Regionens revisorer
Hans Strandlund

2022-10-12

Till
Regionstyrelsen för svar
Regionfullmäktige för kännedom

Uppföljande och fortsatt granskning av informationssäkerhet och GDPR

PwC har på uppdrag av Region Västmanlands revisorer genomfört en uppföljning och fortsatt granskning av informationssäkerhet och GDPR. Granskningen syftar till att bedöma om regionstyrelsen har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.

Vi bedömer sammantaget att regionstyrelsen inte helt har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats. Vidare bedömer vi att regionstyrelsen ej har säkerställt en ändamålsenlig personuppgiftshantering.

Utifrån vår uppföljning av tidigare granskning rekommenderas regionstyrelsen att säkerställa att:

- Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2, SSO:n, uppdateras och förtydligar Informationsäkerhetsrådets syfte och ansvar.
- Tydliggöra kopplingen mellan ansvar och roll, exempelvis för informationssäkerhetssamordnaren och informationssäkerhetsstrategen.
- Förtydliga ansvar och roller i PM3-modellen kopplat till säkerhetsåtgärder som riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser.
- Intensifiera planen med att införa obligatoriska, regelbundna utbildningsmoment för samtliga medarbetare inom regionen. I sammanhanget bör rutin tas fram för att säkerställa genomförande av framtagna utbildningar.
- Genomföra projekt med målsättningen att förbättra behörighetshantering i journalsystemet. Fokusområden bör vara genomförande av riskanalys vid behörighetstilldelning, tydliggöra gallringsrutiner samt säkerställa godtagbar följsamhet av interna rutiner inkluderat kontinuerliga stickprov i patientjournalsystemet.
- Verksamhetsplan 2022 blir en formellt beslutad verksamhetsplan och att planerade aktiviteter är budgeterade.
- Metoder och riktlinjer för upphandlingsprocessen tas fram.

Gällande Region Västmanlands arbete med GDPR rekommenderar vi regionstyrelsen att säkerställa att:

- Framtagna riktlinjer och policies är uppdaterade och att kontinuerlig revidering införs, samt tydlig märkning med datum vilket kommer skapa en tydlighet för medarbetare och öka spårbarhet av ändringar.
- Utforma fler riktlinjer kopplat till GDPR, exempelvis rutin för konsekvensbedömning, för att standardisera regionens arbetssätt.
- Tydliggöra hur organisationen ska ta del av styrdokumentationen kring GDPR.

Region Västmanlands revisorer
c/o PwC
Box 885
721 23 VÄSTERÅS
Telefon: 010-212 61 18

- Prioritera utbildningsinsatser kring dataskydd.
- Framtagande av en registerförteckning av personuppgiftsbehandlingar genomförs.
- Det utses lokalt ansvariga inom förvaltningarna för dataskyddsfrågor, t.ex. i form av en roll som dataskyddssamordnare, eller tydliggöra för verksamhetschefer om vilket ansvar de faktiskt har över sina förvaltningar då denna insikt är låg i dagsläget.
- En systematisk internkontroll av verksamheternas dataskyddsarbete återstartas så snart som möjligt.

Iakttagelser i sin helhet framgår i bifogad rapport som har godkänts vid revisorernas sammanträde 2022-10-12. Revisorerna översänder rapporten till regionstyrelsen och önskar svar senast 2023-01-11.

FÖR REGIONENS REVISORER

Hans Strandlund
Ordförande

Elisabeth Löf
Revisor

Uppföljande och fortsatt granskning av informationssäkerhet och GDPR

Region Västmanland

September 2022

Marie Lindblad, certifierad kommunal revisor

Nur Nauti

Elinore Silander Hammarin

Carl Nisser

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av Region Västmanlands revisorer genomfört en uppföljning och fortsatt granskning av informationssäkerhet och GDPR. Granskningen syftar till att bedöma om regionstyrelsen har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.

Vi bedömer sammantaget att regionstyrelsen **inte helt** har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats. Vidare bedömer vi att regionstyrelsen **ej** har säkerställt en ändamålsenlig personuppgiftshantering.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet “Sammanfattande bedömningar utifrån revisionsfrågor”.

Revisionsfrågor	**Bedömning**
Har regionstyrelsen vidtagit aktiva åtgärder för att åtgärda de tidigare identifierade bristerna, och beaktat de tolv rekommendationerna i rapporten från 2019?	Delvis 
Är regionstyrelsens policy och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?	Delvis 
Har regionstyrelsen ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?	Ej uppfylld 

Rekommendationer redovisas i slutet av rapporten.

Innehållsförteckning

Sammanfattning	1
Inledning	3
Bakgrund	3
Syfte och revisionsfrågor	4
Revisionskriterier	4
Avgränsning	4
Metod	4
Granskningsresultat	6
Åtgärder utifrån tidigare identifierade brister	6
Iakttagelser	6
Bedömning	12
Styrning avseende GDPR	14
Iakttagelser	14
Bedömning	16
Kontroll och uppföljning av GDPR	17
Iakttagelser	17
Bedömning	18
Samlad bedömning	19
Rekommendationer	19
Sammanfattande bedömningar utifrån revisionsfrågor	21
Bilagor	21

Inledning

Bakgrund

Vår tids nya teknik är digitalisering och den behöver användas i effektiviseringens syfte. Digitalisering är ett globalt fenomen och för regionerna innebär det att allt fler aktiviteter inom verksamheten i olika grad är beroende av informationssystem. Information ska inte bara vara tillgänglig utan lika viktigt är att den håller rätt kvalitet och kan hanteras utan att känsliga uppgifter förändras eller sprids till obehöriga. Det medför att både information i sig och de system som används för att förvara och överföra information behöver skyddas. För att skapa en informationssäkerhet som motsvarar verksamhetens behov ställs krav på organisatorisk styrning och kontroll.

Inom just IT- och informationssäkerhet gjordes det för Region Västmanland mellan 2016-2018 ett flertal granskningar där flera brister uppmärksammades:

- Teknisk IT-granskning (2016)
- Granskning av informationssäkerhet (2017)
- Granskning av säkerhet i patientsystemet och hantering av patientjournaler (2018)

2019 gjordes det en uppföljande granskning av hanteringen av bristerna som upptäcktes 2016-2018 samt hur informationssäkerhetsarbetet har utvecklats inom regionen. I den granskningen framkom det att en rad utvecklingsområden fanns kvar - framförallt kopplat till ledningssystemets utformning.

