service Desk via självservice med hjälp av e-post eller telefon. Även informationssäkerhetsorganisationen är en kontaktyta när det gäller informationssäkerhet.

3.3. Definitioner och begrepp

Informationsklassning: Inom Region Västernorrland klassas informationstillgångar utifrån den typ, funktion och betydelse den har för verksamheten samt de konsekvenser det medför om informationstillgången skulle hanteras felaktigt, förvanskas, bli otillgänglig eller komma i orätta händer. Klassningsmodellen omfattar informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.[2]

- **Konfidentialitet:** Att innehållet i informationstillgången (eller ibland dess existens) inte får göras tillgänglig eller avslöjas för obehöriga.
- **Riktighet:** Att informationen inte förändras vare sig av obehöriga, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.
- **Tillgänglighet:** Att informationstillgångar ska kunna nyttjas i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

Riskanalys: Riskanalys avser en metodisk process som identifierar säkerhetsrisker och bestämmer dess betydelse.[3]

Riktlinje: Riktlinje är ett dokument som kan omfatta flera verksamheter och anger ramar för vad som ska utföras. Dokumentets funktion är att utgöra ett konkret stöd och en beskrivning av hur en specifik fråga, uppgift eller process ska utföras, men lämna

[2] Enligt mejlkonversation med funktion IT-säkerhetsansvarig och dataskyddsombud, 2023-10-24

[3] *Riktlinje informationssäkerhet* (2020). Inom ramen för dokumentgranskningen har det framkommit att ytterligare definition finns för begreppet riskanalys inom regionen. I *Riktlinje Organisation av informationssäkerhet* (reviderat 2021) definieras riskanalys som en process för att förstå riskens natur och för att avgöra risknivån. Det faktum att det finns fler definitioner medför otydligheter.

utrymme till respektive verksamhet att själv utforma detaljerna. Det kan exempelvis ske genom rutiner. [4]

Rutin: En rutin är ett dokument som anger hur något ska utföras, av vilken funktion och när. En rutin anger vilka förutsättningar och gränser som gäller i en viss fråga. Vanligt förekommande benämningar som exempelvis instruktion, arbetsbeskrivning och manual kan ersättas av benämningen rutin, där dessa innehållsmässigt är att betrakta som styrdokument.[5]

Virtuell informationssäkerhetsorganisation: en horisontell organisation för informationssäkerhet som går över linjestrukturen. I den virtuella informationssäkerhetsorganisationen finns IT-säkerhetsansvarig, informations-säkerhetsansvarig, informationssäkerhetssamordnare, juridiskt stöd samt lokala informationssäkerhetssamordnare.[6]

4. Iakttagelser, bedömningar och rekommendationer

4.1. Styrning och hantering av skyddade personuppgifter

Följande avsnitt behandlar revisionsfrågorna ”Har ändamålsenliga styrdokument upprättats för hantering av skyddade personuppgifter?” och ”Utgår hanteringen av skyddade personuppgifter från riskanalyser?”.

4.1.1. Styrdokument för hantering av skyddade personuppgifter

I *rutin Skyddade personuppgifter* (reviderat 2022) framgår att uppgifter som registreras i folkbokföringen som huvudregel är offentliga. Det finns fall där det kan skada en person om uppgifter om denne lämnas ut. I *rutinen* beskrivs att det exempelvis kan vara när en person riskerar att utsättas för brott, förföljelser eller allvarliga trakasserier. En säker hantering av skyddade personuppgifter bygger på säkra IT-system, begränsad tillgång till

[4] *Riktlinje Styrdokument* (reviderat 2022)
[5] *Riktlinje Styrdokument* (reviderat 2022)
[6] Intervju med verksamhetschef Regionledningsförvaltningens kansli samt IT-säkerhetsansvarig och tillika dataskyddsombud, 2023-12-07.

skyddade personuppgifter, tydliga rutiner för hur personalen ska hantera skyddade personuppgifter samt kunskap om hantering vid begäran om utelämnande av allmänna handlingar som innehåller skyddade personuppgifter.

Syftet med rutinen är att reglera hur regionen ska hantera skyddade personuppgifter. Av *dokumentet* framgår att rutinen ska tillämpas vid all hantering av personuppgifter, vilket innebär för såväl patienter, medborgare, medarbetare som andra uppdragstagare med flera inom Region Västernorrland. *Rutinen* är regiongemensam och är giltig till och med 2024-08-15. Av *riktlinje Styrdokument* (reviderat 2022) framgår att samtliga styrdokument som fastställs på tjänstepersonsnivå ska ses över minst en gång per år för att säkerställa att styrdokumenten alltid är aktuella och relevanta. Dokumentgranskningen visar att *rutinen Skyddade personuppgifter* reviderats 2022 men det framgår inte om den har setts över årligen.

I *rutin Skyddade personuppgifter* redogörs för olika typer av skyddade personuppgifter vilket innefattar skyddad folkbokföring, sekretessmarkering, fingerade personuppgifter samt sekretess för uppgift om hotade och förföljda personers adress med mera. I *rutinen* beskrivs vilken information som ska skyddas i de olika typerna. Därtill framgår hur Region Västernorrland ska kommunicera med eller om en person med skyddade personuppgifter. *Dokumentet* belyser även behovet av att lokala rutiner upprättas av ansvarig chef när en medarbetare har skyddade personuppgifter. Den lokala rutinen syftar till att säkerställa att skyddet för medarbetaren bibehålls i den dagliga verksamheten. Som en del av den lokala *rutinen* uppmanas respektive verksamhet att göra en översyn över vilka personuppgifter som behöver anges i ansökningar, beslut, journaler, protokoll och andra handlingar. Skyddade personuppgifter ska inte i onödan begäras in via handlingar eller registreras i system, oavsett om det gäller en medarbetare, patient eller annan. *Rutinen* redogör även för hantering av skyddade personuppgifter i de administrativa IT-systemen som används i regionen. I *rutin för hantering av känslig grunddata samt skyddad personuppgift i Heroma* (2017) framgår bland annat hur Löneservice ska hantera anställning av en person med skyddade personuppgifter. Granskningen har även tagit del av *rutin Hantering av personer med skyddad identitet – BUP* (reviderat 2023) som avser länsverksamhet Barn- och ungdomspsykiatri samt *riktlinje Skyddade personuppgifter* (reviderat 2023) för Hälsocentralen Bjästa, vilka är lokala rutiner.