Rapporten 2019 utmynnade i följande rekommendationer:

1. Region Västmanland bör se över åtgärdsmålen i ISO/IEC 27001 för att säkerställa att regionen täcker samtliga för att i framtiden kunna vara certifieringsbara.
2. Säkerställ att styrande dokument är reviderade med lämplig intervall samt att informationssäkerhetspolicyn och riktlinjerna följs upp regelbundet.
3. Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten.
4. Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur.
5. Ett fortsatt arbete gällande riktlinjerna generellt behöver ses över.
6. Region Västmanland bör utforma metoder och riktlinjer kring incidenthantering och informationssäkerhet i upphandling.
7. Inkludera informationssäkerhetsarbetet i regionens framtida plan och budget.
8. Specificera och kommunicera ut tydliga roller och ansvar för säkerhetsåtgärder i verksamheten.
9. Ta fram styrdokument och processer för kravställning mot informationssäkerhetsarbetet.
10. Gör e-utbildningen obligatoriskt för att säkerställa att alla medarbetare genomgår den. Se även till att ha regelbundna utbildningstillfällen och inte enbart vid nyanställning

11. Region Västmanland bör göra uppföljning av riskanalyser för behörighetstilldelning samt ta fram gallringsrutiner gällande behörighetssystemet. Regionen bör även se över kontinuerliga stickprov i patientjournalsystemet.
12. Region Västmanlands lösenordspolicy bör stärkas.

Revisorerna har utifrån sin bedömning av risk och väsentlighet beslutat att följa upp den senaste granskningen samt att även granska om regionen arbetar på ett ändamålsenligt sätt med sin personuppgiftshantering (GDPR).

Syfte och revisionsfrågor

Granskningen syftar till att bedöma om regionstyrelsen har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.
Revisionsfrågor:

- Har regionstyrelsen vidtagit aktiva åtgärder för att åtgärda de tidigare identifierade bristerna, och beaktat de tolv rekommendationerna i rapporten från 2019?
- Är regionstyrelsens policy och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har regionstyrelsen ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

- ISO/IEC 27001
- GDPR
- Regionens regler, policys och riktlinjer för informationssäkerhet

Avgränsning

Granskningen kommer delvis fokusera på identifierade brister i regionens informationssäkerhetsarbete och uppföljning av tidigare rekommendationer för att bedöma nuläget, samt delvis granska ändamålsenlighet rörande personuppgiftshantering. Revisionsobjekt är regionstyrelsen.

Metod

Granskningen har skett genom

- dokumentstudier (exempelvis av styrande dokument och dokumenterade uppföljningar) samt stickprov av utvalda förvaltningar inom Region Västmanland.
- intervjuer och mailkontakter med relevanta tjänstepersoner (för att följa upp hur de tidigare rekommendationerna har hanterats)
- totalt sju intervjuer med elva tjänstepersoner från både central nivå och inom olika förvaltningar.
    - mot bakgrund av den första revisionsfrågan hölls fyra intervjuer med fem personer från; verksamheten Juridik och Säkerhet inom Förvaltning

Regionkontoret, Förvaltning för digitaliseringsstöd, FDS, samt verksamheten IT-drift och -förvaltning inom FDS.

    - mot bakgrund av de två revisionsfrågorna gällande GDPR hölls tre intervjuer med sex personer från tre verksamheter;
        - Regionkontoret;
        - Centrum för HR, vilket är en verksamhet inom Regionkontoret;
        - Vuxenpsykiatrin, vilket är en verksamhet inom Hälso- och sjukvårdsförvaltningen.
- Dokumentgranskning samt stickprov avseende GDPR-delen i granskningen sker i tre olika verksamheter; Regionkontoret; Centrum för HR, vilket är en verksamhet inom Regionkontoret; och Vuxenpsykiatrin, vilket är en verksamhet inom Hälso- och sjukvårdsförvaltningen.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Åtgärder utifrån tidigare identifierade brister

Revisionsfråga 1: Har regionstyrelsen vidtagit aktiva åtgärder för att åtgärda de tidigare identifierade bristerna, och beaktat de tolv rekommendationerna i rapporten från 2019?

Iakttagelser

I Region Västmanland finns en organisation för systematiskt säkerhetsarbete vilken är dokumenterad i *Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2* (2017). Syftet med säkerhetsorganisationen är att genom samordning och helhetssyn skapa en struktur och kultur som stödjer styrning och uppföljning av regionens systematiska säkerhetsarbete. Säkerhetsorganisationen, SSO, består av en Riskkommité med strategiskt ansvar och är ett beslutande organ som exempelvis kan besluta om förslag till åtgärder, planer och policys samt finansieringsprinciper för att genomföra beslutade åtgärder. Vidare finns ett Riskråd vilket är beredande till Riskkommittén samt Informationssäkerhetsrådet, Rådet för allmän säkerhet och Kris- och katastrofmedicinska rådet. Syftet med informationssäkerhetsrådet är att verka för att Region Västmanland upprätthåller rätt säkerhet för sin information med hänsyn till krav om konfidentialitet, riktighet, tillgänglighet och spårbarhet. Arbetet utgår från den verksamhetsstyrning som sker genom informationssäkerhetspolicy och riktlinjer i ledningssystemet.

Förvaltningen för digitaliseringsstöd, FDS, tillsammans med enheten Juridik och säkerhet inom förvaltningen Regionkontoret är drivande och ett stöd i arbetet med informationssäkerhet för Region Västmanlands förvaltningar.

I intervju beskrivs att informationssäkerhetsstrategen, tillika dataskyddsombud, tillhör Juridik och Säkerhet och ansvarar för att stödja regionens linjeverksamheter i dess implementering och följsamhet av informationssäkerhet och GDPR, därtill ansvarig för samtliga dataskyddsfrågor och styrning samt analyser av hur regionen ska arbeta med dem samma. Vid intervju redovisas att organisationen ska kompletteras med en informationssäkerhetssamordnare i närtid.

I denna sammanställning av rekommendationerna kommer vi att vid flertalet tillfällen återkomma till att regionen har under stor del av tiden som förlöpt sedan 2019 hanterat en pandemi och det primära fokuset har varit att kunna ha igång regionens alla verksamheter och de aktuella rekommendationer har således prioriterats ned.

1.1 Region Västmanland bör se över åtgärdsmålen i ISO/IEC 27001 för att säkerställa att regionen täcker samtliga för att i framtiden kunna vara certifieringsbara.

I granskningen som gjordes 2019 var 130 av 140 kontroller genomförda, vilka finns dokumenterade i en excelfil. I intervju beskrivs att det pågår aktiviteter inom regionen för att leva upp till en ISO-certifiering men det saknas uppföljning huruvida dessa kontroller

efterlevs och det finns ett behov av en göra en ny gapanalys för att ta reda på var regionen befinner sig idag. Vidare har pandemin tvingat regionen att nedprioritera dessa aktiviteter. I *Verksamhetsplan 2022* beskrivs gapanalys som en aktivitet som ej genomfördes 2021 och flyttas till 2022.