Inom ramen för hantering av post till personer med skyddade personuppgifter finns en särskild rutin som gäller för privata vårdgivare, Rättspsykiatriska sluten- och öppenvårdskliniken, Närsjukvårdsområde Norr, Närsjukvårdsområde Söder, Närsjukvårdsområde Väster, Länssjukvårdsområde somatik och Länssjukvårdsområde psykiatri och habiliteringen. I *rutin Hantering av post till personer med skyddade*

personuppgifter (reviderat 2022) beskrivs bland annat Skatteverkets postförmedlingsservice och hantering av post till vissa asylsökande. *Rutinen* är giltig till och med 2025-03-02 och det framgår inte om den har setts över årligen.

I intervjuer uppger en majoritet att det finns upprättade styrdokument och instruktioner för hur skyddade personuppgifter ska hanteras. Av intervjuer framgår att det finns ett generellt regiongemensamt dokument som beskriver grundhantering och vilken information som ska hämtas från vilka källor samt att det finns en beskrivning av vanligt förekommande tjänster och system. Intervjuade uppger även att det finns rutiner som fångar de flesta situationer och är riktade till olika funktioner som exempelvis HR och Löneservice. Därtill uppger ett antal intervjuade att de känner till att dessa styrdokument kontinuerligt revideras.

4.1.2. Riskanalyser avseende hanteringen av skyddade personuppgifter

Riktlinje Informationssäkerhet (2020) beskriver att Region Västernorrland ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett LIS. Arbetet ska, enligt *riktlinjen*, bland annat utgå från informationsklassningar och riskanalyser. Med riskanalys avses en metodisk process som identifierar säkerhetsrisker och bestämmer dess betydelse. Av *riktlinjen* framgår att centrala informationssäkerhetsåtgärder som informationsklassning, riskanalyser, styrning av åtkomst, loggning samt incident- och kontinuitetshantering ska vara prioriterade i informationssäkerhetsarbetet.

I *Patientsäkerhetsberättelse för Region Västernorrland* (2022) framgår att informationssäkerhetsorganisationen kontinuerligt arbetar med hanteringen av regionens informationshanteringsplan, klassificering av information, riskanalyser, upphandlingskrav, personuppgiftsbiträdesavtal och instruktioner, analys av informationshantering, bedömningar samt stöd och vägledning.

Förtroendevalda inom Regionstyrelsen och Hälso- och sjukvårdsnämnden samt tjänstepersoner inom HR uppger att de inte känner till om det genomförs regelbundna riskanalyser avseende hanteringen av skyddade personuppgifter eller att de inte tagit del av sådan. Samtidigt framkommer det enligt uppgift i intervju att arbete ska ske i organisationen kring riskanalyser och identifiering av risker. I intervjuer framkommer att IMS är ett nytt IT-stöd som används för bland annat informationsklassningar, tidigare

användes KLASSA[7]. Intervjuade uppger att enligt rutinen för klassning av information, IT-system och tjänster ska uppföljning genomföras årligen eller vid förändringar. Utifrån klassningen görs en riskanalys och -hantering. På objektmöten, som hålls regelbundet var tredje eller var fjärde vecka i syfte att säkerställa god styrning av IT-stöd, är riskhantering en stående agendapunkt. Listan med identifierade risker gås igenom för att få en överblick över vidtagna åtgärder samt pågående och återstående arbete. I intervju framkommer det att det finns mallar för olika riskanalyser beroende på vad för risker som ska analyseras. Intervjuade uppger samtidigt att det finns ett pågående arbete för att genom IT-stöd ge verksamheterna tydligare vägledning för riskanalyser. Tidigare har verksamheterna själva genomfört riskanalyserna vilket skapat utmaningar då dessa inte alltid varit konsekventa och jämförbara. I IT-stödet IMS dokumenteras riskanalyser och verksamheterna erbjuds möjlighet att få stöd vid genomförandet av en analysledare från informationssäkerhetsorganisationen.

4.1.3. Bedömningar och rekommendationer

Helseplan bedömer att Regionstyrelsen och Hälso- och sjukvårdsnämnden har säkerställt att ändamålsenliga styrdokument upprättats för hanteringen av skyddade personuppgifter. Det finns regiongemensamma styrdokument med upprättade rutiner för hantering av skyddade personuppgifter som ska ses över minst en gång per år men det framgår inte att så sker. Av de regiongemensamma styrdokumenten framgår att lokala rutiner ska tas fram för hanteringen av skyddade personuppgifter för såväl medarbetare som invånare.

Helseplan bedömer att hanteringen av skyddade personuppgifter till viss del utgår från riskanalyser. Riskanalyser ska vara prioriterade i informationssäkerhetsarbetet och det finns mallar för olika riskanalyser. Emellertid finns det en låg kännedom om huruvida det genomförs riskanalyser. Det förekommer också att verksamheterna på egen hand genomför riskanalyser, vilket medför bristande följsamhet till regionens beslutade rutin. Ett nytt IT-stöd för riskanalyser är under framtagande. Därtill visar dokumentgranskningen att definitionen för riskanalys skiljer sig mellan olika styrande dokument inom regionen.

[7] KLASSA är ett verktyg som hjälper organisationer att systematiskt arbeta med informationssäkerhet. KLASSA (skr.se), hämtad 2023-11-27.

Utifrån identifierade förbättringsområden ger vi följande rekommendation:

- Helseplan rekommenderar att Regionstyrelsen och Hälso- och sjukvårdsnämnden följer upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- Helseplan rekommenderar att Regionstyrelsen säkerställer och följer upp att en regiongemensam struktur för riskanalyser avseende hanteringen av skyddade personuppgifter upprättas.

4.2. Kompetens och kapacitet avseende informationssäkerhet och skyddade personuppgifter

Följande avsnitt behandlar revisionsfrågorna ”Är styrdokument och rutiner för hantering av skyddade personuppgifter förankrade i organisationen?”, ” Har tillräcklig kunskap om gällande regelverk säkerställts för berörd personal?”, ”Finns det kompetens och kapacitet för att arbeta med informationssäkerhet och skyddade personuppgifter?” samt ”Erbjuds berörd personal teoretiska och/eller praktiska utbildningar i informationssäkerhet och skyddade personuppgifter?”.