1.2 Säkerställ att styrande dokument är reviderade med lämplig intervall samt att informationssäkerhetspolicyn och riktlinjerna följs upp regelbundet.
I ett förtydligande från regionen beskrivs att revidering av styrande dokument sker av den funktion som är utsedd ägare, detta görs i regionens ledningssystem Centuri. Inom informationssäkerhetsområdet finns det olika ägare beroende på dokumentets natur, informationssäkerhetsstrategen och regionjuristen är exempelvis ägare av flertalet riktlinjer. Styrande dokument av teknisk karaktär ägs oftast av en funktion inom FDS, av en verksamhetschef eller en enhetschef. Vidare beskrivs att varje styrande dokument taggas med ett intervall om hur ofta de behöver revideras. I en intervju framkommer att uppdatering av styrande dokument är pausad sedan 2020, dels med anledning av pandemin, dels för att rollen informationssäkerhetsstrateg var vakant under ett års tid innan den återigen tillsattes 2021. Vilket kan förklara varför en del av de styrande dokument som har skickats in för denna granskning är senast reviderade någon gång mellan 2017-2019. Däribland Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2 och Informationssäkerhetspolicyn.

I *Informationssäkerhetspoliyn* fastställs att Regiondirektören och chefer ansvarar för framtagande av rutiner och instruktioner för den egna verksamheten. Likaså fastställs att uppföljning gällande informationssäkerhet regelbundet ska genomföras med interna kontroller och revisioner av oberoende part. Den enda uppföljning och revision som vi kunnat identifiera är den revisionsrapport (*Revisionsrapport informationssäkerhet)* som de förtroendevalda revisorerna beställt för år 2019. Någon av regionen identifierad intern uppföljning har inte kunnat verifieras förutom *Verksamhetsrapport för informationssäkerhet* samt ledningens genomgång, vilka beskrivs närmare under nästa fråga, 1.3.

1.3. Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten.
I Region Västmanland utgörs systematisk dokumentation av *Verksamhetsplan 2022*, *Verksamhetsrapport för informationssäkerhet* och *protokoll från ledningens genomgång. Verksamhetsplan 2022* beskriver varje planerad aktivitet utifrån fokusområde, syfte/mål, aktivitet, prioritering och status av aktuell åtgärd. Verksamhetsplan 2022 saknar beslutandedatum och vad för typ dokumentet är, under intervju förklaras att dokumentet är att betraktas som ett informellt arbetsdokument.

I *Verksamhetsrapport för informationssäkerhet* sammanfattas årets genomförda och icke genomförda informationssäkerhetsåtgärder och överlämnas därmed till regionstyrelsen. Rapporten omfattar bl.a. riskanalyser, informationsinsatser, inköp, dataskydd och cybersäkerhet, registerförteckning och konsekvensbedömning, incidenter, logguppföljning och omvärldsbevakning.

I forumet *Ledningens genomgång*, får koncernledningen en muntlig föredragning av informationssäkerhetsarbetet . I ett granskat protokoll från ledningens genomgång finns bl.a. grad av måluppfyllelse dokumenterat; uppfyllt; delvis uppfyllt; ej uppfyllt, resultat av internrevisioner, avvikelserapportering och förslag på förbättringsområden. Ledningens genomgång genomförs årligen.

1.4. Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur.
I PwCs rapport från 2019 omskrivs ett dokument som heter *Verksamhetsplan informationssäkerhet 2019.* I mailkonversation bekräftas att Verksamhetsplan 2022 motsvarar samma typ av verksamhetsplan med samma syfte. Som nämns ovan beskriver *Verksamhetsplan 2022* varje planerad aktivitet men är inte ett formellt beslutat dokument.

1.5. Ett fortsatt arbete gällande riktlinjerna generellt behöver ses över.
I intervju framkom att SSO:n bidrar till goda förutsättningar att generellt se över riktlinjer, men att arbetet inte levt upp till önskad framfart. I intervju med medarbetare från FDS samt Juridik och Säkerhet, Regionkontoret, anges framförallt två skäl som förklaring. Dels under 2020 och 2021 har en pandemi tvingat Region Västmanland att omprioritera stora delar av sin verksamhet och att “generellt se över riktlinjer” har nedprioriterats. Dels att endast en informationssäkerhetsstrateg är en för liten resurs i förhållande till vad som förväntas ingå i rollens ansvar.

1.6. Region Västmanland bör utforma metoder och riktlinjer kring incidenthantering och informationssäkerhet i upphandling.

1.6.1 Metoder och riktlinjer kring incidenthantering
I *Instruktion för IT-chef i beredskap Förvaltningen för digitaliseringsstöd* från 3 januari 2022 framkommer att IT-chef beredskap ansvarar för uppkomna incidenter. I intervju beskrivs att incidenter hanteras enligt en metod som bygger på ITIL-processer. ITIL är bland annat en incidenthanteringsprocess med tydligt definierade steg, från att en incident upptäcks till hur den ska hanteras och till sist avslutas. Vilket kan styrkas med nedan riktlinjer och instruktioner för incidenthantering:

- Riktlinjen Incidenthantering (51316_1). En riktlinje för incidentrapportering, incidenthantering (ink bevissäkring, återställning och uppföljning)
- Instruktionen Incidenthantering inom Förvaltningen för digitaliseringsstöd och Rutin vid allvarlig händelse - Förvaltningen för digitaliseringsstöd. (Som allvarlig händelse räknas enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten och informationssäkerheten) för när en It-relaterad informationssäkerhetsincident såväl som för personuppgiftsincidenter.
- Instruktion för IT-chef i beredskap Förvaltningen för digitaliseringsstöd (2022).
- Mall IT-incidentrapport FOA (2022), en mall för hur en IT-incidentrapport ska upprättas inom förvaltningsobjekten.
- It-säkerhet i drift och förvaltning (2018).

Det finns två roller/funktioner för en dygnet-runt-hantering av it-relaterade informationssäkerhetsincidenter, en it-chef i beredskap, CiB, samt en tjänsteman i beredskap, TiB. Dessa ansvarar även för att rapportera en inträffad incident till Riskrådet inom SSO:n. Utöver det finns en incident manager som är ansvarig att utveckla processer för incidenthantering.

Utöver ovan nämnda dokument har en målbild tagits fram för hur ett mer aktivt och proaktivt arbete ska bedrivas för att upptäcka och hantera dataintrång och informationsläckage. I dokumentet *IT-säkerhet målbild* sammanfattas planerade aktiviteter för 2021-2023 för en SIEM-funktion[1] och en SOC-funktion[2]

1.6.2 Metoder och riktlinjer kring informationssäkerhet i upphandling
Under 2021 har Region Västmanland tillsammans med Region Sörmland och inköpsenheten (som bistår båda regionerna) tagit fram en arbetsprocess till vilken dokumentet *Lösningsbeskrivning* används som en mall för processen, samt stödmaterialet *Skyddsnivåer Kravkatalog* för att säkerställa att it-säkerhetskrav beaktas i anskaffningsprocessen. I intervju förklaras att samtliga inköpare har fått utbildning i informationssäkerhet och personuppgiftsbiträdesavtal, vilket bekräftas av granskat utbildningsmaterial *För inköp.* Vidare beskrivs att upphandlingsfunktionen anses som en gatekeeper-funktion och inget ska kunna passera den funktionen utan att informationssäkerhet har beaktats i varje enskild upphandling. Lösningsbeskrivningen är ej antagen som en formell riktlinje utan är snarare ett metodstöd och en mall.

Lösningsbeskrivning består av bl.a. verksamhetanalys, kravanalys och lösningsförslag. Verksamhetsanalys inkluderar beskrivning av information som systemet kommer att hålla, informationsklassificiering samt riskanalys. Kravanalys tar sikte på både funktionella och icke funktionella krav, ett icke funktionellt krav är exempelvis systemets tillgänglighet. Vidare beskrivs tekniska krav i lösningsförslag. I intervju beskrivs att regionens informationssäkerhetsstrateg samt medarbetare från FDS, IT-drift och IT-förvaltning, är förvaltningarna behjälpliga för att samtliga kravområden ska kunna genomföras med rätt kompetens.

För att en upphandlingsprocess ska initieras behöver arbetsprocessen bestående av *Lösningsbeskrivning* samt *Skyddsnivåer kravkatalog* behandlas samt vara genomförd. Dock saknas dokumenterade riktlinjer för en upphandlingsprocess.

I intervju beskrivs att informationssäkerhetsstrategen, tillika dataskyddssamordnaren, ansvarar för alla personuppgiftsbiträdesavtal, pub-avtal, som har blivit påskrivna de senaste året. Under intervju klargjordes att medvetenhet finns hos enskilda medarbetare om att detta innebär en stor risk att avtalen inte hinner följas upp inom rimliga tidsintervaller och kan orsaka regionen skada om leverantören inte följer pub-avtalet.

[1] Security Incident Event Management, ett set av it-system som tillsammans övervakar och analyserar loggad data för att upptäcka avvikelser och på så sätt förebygga incidenter.
[2] Security Operations Center, är en benämning av en sammansättning av roller, processer och teknologier för att hantera incidenter.

I intervju beskrivs att upphandling kring ett IT-system idag går relativt smärtfritt men det är en desto större utmaning när det kommer till medicinsk utrustning som drivs av ett it-system p.g.a mer komplexa frågeställningar att ta hänsyn till.

1.7. Inkludera informationssäkerhetsarbetet i regionens framtida plan och budget.
I intervju beskrivs att i nuläget finns ingen separat budget som är öronmärkt för just informationssäkerhet men att de aktiviteter som är kopplade till informationssäkerhet inom respektive verksamhet, t.ex. informationssäkerhetsutbildning, budgeteras i verksamhetens totala budget. Varje verksamhet ansvarar för att implementera planerade informationssäkerhetsaktiviteter med stöd från informationssäkerhetsstrategen. *Verksamhetsplan 2022* är ett informellt dokument som beskriver regionens informationssäkerhetsarbete men vi har inte kunnat verifiera på vilket sätt dessa aktiviteter budgeteras.

1.8. Specificera och kommunicera ut tydliga roller och ansvar för säkerhetsåtgärder i verksamheten.
I styrdokumentet *Region Västmanlands Organisation för systematiskt säkerhetsarbete*, SSO, beskrivs syftet med SSO:n vilket är att genom samordning och helhetssyn skapa en struktur och kultur som stödjer styrning och uppföljning av regionens systematiska säkerhetsarbete. Exempel på övergripande mål är att SSO:n ska stödja förvaltningar och verksamheter i framtagandet av bland annat riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser. Dock saknas en dokumenterad rollbeskrivning i vilken dessa ansvar tilldelas. Ytterligare en notering är att styrdokumentet innehåller utdaterade förkortningar för förvaltningar som har bytt namn eller slagits ihop.

Jämte SSO:n finns även systemförvaltarmodellen PM3, och i *FOA Region Västmanland* (FOA, Förvaltningsobjektarkitektur), beskrivs objektroller[3] och ansvar i förhållande till regionens systemförvaltarobjekt. Syftet är att underlätta strategiska beslut för förvaltning och vidareutveckling av regionens IT-stöd. Däremot saknas återigen dokumenterat ansvar för säkerhetsåtgärder som riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser. I intervju förklaras att FDS och informationssäkerhetsstrategen är förvaltningarna behjälpliga i ovan nämnda analyser.

I *Informationssäkerhetspolicyn* beskrivs att informationsäkerhetssamordnaren ansvarar för samordning och utveckling av informationssäkerhetsarbetet men i intervju förklaras att informationssäkerhetsstrategen bär det ansvaret. Rollen som informationssäkerhetsstrateg och dataskyddssamordnare innehas, vid tiden för granskningen, av samma person. I rollen som dataskyddsombud ingår ansvar för samtliga dataskyddsfrågor, exempelvis behörighetstilldelning och styrning samt analyser av hur regionen ska arbeta med dem, i detta ingår även genomförande av loggranskning

[3] I PM3-modellen finns fördefinierade roller för systemförvaltning: Objektägare, Objektägare IT, Förvaltningsledare och Förvaltningsledare IT.

i utvalda system kopplade till Loggkoll, samt hur de ska arbeta med sekretessuppgifter. Därtill ingår ansvar för regionens samtliga personuppgiftbiträdesavtal för leverantörer.

1.9. Ta fram styrdokument och processer för kravställning mot informationssäkerhetsarbetet.
På en övergripande och styrande nivå finns styrdokumentet *Region Västmanlands Organisation för systematiskt säkerhetsarbete.* Där beskrivs att SSO:ns övergripande mål är att stödja förvaltningar och verksamheter i framtagandet av bland annat riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser vilket i sin tur kan användas som kravställning i informationssäkerhetsarbetet. Däremot saknas dokumenterade processer hur detta förverkligas och i intervju påtalas att det saknas processer för kravställning mot säkerhetsarbetet.

1.10. Gör e-utbildningen obligatorisk för att säkerställa att alla medarbetare genomgår den. Se även till att ha regelbundna utbildningstillfällen och inte enbart vid nyanställning.
Under intervju framkom att e-utbildningen för informationssäkerhet är obligatorisk. Däremot påtalas att befintligt utbildningsmaterial är till viss del utdaterat. Vid stickprovskontroll som genomfördes under granskningen identifierades dock att enbart 245 av ca 1045 personer genomgått utbildningen mellan 1 januari och 20 juni 2022. Då 2022 inte är över har vi under granskningen inte kunnat verifiera huruvida regionen kan säkerställa att alla medarbetare genomför utbildningen.