4.2.1. Förankring av styrdokument och rutiner i organisationen

Det övergripande ansvaret för informationssäkerhet innehas av Regionstyrelsen vilket framgår av *riktlinje Informationssäkerhet, organisation av* (2020). Även Regionfullmäktige, regiondirektören, informationssäkerhetsansvarig och informationssäkerhetssamordnare har uttalade roller och ansvar för att regionen ska uppnå och behålla en god informationssäkerhet. Det yttersta tjänsteansvaret att genomföra den fastslagna informationssäkerhetspolicyn ligger på regiondirektören, enligt *riktlinjen*. I *dokumentet* beskrivs att riktlinjer för informationssäkerhet ska styra hanteringen av informationssäkerhetsarbetet inom regionen mot ett proaktivt och systematiskt arbete som tar hänsyn till samtliga aspekter av informationssäkerhet.

Av *riktlinje Styrdokument* (reviderat 2022) framgår att det är ett chefsansvar att säkerställa att för verksamheten relevanta styrdokument tillgängliggörs och introduceras för medarbetarna. Medarbetarna har i sin tur ansvar för att tillämpa gällande version av styrdokumentet. I *riktlinjen Informationssäkerhet* (2020) beskrivs att det i regionen ska finnas en informationssäkerhetskultur som uppmuntrar engagemang hos alla medarbetare, utöver att följa gemensamma regler, vilket motiverar medarbetarna att delta i att ständigt förbättra informationssäkerheten. I avsnitt *3.2*

Informationssäkerhetssansvar i denna granskning redogörs för olika rollers ansvar inom regionen.

Intervjuade inom Regionledningsförvaltningen och HR upplever att styrdokument och rutiner för hantering av skyddade personuppgifter är förankrade i organisationen. Av intervjuer framgår att det finns ett IT-system för styrdokument, Platina[8], som har en tydlig struktur för granskning, fastställande och distribution av rutiner och riktlinjer. När nya styrdokument finns eller dokument blivit fastställda eller reviderade meddelas verksamhetschefer och enhetschefer som sedan ansvarar för att sprida informationen vidare. Trots denna struktur uppger ett antal av de intervjuade att det finns en risk att informationen inte når fram till alla medarbetare då organisationen är stor.

4.2.2. Personalens kunskap om gällande regelverk

Av *riktlinje Informationssäkerhet, organisation av* (2020) framgår att Regionstyrelsen har det övergripande ansvaret för informationssäkerhet inom Region Västernorrland. Som framgår av avsnitt *4.2.1 Förankring av styrdokument och rutiner i organisationen* har även Regionfullmäktige, regiondirektör, informationssäkerhetsansvarig och informationssäkerhetssamordnare uttalade roller och ansvar. *Riktlinjen* framhåller därtill att ansvaret för det dagliga informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Målet med riktlinjen är att upprätta ett organisatoriskt regelverk i syfte att styra arbetet kring informationssäkerhet och att samtliga medarbetare är medvetna om sitt ansvar för informationssäkerheten.

Medarbetarens ansvar framgår av *riktlinjen* och handlar om att ansvara för att givna informationssäkerhetsregler följs för den informationsbehandling medarbetaren utför. Därtill ska medarbetaren rapportera informationssäkerhetsbrister, funktionsfel och brister enligt fastställda rutiner. I *riktlinje Informationssäkerhet* (2020) framgår att en av LIS viktigaste delar är medarbetarnas kunskap, medvetenhet och motivation. Forum för dialog och utveckling i informationssäkerhetsfrågor samt målgruppsanpassat material lyfts därför fram som centrala funktioner i LIS. Intervjuade uppger att det finns utbildningsmaterial på intranätet för målgrupperna informationsägare, lokal informationssamordnare, objektägare, förvaltningsledare, chef och medarbetare.

[8] Platina är ett dokument- och ärendehanteringssystem. Platina - Ett dokument- och ärendehanteringssystem - Formpipe, hämtad 2023-10-13.

Materialet består av film och presentation inom området säkerhetsmedvetandet, informationssäkerhet, riktlinjer för informationssäkerhet och informationshanterings-plan. Det framkommer i intervju att det finns ett forum för lokala informations-säkerhetssamordnare där utbildning och information ges i aktuella frågeställningar. Möten i forumet hålls två till fyra gånger per år. Det finns även ett säkerhetsforum med driftleverantör där regelbundna möten sker. Även den virtuella informationssäkerhets-organisationen har överenskomna regelbundna möten.

Inom ramen för dokumentgranskningen framgår inte att systematisk uppföljning av personalens kunskap och deltagande i utbildning kring hantering av skyddade personuppgifter genomförs.

Ett flertal intervjuade upplever att medarbetarna är försiktiga när det kommer till hanteringen av skyddade personuppgifter, att medarbetarna är måna om att göra rätt samt att medarbetarnas kännedom om gällande regelverk är god. I intervjuer lyfts därtill att det är viktigt att säkerställa att de rutiner som finns är tillgängliga och att medarbetare använder sig av dessa. Intervjuade inom Regionledningsförvaltningen uppger att det inte genomförs någon systematisk och regelbunden uppföljning av följsamhet till befintliga rutiner. Ett flertal intervjuade menar att utbildningar behöver ske regelbundet och i större utsträckning. Det framkommer i intervjuer att det ska ha tagits fram underlag och utbildningar kring informationssäkerhet. Enligt uppgift i intervju ska det finnas rutiner för att nya medarbetare erhåller utbildning men samtidigt upplevs det svårare att hitta tid för att utbilda cheferna. Intervjuade uppger att det pågår ett arbete med att ta fram utbildningssidor för dessa frågor. Se avsnitt *4.2.4 Utbildning inom informationssäkerhet och skyddade personuppgifter* för mer information. Vad avser skyddade personuppgifter som omfattar medarbetare uppger intervjuade att de anser att det dels finns rutiner, dels stöd att få ifall ansvaret för att hantera medarbetaren faller inom ens egen roll.

4.2.3. Kompetens och kapacitet för att arbeta med informationssäkerhet och skyddade personuppgifter

Av *riktlinje Informationssäkerhet* framgår att Region Västernorrland ska ha tillgång till tillräcklig kompetens inom informationssäkerhetsområdet för att kunna hantera den komplexa kravbild som finns avseende informationssäkerhet. Den komplexa kravbilden gör det nödvändigt med en fast styrning och ett systematiskt arbetssätt för att upprätthålla en informationshantering med tillräcklig informationssäkerhet och kvalitet. Vidare framhålls att kompetensen ska finnas såväl i form av spetskompetens som i form av en bred förståelse för betydelsen av informationssäkerhet hos medarbetarna. *Riktlinjen* utgör grunden för Region Västernorrlands systematiska arbete med

informationssäkerhet i syfte att säkerställa en ändamålsenlig nivå av skydd och kvalitet i regionens informationshantering. Systematiska arbetssätt är nödvändigt för att upprätthålla en hantering av tillräcklig informationssäkerhet. Ett uppdaterat och implementerat LIS är ett verktyg för att uppnå det. Av *Regionstyrelsens protokoll* (2021-06-10) framgår att regionen under 2020 sett över sitt LIS och i samband med det även sett över involverade roller. I *protokollet* framgår att utbildning skapas för identifierade roller med informationssäkerhetsansvar för att bygga kompetens och kunskap i hantering av informationssäkerhet. Se avsnitt *3.2 Roller och ansvar inom informationssäkerhet* för mer information om de olika rollernas ansvarsområden.

I intervjuer framgår att det byggts upp en kompetens och kapacitet kring informationssäkerhet och att det finns en virtuell organisation för informationssäkerhet i regionen. Flertal intervjuade upplever att det finns kompetens och kapacitet att arbeta med informationssäkerhet och skyddade personuppgifter och att organisationen för detta är välfungerande. Några intervjuade lyfter att det finns en osäkerhet kring hur kunskapen att arbeta med detta längre ut i verksamheten är då all information inte finns i den övergripande rutinen.

Det framkommer att det finns en önskan att kunna arbeta mer strategiskt och proaktivt kring informationssäkerhet och skyddade personuppgifter, vilket enligt uppgift i intervju skulle vara möjligt om de personella resurserna skulle öka. Intervjuade uppger att det i informationssäkerhetsorganisationen ingår en informationssäkerhetsansvarig, en informationssäkerhetssamordnare, IT-säkerhetsansvarig samt regionjurist vid behov. Det finns ingen fastställd procentsats för rollerna och i rollerna ingår även andra arbetsuppgifter, framgår av intervjuer. Intervjuade upplever att en stor del av arbetet är operativt, med till exempel många öppna ärenden, vilket leder till att det utvecklande arbetet ibland inte prioriteras. Vidare är säkerhetsfrågorna omfattande och det är ofta samma personella resurser som involveras, vilket gör att den kapacitet som finns blir ansträngd. Intervjuade uppger att det inte finns tillsatta resurser för att arbeta med skyddade personuppgifter inom informationssäkerhetsorganisationen då organisationen inte har ett uppdrag kring skyddade personuppgifter. I intervju uppges att det saknas en organisation för frågor rörande skyddade personuppgifter och att frågor från verksamheten inom detta område som skickas till informationssäkerhetsorganisationen ofta skickas vidare till exempelvis IT-stöd eller jurist.

4.2.4. Utbildning inom informationssäkerhet och skyddade personuppgifter

Intervjuade beskriver att teoretiska utbildningar finns tillgängliga på regionens intranät, där det även finns tillgång till fastställda styrdokument. Närmaste chef har ansvar för att

säkerställa att nya medarbetare genomgår för sin roll aktuella utbildningar. Som stöd har chefen checklistor som beskriver hur introduktion av nya medarbetare ska ske. Av intervjuer framkommer det att inom Region Västernorrland pågår ett arbete med att implementera en ny digital lärplattform, Kompass. Plattformen kommer att kunna styra obligatoriska utbildningar utifrån medarbetarens roll/funktion, det vill säga att medarbetaren kommer att få automatisk information om vilka utbildningar som hen ska genomföra. Detta sker dels vid nyanställning, dels när nya obligatoriska utbildningar skapas för den berörda rollen/funktionen. Syftet är att underlätta för chefer och medarbetare, till exempel enklare anmälan till utbildningar, samt också att aktivt kunna arbeta med uppföljning/kontroll av att medarbetare genomgår sina obligatoriska utbildningar. I lärplattformen kommer även frivilliga utbildningar att finnas med samma möjlighet för chefer att följa upp om medarbetaren har genomfört överenskomma utbildningar.

De utbildningar som erbjuds vid tidpunkten för denna granskning avseende informationssäkerhet och skyddade personuppgifter är av teoretisk karaktär och är inte obligatoriska. Inga praktiska utbildningar erbjuds. Utbildningar inom området genomförs både via webben och genom kurser som sker på plats i regionens utbildningslokaler. Två exempel på digitala utbildningar är *Informationssäkerhet vid distansarbete* samt *Säkerhetsmedvetenhet* som granskningen tagit del av i form av utklipp från intranätet. Utbildning i informationssäkerhet kan genomföras fysiskt eller digitalt med exempelvis läkare och sjuksköterskor. Utbildningarna är totalt cirka tre timmar och finns tillgängliga digitalt. Vid intervjuer framgår att utbildningen kan ske lärarledd vid ett tillfälle men att materialet även går att ta del av i efterhand. Intervjuade uppger att utbildningen inte är obligatorisk.

Intervjuade uppger att utbildningsmaterial om informationssäkerhet är framtaget till rollerna informationsägare, lokal informationssäkerhetssamordnare, objektägare, förvaltningsledare, chef och medarbetare. Materialet består av film inom området säkerhetsmedvetandet, informationssäkerhet, riktlinjer för informationssäkerhet och informationshanteringsplan och finns tillgängliga via intranätet, vilket urklipp som granskningen tagit del av bekräftar. Vid behov eller vid önskemål om utbildning från verksamheten om skyddade personuppgifter ges den av informationssäkerhetsansvarig och-/eller jurist.

Av dokument *Utvärdering Grundutbildning skyddade personuppgifter 4 december 2019* framgår att 56 procent av de totalt 82 respondenterna bedömer att grundutbildningen i skyddade personuppgifter som helhet var mycket bra och 40 procent bedömer att den var bra. Av utvärderingen framgår vidare att 75 procent uppger att de kommer kunna tillämpa det de lärt sig under utbildningen i sitt dagliga arbete.

En majoritet av de intervjuade uppger att de känner till att det finns teoretiska utbildningar kring informationssäkerhet och skyddade personuppgifter. Utbildningarna genomförs framförallt för nya medarbetare. Intervjuade lyfter vidare att det finns planer på att nya medarbetare ska få ta del av ett utbildningspaket när de börjar och att detta förhoppningsvis ska finnas på plats inom kort.