Det framkom under intervjuer att informationssäkerhetsrådet inom SSO:n planerar att ta fram uppdaterad utbildning samt påtala och uppmana samtliga anställda att genomföra befintlig e-utbildning. Utöver den obligatoriska e-utbildningen genomförs kompetenshöjande åtgärder, ett urval av dessa aktiviteter är informationskampanjer, vilka skickas ut av Juridik och Säkerhet samt FDS och syftar till att bland annat medvetandegöra ett säkrare beteende på internet. Vidare har lösenordsveckor genomförts med tillhörande quiz samt att informationssäkerhetsstrategen har varit på arbetsplatsträffar (APT) i flertalet förvaltningar och utbildat medarbetare inom ramen för dataskyddsförordningen.

1.11. Region Västmanland bör göra uppföljning av riskanalyser för behörighetstilldelning samt ta fram gallringsrutiner gällande behörighetssystemet. Regionen bör även se över kontinuerliga stickprov i patientjournalsystemet.
Från tidigare granskning har regionen arbetet vidare med att utforma dokument "Beställning av Cosmicbehörigheter i HSA-användarmanualer" i vilket det framgår att tilldelning av behörigheter sker utifrån medarbetarens yrkesroll i verksamheten. Objektägare tillsammans med verksamheten definierar grundbehörigheter utifrån arbetsbeskrivningar. I intervjuer framkom att det är respektive verksamhetschef som ska genomföra en riskbedömning avseende vilken behörighet respektive medarbetare ska få

i enlighet med deras yrkesroll. På uppdrag av verksamhetschefen ansvara sedan HSA-redaktören för att rätt behörighet tilldelas.

Det framkom i intervjuer att region västmanland under hösten 2021 har genomfört en förstudie med syfte att skapa en aktuell bild av regionens följsamhet till gällande lagkrav för hantering av behörigheter i journalsystemet inkluderat stickprovskontroller. Genomförda stickprovskontroller har påvisat brister i följsamhet av regionens interna rutiner. Mot bakgrund av detta har regionen beslutat att initiera ett projekt med målsättning att förbättra behörighetshanteringen i journalsystemet. Syftet med projektet är att Region Västmanland utifrån gällande lagstiftning säkerställer åtkomst till journalinformation med bibehållen hög patientsäkerhet. Uttalade effektmål med projektet förväntas vara att förbättra följsamhet till gällande lagkrav samt upprätta en godtagbar följsamhet till interna rutiner med hänsyn till behörighetstilldelning, riskanalys samt gallringsrutiner. Beslut om projektets etableringsfas ska startas sker 1 september 2022 för vidare beslut för genomförande av projekt 1 oktober 2022.

1.12. Region Västmanlands lösenordspolicy bör stärkas.
Vi noterar under granskningen att Region Västmanland i rutin “Informationssäkerhet för medarbetare” stipulerat vilka krav på lösenord som är gällande. Lösenord för att logga in på regionens domän ska vara minst tio tecken långt samt innehålla krav på komplexitet. Vidare framkommer att krav på lösenord för att logga in till olika system eller tjänster beslutas av respektive objektägare med utgångspunkt från informationsklassificering och känsligheten av den information som hanteras i systemet eller tjänsten. Detta innebär att det beroende på klassificering för vissa system och tjänster kan förekomma hårdare lösenordskrav än de som riktlinjen anger. Slutligen beskrivs i intervjuer att Region Västmanland inom Office 365 infört teknisk funktionalitet i syfte att begränsa möjligheten för användare att använda enkla lösenord såsom exempelvis “vinter 2021”. Som en del i arbetet med att stärka lösenordspolicyn har samtlig personal inom IT-avdelningen med höga behörigheter som ger tillgång till infrastrukturkomponenter alltid multifaktorautentisering (MFA) påslagen.

Bedömning
Har regionstyrelsen vidtagit aktiva åtgärder för att åtgärda de tidigare identifierade bristerna, och beaktat de tolv rekommendationerna i rapporten från 2019?

Delvis

Tidigare rekommendation	Vår bedömning nu
1.1 Region Västmanland bör se över åtgärdsmålen i ISO/IEC 27001 för att säkerställa att regionen täcker samtliga för att i framtiden kunna vara certifieringsbara.	
1.2 Säkerställ att styrande dokument är reviderade och med lämpligt intervall samt att informationssäkerhetspolicyn och riktlinjerna följs upp regelbundet.	

1.3 Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten.	
1.4. Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur.	
1.5. Ett fortsatt arbete gällande riktlinjerna generellt behöver ses över.	
1.6. Region Västmanland bör utforma metoder och riktlinjer kring incidenthantering och informationssäkerhet i upphandling.	
1.7. Inkludera informationssäkerhetsarbetet i regionens framtida plan och budget.	
1.8. Specificera och kommunicera ut tydliga roller och ansvar för säkerhetsåtgärder i verksamheten.	
1.9. Ta fram styrdokument och processer för kravställning mot informationssäkerhetsarbetet.	
1.10 Gör e-utbildningen obligatoriskt för att säkerställa att alla medarbetare genomgår den. Se även till att ha regelbundna utbildningstillfällen och inte enbart vid nyanställning	
1.11. Region Västmanland bör göra uppföljning av riskanalyser för behörighetstilldelning samt ta fram gallringsrutiner gällande behörighetssystemet. Regionen bör även se över kontinuerliga stickprov i patientjournalsystemet.	
1.12. Region Västmanlands lösenordspolicy bör stärkas.	

Vi bedömer att det finns en god struktur inom regionen att hantera säkerställandet av att styrande dokument revideras, men en del av de styrande dokument som har skickats in för denna granskning är senast reviderade någon gång mellan 2017-2019. Då *Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2* är från 2017 är en uppdatering och förtydligande av framförallt Informationsäkerhetsrådets syfte och ansvar aktuell.

Verksamhetsplan 2022 är vid tiden för granskningen ett informellt dokument men innehåller planerade aktiviteter kopplade till informationssäkerhet samt att främja en god säkerhetskultur. För att få helt godkänt på denna punkt anser vi att dokumentet behöver formaliseras och beslutas/fastställas.

Det finns en tydlig arbetsprocess inför upphandling däremot saknas tydliga metoder och riktlinjer för själva upphandlingsprocessen. En väl utförd och träffsäker arbetsprocess kan ses som en kvalitetssäkring att rätt krav ställs i upphandlingsprocessen.

I regionen budgeteras informationssäkerhetsarbete inom varje verksamhets budget. I *Verksamhetsplan 2022* där regionövergripande informationssäkerhetsarbete planeras har vi inte kunnat verifiera på vilket sätt dessa aktiviteter budgeteras. För att få godkänt bedömer vi att utöver att *Verksamhetsplan 2022* fastställs behöver den även få en tydlig koppling till årets budget.

Inom Regionen finns en medvetenhet at vikten att säkerställa och främja en säkerhetskultur inom befintligt informationssäkerhetsarbete. Den utbildning som lanserades under 2018 är numer obligatorisk men bedöms vara till viss del utdaterad. Främjandet av att säkerställa en god säkerhetskultur framkommer under intervjusvar, däremot saknas en dokumenterad systematisk genomförandeplan för hur utbildningar ska genomföras på regelbunden basis. Informationskampanjer för att öka medarbetarna medvetenhet om säkerhetsrisker där de själva kan utgöra den svagaste länken, exempelvis genom nätfiske kampanjer (phishing) genomförs och testas med quiz.

Likt tidigare granskning noteras att Region Västmanland har processer, rutiner samt verktyg implementerade för att säkerställa att medarbetare har rätt behörighetstilldelningar i patientjournalsystemet. Vidare har regionen arbetat fram och utformat dokumentation kring behörighetstilldelning och åtkomst till patientuppgifter. Däremot har det i regionens egna interna kontroller framkommit att följsamhet av processer och rutiner är bristfällig. Mot bakgrund i den förstudie som genomfördes under hösten 2021 har regionen beslutat att initiera ett projekt med målsättning att förbättra behörighetshanteringen i journalsystemet vilket i enlighet med PwC:s rekommendation inkluderar uppföljning av riskanalyser av behörighetstilldelning, tydliggörande av gallringsrutiner samt säkerställa godtagbar följsamhet samt genomförande av kontinuerliga stickprov i patientjournalsystemet. Vid tiden för granskningen var projektet beslutat men ej initierat. Skyddseffekt av projektet uppfylls först då projektmålen med tillhörande åtgärder är implementerade och efterlevs.

Styrning avseende GDPR

Revisionsfråga 2: Är regionstyrelsens policy och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?

Iakttagelser

Styrning

Under granskningen har det framkommit att en stor del av regionens arbete för att få styrning på arbetet med dataskydd har bestått av att ta fram lämplig dokumentation i form av policys och riktlinjer som organisationen förväntas följa. Av intervju har det framkommit att dessa dokument har tagits fram med regionens dataskyddsombud för att sedan fastställas hos Regionstyrelsen. De styrdokument som vi tagit del av gällande persondataskydd är:

- Behandling av personuppgifter (2019)
- Hantering av personuppgiftsincidenter (2019)
- Behörighetsbeställning i HSA (2021)
- Åtkomst till patientuppgift i journal (2020)
- Krav för åtkomst till uppgifter i regionens huvudjournalsystem (2020)
- Sekretess och tystnadsplikt i region Västmanland (2017)
- Utlämnande av journalanteckningar (2016)
- Loggranskning (2020)
- Loggkoll - genomförande av loggranskningar (2020)

Som nämnts har det för oss beskrivits att riktlinjerna uppställda ovan är framtagna av dataskyddsombudet och godkända av Regionstyrelsen, något som dock inte kan avläsas från själva dokumenten. Det framgår inte heller när dokumentationen reviderats senast, enbart datum för när respektive dokumentet tagits fram. Dokumentationen är i övrigt av god kvalitet och täcker till stor del vad anställda förväntas göra med hänvisning till dataskyddsförordningen i olika sammanhang. *Behandling av personuppgifter* fastställer en grund för vad personuppgifter är samt dataskyddsförordningens grundläggande principer, vilket kan liknas vid en GDPR-manual för anställda. Då regionen hanterar sjukvård finns det ett redan inarbetat arbetssätt att skydda personuppgifter vilket också återspeglas i riktlinjerna och utifrån svar i intervjuer med förvaltningarna för hur det dagliga arbetet sker vilket är positivt ur ett GDPR-perspektiv. Avsaknad av ett standardiserat arbetssätt där verksamheterna kan agera fristående har tydliggjorts i intervjuer där det framkommit att dataskyddsombudet fått ägna stor del av sin tid att stödja olika delar av organisationen att utföra konsekvensbedömningar och upprätta PuB-avtal på bekostnad av andra viktiga GDPR-relaterade insatser, exempelvis utbildning.

Vid intervjuer med två förvaltningar framkommer det att GDPR-material uppfattas som svårtillgängligt att hitta för både medarbetare och verksamhetschefer. Detta har lett till att förvaltningarna i praktiken själva tagit fram egna arbetssätt för att försöka uppfylla förordningens krav.

Både ledande personer inom förvaltningar och medarbetare måste själva till vardags söka upp relevant information kring dataskydd inom regionens ledningssystem vilket beskrivs som svårnavigerat. Ett resultat av detta är att vissa förvaltningar själva tagit fram egna interna rutiner just kring dataskydd utan insyn från dataskyddsombudet.

Register över behandling av personuppgifter
För att kunna arbeta systematiskt med att skydda personuppgifter krävs det att en kartläggning görs för att veta vilka personuppgiftsbehandlingar som görs vilket också är en av dataskyddsförordningen grundläggande krav på organisationer (artikel 30). Förvaltning för digitaliseringsstöd har påbörjat ett arbete att ta fram en registerförteckning men den är i dagsläget inte komplett över Region Västmanlands personuppgiftsbehandlingar vilket är en direkt avvikelse från förordningen. I intervju framkommer att regionen inser denna brist och att man avser åtgärda detta men att

andra aktiviteter har prioriterats. Av intervju framkommer att regionen har som ambition att utveckla ett centralt IT-stöd som ska integreras med regionen katalogsstruktur (Active Directory). IT-stödet kommer att användas till registerförteckning och konsekvensbedömningar och ska spegla regionens organisationsstruktur.

De registrerades rättigheter

Vi har även tagit del av regionens integritetspolicy som är en av förordningens grundläggande krav att ha framtaget i en organisation likt Region Västmanlands. En integritetspolicy beskriver hur organisationen hanterar olika kategorier av registrerades personuppgifter och vilka deras rättigheter är gällande hanteringen. Policyn granskades i slutet av april 2022 av oss. Vi identifierade ett antal brister - bland annat riktade sig policyn endast mot vårdtagare vilket enbart är en kategori av registrerade medan regionen även behandlar t.ex. anställdas personuppgifter. Det framgick inte heller vilka rättigheter registrerade hade och hur de drar tillbaka sitt samtycke till behandling. Under intervju med dataskyddsombud framkom det att en uppdaterad version av integritetspolicy fanns planerad att tas fram, något som också skett i maj 2022. Den nya policyn finns på regionens hemsida https://regionvastmanland.se/om-personuppgifter/ men har inte granskats i detalj då den tillkom i slutet av vår granskning.