4.2.5. Bedömningar och rekommendationer

Helseplan bedömer att styrdokument och rutiner för hanteringen av skyddade personuppgifter delvis är förankrade i organisationen. Av redovisade dokument framgår att det är ett chefsansvar att säkerställa att för verksamheten relevanta styrdokument tillgängliggörs och introduceras för medarbetarna. Intervjuade uppger att styrdokument och rutiner är förankrade i organisationen. Granskningen visar inte att någon systematisk uppföljning av kännedomen kring dessa styrdokument genomförs.

Helseplan bedömer att Regionstyrelsen inte har säkerställt att berörd personal har tillräcklig kunskap om gällande regelverk. Det finns en tydlig rollfördelning mellan olika organisatoriska nivåer som beskriver hur ansvaret struktureras mellan till exempel medarbetare och chef. Det finns också utbildningar som syftar till att bygga kunskap inom berörda regelverk. Däremot har det inom ramen för granskningen inte framgått om det genomförs en systematisk uppföljning för att säkerställa tillräcklig kunskap om gällande regelverk hos personalen.

Helseplan bedömer att det upprättats en virtuell informationssäkerhetsorganisation med kompetens att arbeta med informationssäkerhet. I informationssäkerhetsorganisationen ingår en informationssäkerhetsansvarig och en informationssäkerhetssamordnare samt en IT-säkerhetsansvarig och tillgång till regionjurist finns vid behov. Emellertid framgår det i intervju att personella resurser som arbetar med informationssäkerhetsfrågor är ansträngda Helseplan bedömer att det finns kompetens att arbeta med informationssäkerhet men att kapaciteten är begränsad. Därtill bedömer Helseplan att det saknas en tydlig organisation med uttalat uppdrag för att hantera frågor rörande skyddade personuppgifter. Helseplan bedömer att det finns fragmenterad kompetens inom regionen men ingen struktur i hur frågorna hanteras. Det finns begränsad organisatorisk kapacitet för att arbeta med skyddade personuppgifter.

Helseplan bedömer att berörd personal erbjuds teoretiska utbildningar i informationssäkerhet och skyddade personuppgifter. Utbildningstillfällen erbjuds huvudsakligen nya medarbetare strukturerat och material finns tillgängligt efter

genomförd utbildning. Utbildningarna är inte obligatoriska. Inga praktiska utbildningar erbjuds.

Utifrån identifierade förbättringsområden ger vi följande rekommendationer:

- Helseplan rekommenderar att Regionstyrelsen säkerställer en ändamålsenlig struktur för förankring av styrdokument och rutiner för skyddade personuppgifter inom organisationen.
- Helseplan rekommenderar att Regionstyrelsen säkerställer en ändamålsenlig uppföljning av personalens kunskap kring gällande regelverk samt att tydliggöra vem som ansvarar för att uppföljning genomförs.
- Helseplan rekommenderar att Regionstyrelsen säkerställer tillgång till tillräckliga resurser för att regionen ska kunna upprätthålla ett ändamålsenligt arbete avseende informationssäkerhet. Avseende arbetet med skyddade personuppgifter behöver ett tydligt uppdrag och resurser ges till ansvarig enhet.
- Helseplan rekommenderar Regionstyrelsen att utreda behovet av att göra utbildning i informationssäkerhet och skyddade personuppgifter obligatorisk för berörd personal i syfte att säkerställa tillräcklig kunskap om informationssäkerhet samt hantering av skyddade personuppgifter inom organisationen.
- Helseplan rekommenderar Regionstyrelsen att säkerställa att alla medarbetare återkommande genomgår relevanta utbildningar med lämpligt intervall för att trygga bestående kunskap över tid.
- Helseplan rekommenderar Regionstyrelsen att utreda behovet av att erbjuda praktiska utbildningar i hantering av skyddade personuppgifter.

4.3. Rutiner, uppföljning och rapportering av efterlevnad till rutiner avseende skyddade personuppgifter

Följande avsnitt behandlar revisionsfrågorna ”Har det tillsetts att det sker en tillräcklig uppföljning av att rutinerna för hanteringen av skyddade personuppgifter efterlevs?” och ”Finns ändamålsenliga rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter och efterlevs de?”

4.3.1. Uppföljning av efterlevnad till befintliga rutiner för hantering av skyddade personuppgifter

Den regiongemensamma *riktlinjen Efterlevnad-hantering av efterlevnad för informationssäkerhet* (reviderat 2021) beskriver hanteringen av efterlevnad för informationssäkerhet inom Region Västernorrland. Inom ramen för granskningen har inga motsvarande dokument för skyddade personuppgifter framkommit.

I intervju framgår att Region Västernorrland under 2020 ändrade sin styrmodell. En del av syftet med den nya styrmodellen var att från politisk nivå lättare kunna följa upp arbetet som sker i organisationen. I intervjuer beskrivs att Regionstyrelsen inte har fått någon detaljerad uppföljning av efterlevnad till befintliga rutiner för hanteringen av skyddade personuppgifter. Däremot finns det i patientsäkerhetsberättelsen ett avsnitt om informationssäkerhet som informationssäkerhetsorganisationen tar fram. Patientsäkerhetsberättelsen beslutas politiskt av Regionstyrelsen. Intervjuade uppger att det pågår ett arbete med att skapa en systematisk uppföljning kring informationssäkerhet i allmänhet men arbetet har ännu inte färdigställts.

Vidare uppger intervjuad att förvaltningsobjekten arbetar med internkontroll som en del av det årliga systematiska förbättringsarbetet. Inom ramen för Oktav[9] har ett revisionspaket tagits fram som består av dokument som beskriver vem som gör vad och lämpliga kontrollpunkter. Rutinen, som bland annat innehåller kontrollfrågor om skyddade personuppgifter, gäller alla IT-stöd men genomförs bara för Oktav och SITHS[10] där det finns utpekade resurser för att arbeta med denna form av revision.

4.3.2. Rutiner för rapportering vid genomförd uppföljning

Av den regiongemensamma *riktlinjen Efterlevnad - rapportering av informationssäkerhet* (reviderat 2021) framgår att resultaten av informationssäkerhetsgranskningar, inklusive rekommendationer, ska dokumenteras

[9] Oktav är en förkortning för Organisationskatalog Västernorrland *Handbok För Lokal administratör i oktav* (2022).