Bedömning

Är regionstyrelsens policy och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?

Delvis.

Region Västmanland har tagit fram en grund när det gäller policies och rutiner för efterlevnad av GDPR som är god men som kan utvecklas för genomförande av nyckelaktiviteter. Exempelvis saknas rutiner för hur registerförteckning ska upprättas samt hur konsekvensbedömningar ska utföras. Avsaknad av tydliga rutiner ökar risken kopplat till regionens stora beroende till huvudsakligt dataskyddsombud då det i dagsläget enbart är den rollen som besitter kunskap om hur dessa aktiviteter ska genomföras.

Policies och rutiner saknar i dagsläget tydlig märkning om vem som fastställt dokumenten samt om eller när revidering har skett. Utan tydlig märkning går det inte att fastställa att Regionstyrelsen fastställt och beslutat om befintliga dokument med tillhörande arbetssätt. Detta påvisas även i granskningen då granskningen visar att förvaltningar tagit fram egna rutiner och arbetssätt som inte härrör från central dokumentation vilket ökar risken för bristande efterlevnad och följsamhet av centralt tillhandahållen dokumentation.

Då regionen saknar ett behandlingsregister över personuppgiftsbehandlingar tolkas regelefterlevnaden av dataskyddsförordningen som bristfällig. Det finns dock flertalet mallar framtagna för hur registret ska utformas vilka bygger på Sveriges Kommuner och Regioners (SKR) grundmall. Utestående arbete är att färdigställa arbetet genomgående för samtliga behandlingar.

Kontroll och uppföljning av GDPR

Revisionsfråga 3: Har regionstyrelsen ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

Iakttagelser

Roller och ansvar

För att kunna uppnå en god nivå av intern kontroll och uppföljning av en regions organisering av GDPR krävs en tydlig roll- och ansvarsfördelning att följa upp gentemot. Inom Region Västmanland har vi identifierat ett par nyckelroller relaterat till arbetet med dataskyddsförordningen. Den mest centrala rollen är regionens *Dataskyddsombud* (DSO). Inom regionen finns enbart ett registrerat dataskyddsombud vilket inkluderar de nämnder som är personuppgiftsansvariga och därmed utser eget dataskyddsombud. Dataskyddsombudet driver i huvudsak själv det regionövergripande GDPR-arbetet men fungerar även som ett sakkunnigt stöd åt verksamheterna. Detta inkluderar i dagsläget uppgifter såsom framtagande av registerförteckning av personuppgiftsbehandlingar, tecknande av PUB-avtal, konsekvensbedömningar, framtagande av ledningssystem, hantering av skyddade personuppgifter, driva utbildningsinsatser, samt ge allmän rådgivning åt förvaltningarna. Som stöd till dataskyddsombudet finns det en *Regionjurist* att rådfråga. Det framkom dock under intervju att denna resurs är nyanställd sedan september 2021 samt att denne inte är en dedikerad specialiserad resurs för enbart dataskyddsfrågor och genomgår en inskolningsperiod i organisationen.
Under intervjuer framgick det att säkerställandet av efterlevnad av GDPR är en verksamhetsfråga vilket innebär att *förvaltningarna har* ett stort ansvar att själva driva dataskyddsarbetet. Det saknas dock en tydlig befattning inom förvaltningarna idag som ansvarar för dataskyddsfrågor vilket innebär att frågan hamnar inom verksamhetschefernas ansvarsområden, ofta bortom deras vetskap. Detta verifieras även vid intervjuer med de två förvaltningarna då de själva inte kunde återge vem som ansvarar för sin förvaltnings arbete med GDPR.

En del i att systematiskt arbeta med dataskyddsfrågor är att säkerställa att regionen följer satta policys och riktlinjer genom att utföra interna uppföljningar och kontroller. Vid intervju framkommer att Region Västmanland utför internkontroll av organisationens arbete med GDPR genom en internkontrollsgrupp med stöd av dataskyddsombudet. Det framkom även att det finns en uppsamlad skuld av uppföljningsarbete då ingen internkontroll gjordes 2021 med anledning av pandemin som påverkade hur regionen brukade sina personalresurser. Detta berörde även regionens GDPR-rutiner som inte blev kontrollerade. I intervju framkom dock att det finns planer att genomföra internkontroll för innevarande år.

Molntjänster

Allt fler IT-lösningar tillhandahålls idag av tredjepartsleverantörer där lagringsmöjligheter av data finns i det s.k. molnet istället för hur det varit traditionellt med att ha egna servrar lokalt. Den trenden gäller även Region Västmanland och är viktig ur ett GDPR perspektiv då förordningen ställer krav på hur data får hanteras och lagras. Exempelvis

får data inte lagras utanför EU/EES utan tillräckliga skyddsåtgärder. Behovet att göra se över sina lösningar för molnlagring och tredjelandsöverföringar har ökat i intensitet, i synnerhet efter att det ramverk man lutat sig mot gällande lagring i USA - känt som Privacy Shield - har underkänts. Under granskningen har tredjelandsöverföringar undersökts högst övergripande. Av intervjuer framkommer att många befintliga avtal med systemleverantörer fortfarande lutar sig mot Privacy Shield, ofta på grund av att systemen har ett monopol på marknaden vilket försvårar att byta leverantör. Av intervju har det framkommit att Förvaltningen för Digitaliseringsstöd inom regionen har fått i uppdrag att inom specifika projekt utreda tredjelandsöverföringar för att ta fram alternativa systemlösningar. Däremot saknas ett sådant arbete på regionövergripande nivå.

Bedömning

Har regionstyrelsen ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

Nej

Region Västmanlands arbete med dataskyddsförordningen förlitar sig till stor del på dataskyddsombudet utan tydliga roller framtagna eller kommunicerade ute i organisationen. För att kunna utföra interna kontroller och uppföljningar är en tydlig ansvarsfördelning en nödvändig förutsättning. Förvaltningarna saknar en tydligt definierad roll som ska ansvara för dataskyddsfrågor vilket innebär att det faller inom ramen för verksamhetschefens ansvarsområde vilket leder till att dataskyddsfrågor inte får önskad prioritet. Under granskning framkom det även att internkontroller inte genomförts inom området på flera år vilket också är en svaghet.