[10] SITHS är en elektronisk identitetshandling som används för säker identifiering av personer och system inom regioner, kommuner, privata vårdgivare och statliga myndigheter (SITHS Identifieringstjänst - Inera), hämtad 2022-09-06

samt rapporteras till ägare och chef. Inom ramen för granskningen har inga motsvarande dokument för skyddade personuppgifter framkommit.

En majoritet av de intervjuade kan inte svara på om det finns ändamålsenliga rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter.

Vid större projekt, som överstiger 200 timmar, har IT-förvaltningen en stående rutin där de en gång i månaden har PULS-möten[11] där projekten följs upp. Hade det funnits ett projekt i motsvarande storlek för personuppgifter hade det följts upp på PULS.

Intervjuade lyfter också att trots att det saknas rutiner för hur rapportering av genomförd uppföljning av skyddade personuppgifter ska göras tas ämnet upp med jämna mellanrum i verksamheten, exempelvis i samband med att utlämnande av offentliga handlingar diskuteras.

4.3.3. Bedömningar och rekommendationer

Helseplan bedömer att Regionstyrelsen inte har tillsett att det sker en tillräcklig uppföljning av att rutinerna för hanteringen av skyddade personuppgifter efterlevs. Det saknas riktlinjer för uppföljning av hantering och efterlevnad för skyddade personuppgifter.

Helseplan bedömer att Regionstyrelsen inte har tillsett att det finns ändamålsenliga rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter samt att de efterlevs. Det saknas riktlinjer för uppföljning och rapportering för skyddade personuppgifter.

Utifrån identifierade förbättringsområden ger vi följande rekommendationer:

- Helseplan rekommenderar Regionstyrelsen att säkerställa att riktlinjer för hanteringen av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.

[11] PULS-möten är en uppföljning av pågående projekt där objektledare IT är rapportör, enligt mejlkonversation med verksamhetschef IT, 2023-12-12.

- Helseplan rekommenderar Regionstyrelsen att säkerställa att riktlinjer för uppföljning och rapportering av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.

Då granskningen av skyddade personuppgifter även avser Hälso- och sjukvårdsnämnden som har vårdgivaransvaret för all drift av hälso- och sjukvård och tandvård i egen regi bedömer Helseplan att nämnden bär ett ansvar att tillse att Regionstyrelsen säkerställer att ovan nämnda saknade styrdokument tas fram. Därför ger vi följande rekommendationer:

- Helseplan rekommenderar Hälso- och sjukvårdsnämnden att i dialog med Regionstyrelsen verka för att nödvändiga dokument tas fram.
- Helseplan rekommenderar Hälso- och sjukvårdsnämnden att när dokumenten är beslutade säkerställa att dessa implementeras i verksamheten inom nämndens ansvarsområde.

5. Uppföljning av rekommendationer (2019)

Följande avsnitt behandlar revisionsfrågan ”Har tillräckliga åtgärder vidtagits med anledning av de rekommendationer som lämnades i 2019 års revisionsrapport?”.

5.1. Uppföljning av informationssäkerhetsarbetet

Tabell 1 visar en uppföljning av de rekommendationer som gavs till Regionstyrelsen vid genomförd granskning 2019. Grön färgmarkering med ord ”Ja” i tabellen innebär att rekommendationer från tidigare granskningar åtgärdats, gul färgmarkering med ord ”Delvis” innebär att de delvis åtgärdats och röd färgmarkering med ord ”Nej” innebär att de inte har åtgärdats. En bedömning är markerad med vit färgmarkering och med ord ”Går inte att bedöma”. Detta för att bedömning inte är möjlig att göra.

Rekommendation 2019	Uppföljning 2023	
Människor och processer		
Regionen bör fastställa en färdplan för införandet av ett ledningssystem för informationssäkerhet. En sådan färdplan bör innehålla tydliga målsättningar, ansvarsbeskrivningar för medverkande	Intervjuade uppger att arbetet med att upprätta ett LIS påbörjades 2019. Arbetet har resulterat i att ett LIS har upprättats och implementerats på central nivå inom regionen.	

resurser, samt en konkret tidsram som arbetet för framtagning av ett ledningssystem ska förhålla sig till.		
Regionen bör utreda möjligheten att upprätta en arbetsgrupp för informationssäkerhet som sammanträder regelbundet och inkluderar nyckelpersoner för arbetet - exempelvis informations-säkerhetssamordnaren, IT-chef och/eller IT-säkerhetsansvarig, Administrativ chef, säkerhets-samordnare samt representanter från samtliga fackförvaltningar. Denna grupp bör ha ansvar för förvaltning av Ledningssystemet för informationssäkerhet och bör ha som uppgift att styra och samordna informationssäkerhetsarbetet inom hela regionen. Arbetsgruppen bör vidare ha ett övergripande ansvar för omvärldsbevakning inom informationssäkerhetsområdet.	En virtuell informationssäkerhets-organisation är etablerad. Den sammanträder, enligt intervjuer, i incident- och handläggningsmöten varannan dag samt vid behov. I informationssäkerhetsorganisation en ingår informationssäkerhets-ansvarig, informationssäkerhets-samordnare, IT-säkerhetsansvarig samt regionjurist på behovsbasis. Beskrivning av roller och ansvar för dessa kompetenser finns beskrivna i *riktlinje Informationssäkerhet, organisation av* (2020) samt *riktlinje Organisation av informationssäkerhet – rollbeskrivning* (reviderat 2021).	
Inom ramen för ledningssystemet för informationssäkerhet bör regionen upprätta ett aggregerat riskregister med region-övergripande informations-säkerhetsrisker. Ett sådant register bör uppdateras regelbundet samt användas för åtgärdsplanering, och bör utgöra grunden till en reguljär rapportering till regionstyrelsen eller regionens ledning. Riskregistret bör vara framtaget med regionens huvudsakliga samhällsfunktion och leverans i åtanke.	Ett aggregerat riskregister med regionövergripande informations-säkerhetsrisker har inte upprättats.	

Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation som tillhör ledningssystemet ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.	Intervjuade inom informations-säkerhetsorganisationen uppger att huvudsakliga informations-säkerhetsprocesser är dokumenterade. *Riktlinje Organisation av informations-säkerhet – rollbeskrivning* (reviderat 2021) beskriver arbets-uppgifter och ansvarsområden kopplat till informationssäkerhets-organisationen och *riktlinje Informationssäkerhet* (2020) beskriver principerna för regionens informationssäkerhetsarbete. Av *riktlinje Styrdokument* (reviderat 2022) framgår att styrdokument som fastställs på tjänstepersonnivå ska ses över minst årligen. Styr-dokumenten har reviderats sedan de fastställdes men det framgår inte med vilket intervall. I de dokument som granskats framgår vem som är handläggare samt vem som är fastställare av dokumentet.	
Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhets-policyn till riktlinjer.	Mätbara mål för samtliga åtgärdsmål har inte identifierats och definierats. Intervjuade uppger att informationssäkerhetspolicyn från 2008 ska revideras. Riktlinjer enligt LIS är fastställda.	
Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Västernorrland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.	En informationssäkerhets-utbildning är etablerad men inte obligatorisk. Utbildningarna omfattar framförallt nya medarbetare. Det sker ingen uppföljning av huruvida medarbetare genomför utbildningen. Inga praktiska övningar genomförs. Det pågår ett arbete med att implementera en ny digital lärplattform, Kompass.	

	Plattformen kommer kunna styra obligatoriska utbildningar utifrån medarbetarens roll/funktion samt ge möjlighet för chefer att följa upp om medarbetaren genomfört överenskomna utbildningar.	
Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör även genomföra systematiska uppföljningar av utbildningsverksamheten.	Intervjuade uppger att utbildnings-aktiviteter för att främja en god säkerhetskultur inte har specificerats i verksamhetsplaner. Utbildningsmaterial om informationssäkerhet finns tillgängligt via intranätet och viss uppföljning sker i form av utvärderingar av utbildningen. Utbildningsmaterialet ska flyttas till regionens nya lärplattform, Kompass, som erbjuder funktionalitet att följa upp enskilda medarbetares genomförda utbildningar.	
Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.	Intervjuade uppger att personuppgiftsincidenter registreras i avvikelsehanterings-systemet. Alla IT-incidenter registreras i ett ärendehanterings-system. Större incidenter följs alltid upp för att förhindra att de uppstår igen. Andra IT-incidenter följs upp vid behov uppger intervjuade. Informationssäkerhetsorganisation en arbetar inte systematiskt med utvärdering i avvikelsehanterings-systemet utan det sker behovsstyrt.	
Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.	Informationssäkerhets-organisationen arbetar aktivt med dokumentation av arbetssätt och rutiner för informationssäkerhet och personuppgifter. Det finns enligt intervjuer ett visst, fortsatt personberoende kopplat till	

	resurser inom informations-säkerhet, det vill säga att kunskap finns hos enskilda personer och är inte tillräckligt dokumenterat. Vidare framgår av intervjuer att samtliga verksamheter inom regionen försöker undvika att arbeta i så kallade stuprör för att säkerställa en jämn kännedom och kunskap.	
Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Västernorrland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.	Regionstyrelsen har fastställt riktlinje för *Säkerhetsskydd i Region Västernorrland* (2021). Regionstyrelsen har fastställt en säkerhetsskyddsanalys vid sitt sammanträde 2023-06-07 vilket framgår av protokoll som granskningen tagit del av. Dokumentets säkerhetsskydds-klassning medför att granskningen inte har kunnat ta del av det. Därför kan vi inte bedöma uppföljningen av rekommendationen.	
Regionen bör se över förvaltningsmodellen för verksamhetssystem och utreda möjligheter till att förstärka ansvaret som systemägare har för tillämpning av informations-säkerhetsåtgärder.	En översyn av förvaltnings-modellen för verksamhetssystem pågår. Enligt intervjuade finns det utmaningar mellan regionlednings-förvaltningen och IT gällande bland annat resurser och ekonomi samt olika syn på prioriteringar och efterlevnad av styrdokument.	
Teknik		
Utred möjligheterna till att införskaffa en central behörighetshantering som integreras med övriga verksamhetssystem (i synnerhet HR systemet som regionen använder). Ett sådant system bör till stor del automatisera processer för tilldelning, förändring, och	IT bedriver ett projekt (som är starkt kopplat till nya journalsystemet Cosmic) för ett IGA-verktyg (Identity governance and administration). Verktyget är ännu inte infört. Intervjuade uppger att behörigheter kommer tilldelas utifrån medarbetarens uppdrag, vilket innebär en annan	

borttagning av behörigheter. Utifrån ett sådant system bör behörighetstilldelning och behörighetsgrupper framtas som baseras på i förväg bestämda roller. I synnerhet bör regionens tilldelning av behörigheter till fysiska lokaler ses över, särskilt med hänsyn till känsliga rum som serverhallar.	ordning för behörighetstilldelning. I vissa system, framförallt i system som är mindre kritiska, sker mycket manuell hantering vilket kan innebära risker. Med risker avses att användare överskrider sina befogenheter i förhållande till sina arbetsuppgifter eller att behörigheten inte är tillräckligt för att utföra sina arbetsuppgifter.	
Utred möjlighet till att införskaffa en SIEM-lösning som samlar in och aggregerar säkerhetsloggar från väsentliga nätverkskällor, exempelvis de virtuella brandväggar som i nuläget är placerade mellan nätverkssegment. Införskaffandet av en dedikerad loggserver bör även utredas med krav på bibehållen lagring på minst 180 dagar.	Informationssäkerhetsorganisationen utreder och driver frågan om att införskaffa en SIEM-lösning men enligt intervjuade har frågan inte uppmärksammats i tillräcklig utsträckning samt att det saknas tid och ekonomi för vidare utredning och en framtida implementering.	
Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans.	Regionstyrelsen beskriver i *Svar på revisionsrapporten Granskning av informationssäkerhet* (2020-03-18) ”[a]tt utöka den geografiska spridningen på regionens serverhallar [...] är ett omfattande arbete som måste vägas mot arbetsmängd och kostnad och [...] anses inte [...] vara en prioriterad åtgärd.” Enligt intervjuer har regionen upphandlat ett nytt outsourcingavtal där vissa delar, i samråd med informationssäkerhetsorganisationen, har flyttats utanför befintliga hallar. Server för telefoni finns på respektive sjukhus samt i Regionens hus. Vid upphandling av nya IT-system och -tjänster ställs krav på informationssäkerhet utifrån LIS och relevanta lagar beroende på den information som	

	kommer att behandlas. Det är informationstillgång och informationsklassning som styr informationssäkerhetskraven. De kraven har även ställts vid upphandling av IT-tjänsten (outsourcing) drift och nät samt IT-arbetsplats. Det är informations-säkerhetsorganisationen inom Region Västernorrland som tar fram informationssäkerhetskrav inför upphandling av IT-system och IT-tjänster samt personuppgifts-biträdesavtal inklusive instruktioner om personuppgifter behandlas. Det finns inga planer på att bygga fler serverhallar.	

Tabell 1 - Uppföljning av rekommendationer från granskningen av informationssäkerhet 2019.

Uppföljningen visar att Regionstyrelsen till viss del har genomfört åtgärder för att möta ett antal av de rekommendationer som gavs vid föregående granskning. Ett LIS har upprättats på central nivå inom regionen och en virtuell informationssäkerhetsorganisation har etablerats. Det kvarstår ännu arbete med att implementera LIS fullt ut i verksamheten. För ett flertal av rekommendationerna har Regionstyrelsen inte vidtagit åtgärder. Det saknas ännu ett aggregerat riskregister med regionövergripande informationssäkerhetsrisker och vid tidpunkten för granskningens genomförande saknas möjlighet att systematiskt följa upp utbildningsverksamheten. Det finns ett pågående arbete inom ett antal av rekommendationerna vilket medför att dessa bedöms som delvis åtgärdade. Detta innefattar bland annat att verksamheterna undviker att arbeta i stuprör för att reducera personberoendet, implementering av den nya lärplattformen, Kompass, samt pågående arbete med att införa ett IGA-verktyg. Rekommendationen avseende säkerhetsskyddsanalys har inte gått att bedöma då den säkerhetsskyddsanalys som fastställts av Regionstyrelsen är säkerhetsklassad.

6. Övergripande bedömning

Detta avsnitt besvarar syftet med granskningen som är att bedöma om tillräckliga åtgärder vidtagits utifrån 2019 års granskning samt om det finns en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter. Granskningen avser Regionstyrelsen utifrån sitt övergripande ansvar för regionens informationssäkerhetsarbete. Granskningen av skyddade personuppgifter avser även

Hälso- och sjukvårdsnämnden som har vårdgivaransvaret för all drift av hälso- och sjukvård och tandvård i egen regi. Nämnden ansvarar för att verksamheten inom nämndens ansvarsområde bedrivs i enlighet med anvisningar och direktiv från Regionstyrelsen.

Helseplans samlade bedömning är att Regionstyrelsen inte säkerställt en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter och informationssäkerhet. Ett LIS har upprättats och en virtuell informationssäkerhets-organisation har etablerats. Inom ramen för LIS finns styrande dokument som redogör för riktlinjer och rutiner kring informationssäkerhet och skyddade personuppgifter. Däremot har Regionstyrelsen inte utifrån sitt övergripande ansvar för informations-säkerhet säkerställt att det finns strukturer för uppföljning av att rutinerna för skyddade personuppgifter efterlevs.

Helseplan bedömer att tillräckliga åtgärder inte vidtagits utifrån 2019 års granskning. Regionen har upprättat ett LIS på central nivå och en virtuell informationssäkerhetsorganisation har etablerats vilket skapar förutsättningar för regionens fortsatta informationssäkerhetsarbete. Därtill har även en riktlinje för säkerhetsskyddsanalys fastställts. För ett flertal av rekommendationerna bedömer Helseplan att åtgärder delvis vidtagits eller att åtgärder inte vidtagits utifrån rekommendationerna från föregående granskning.

Helseplans samlade bedömning är att Hälso- och sjukvårdsnämnden utifrån sitt vårdgivaransvar inte har säkerställt en tillräcklig intern styrning och kontroll för hanteringen av skyddade personuppgifter i de verksamheter som ingår i nämndens uppdrag. Det finns en regiongemensam rutin för skyddade personuppgifter men däremot saknas styrande dokument för att tillse att det sker en tillräcklig uppföljning av att rutinerna efterlevs. Av granskningen framkommer att det även saknas rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter.

Korrigerbar signatur

X

Ulrike Deppert
Projektledare, Helseplan Consulting Group AB
Signerat av: 4a83dc0d-14a6-4001-adbb-d0211d97188f

7. Bilagor

7.1. Bilaga 1 – Granskade dokument

- Patientsäkerhetsberättelse för Region Västernorrland (2022)
- Protokoll Regionstyrelsen 2023-06-07
- Riktlinje Styrdokument (reviderat 2022)
- Riktlinje Informationssäkerhet (2020)
- Riktlinje Informationssäkerhet, organisation av (2020)
- Riktlinje Organisation av informationssäkerhet – rollbeskrivning (reviderat 2021)
- Rutin Skyddade personuppgifter (regiongemensamt) (reviderat 2022)
- Rutin Hantering av post till personer med skyddade personuppgifter (reviderat 2022)
- Rutin Hantering av personer med skyddad identitet – BUP (reviderat 2023)
- Rutin för hantering av känslig grunddata samt skyddad personuppgift i Heroma (2017)
- Regionstyrelsens protokoll (2021-06-10)
- Riktlinje Skyddade personuppgifter (Hälsocentralen Bjästa) (reviderat 2023)
- Riktlinjen Efterlevnad-hantering av efterlevnad för informationssäkerhet (reviderat 2021)
- Riktlinje Efterlevnad – rapportering av informationssäkerhet (reviderat 2021)
- Riktlinje för Säkerhetsskydd i Region Västernorrland (2021)
- Utvärdering Grundutbildning skyddade personuppgifter 4 december 2019

7.2. Bilaga 2 – Intervjuförteckning

Funktion, Organisation
Ordförande, Regionstyrelsen
1:e vice ordförande, Regionstyrelsen
Ordförande, Hälso- och sjukvårdsnämnden
1:e vice ordförande, Hälso- och sjukvårdsnämnden
Regiondirektör
HR-direktör
Samordningsdirektör
Informationssäkerhetsansvarig och tillika informationssäkerhetsstrateg
IT-säkerhetsansvarig och dataskyddsombud
Verksamhetschef, Regionledningsförvaltningens kansli
Enhetschef, Systemförvaltning kärnverksamhet
Objektledare, Administration och kommunikation

Objektspecialist HR
Enhetschef Löneservice
Systemspecialist
Chefläkare
IT-tekniker