Även för rollfördelning återkommer risken kopplat till det stora personberoendet gentemot dataskyddsombudet då rollen idag har ett brett ansvarsområde utan täckning om rollen skulle bli vakant. Granskningen visar att det breda ansvarsområdet dataskyddsombudet innehar har medfört att viktiga aktiviteter gällande GDPR haft en långsam progress eller inte arbetas med alls. Då dataskyddsombudet har fått prioritera tiden till att stötta förvaltningarna att genomföra hundratals konsekvensbedömningar och upprättande av PuB-avtal har andra områden eftersatts vilket bland annat inkluderar utbildningsaktiviteter och register över personuppgifter. Mot bakgrund i detta bedömer vi sammantaget att regionstyrelsen inte uppfyller en ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Västmanland genomfört en uppföljande och fortsatt granskning av informationssäkerhet och GDPR. Granskningens syfte är att bedöma om regionstyrelsen har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.

Den fortsatta fördjupade granskningen visar att regionen arbetat aktivt med att adressera ett antal av våra tidigare lämnade rekommendation med hänsyn till informationssäkerhetsarbetet. Arbetet har däremot inte fortgått i önskad takt med anledning av pandemin samt att rollen informationssäkerhetsstrateg varit vakant under ett års tid innan den återigen tillsattes 2021. Det finns ett återstående arbete med att genomföra åtgärder i syfte att verkställa tidigare lämnade rekommendationer.

Gällande arbetet med GDPR visar granskningen att det inom regionen finns en till stor del styrande dokumentation, riktlinjer och policys på plats. Däremot är det en låg medvetenhet hos medarbetarna inom regionen gällande deras existens, samt att fler rutiner bör tas fram för att komplettera befintligt material.

Det framkom även det saknas tydligt utsedda ansvariga inom förvaltningarna för GDPR i rollen som exempelvis dataskyddssamordnare. I dagsläget finns det en låg kännedom bland verksamhetschefer gällande deras ansvar för dataskyddsfrågorna inom sina respektive förvaltningarna. Detta har skapat en situation där arbetet med GDPR inte fått önskad prioritet. Avsaknad av tydliga roller och förankrat ansvar försvårar möjligheterna för en ändamålsenlig kontroll och uppföljning av arbetet med GDPR. Genom att tydligare fördela ansvar och underlätta processer genom tydlig dokumentation kommer dataskyddsombudet att avlastas vars arbetsbörda idag beskrivits som överbelastad.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen **inte helt** har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats. Vidare bedömer vi att regionstyrelsen **ej** har säkerställt en ändamålsenlig personuppgiftshantering.

Rekommendationer

Utifrån vår uppföljning av tidigare granskning rekommenderas regionstyrelsen att säkerställa att:

- *Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2,* SSO:n, uppdateras och förtydligar Informationsäkerhetsrådets syfte och ansvar.
- Tydliggöra kopplingen mellan ansvar och roll, exempelvis för informationssäkerhetssamordnaren och informationssäkerhetsstrategen.
- Förtydliga ansvar och roller i PM3-modellen kopplat till säkerhetsåtgärder som riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser.
- Intensifiera planen med att införa obligatoriska, regelbundna utbildningsmoment för samtliga

medarbetare inom regionen. I sammanhanget bör rutin tas fram för att säkerställa genomförande av framtagna utbildningar.
- Genomföra projekt med målsättningen att förbättra behörighetshantering i journalsystemet. Fokusområden bör vara genomförande av riskanalys vid behörighetstilldelning, tydliggöra gallringsrutiner samt säkerställa godtagbar följsamhet av interna rutiner inkluderat kontinuerliga stickprov i patientjournalsystemet.
- Verksamhetsplan 2022 blir en formellt beslutad verksamhetsplan och att planerade aktiviteter är budgeterade.
- Metoder och riktlinjer för upphandlingsprocessen tas fram.

Gällande Region Västmanlands arbete med GDPR rekommenderar vi regionstyrelsen att säkerställa att:
- Framtagna riktlinjer och policies är uppdaterade och att kontinuerlig revidering införs, samt tydlig märkning med datum vilket kommer skapa en tydlighet för medarbetare och öka spårbarhet av ändringar.
- Utforma fler riktlinjer kopplat till GDPR, exempelvis rutin för konsekvensbedömning, för att standardisera regionens arbetssätt.
- Tydliggöra hur organisationen ska ta del av styrdokumentationen kring GDPR.
- Prioritera utbildningsinsatser kring dataskydd.
- Framtagande av en registerförteckning av personuppgiftsbehandlingar genomförs.
- Det utses lokalt ansvariga inom förvaltningarna för dataskyddsfrågor, t.ex. i form av en roll som dataskyddssamordnare, eller tydliggöra för verksamhetschefer om vilket ansvar de faktiskt har över sina förvaltningar då denna insikt är låg i dagsläget.
- En systematisk internkontroll av verksamheternas dataskyddsarbete återstartas så snart som möjligt.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning
1. Har regionstyrelsen vidtagit aktiva åtgärder för att åtgärda de tidigare identifierade bristerna, och beaktat de tolv rekommendationerna i rapporten från 2019? **Delvis** ***Kommentar:*** Granskningen visar att regionen arbetat aktivt med att adressera ett antal av våra tidigare lämnade rekommendationer. Arbetet har däremot inte fortgått i önskad takt med anledning av pandemin samt att rollen informationssäkerhetsstrateg varit vakant under ett års tid innan den återigen tillsattes 2021. Det finns ett återstående arbete med att genomföra åtgärder i syfte att verkställa tidigare lämnade rekommendationer.	
2. Är regionstyrelsens policy och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)? **Delvis** ***Kommentar:*** En grund för policies och riktlinjer finns men kan utvecklas. Dokument är ej tydligt märkta eller tydligt kommunicerade inom organisationen. Behandlingsregister för personuppgiftsbehandlingar saknas.	
3. Har regionstyrelsen ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)? **Nej** ***Kommentar:*** Internkontroller görs inte i dagsläget. Roller och ansvar är inte tydligt kommunicerat inom organisationen för att möjliggöra uppföljning av efterlevnad. Dataskyddsombudet är involverad i för många processer vilket drabbar helheten negativt.	

Bilagor

Vi har i granskningen tagit del av följande dokumentation:

- *Revisionsrapport informationssäkerhet 2019 RVL slutversion*
- *Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2 (2017)*
- *Informationssäkerhetspolicyn (2019)*
- *Verksamhetsrapport för informationssäkerhet (2021)*
- *Protokoll ledningens genomgång (2021)*
- *Verksamhetsplan 2022*
- *Incidenthantering (51316_1) (2021)*
- *Incidenthantering inom Förvaltningen för digitaliseringsstöd (2022)*
- *Rutin vid allvarlig händelse - Förvaltningen för digitaliseringsstöd (2021)*
- Instruktion: *IT-chef i beredskap Förvaltningen för digitaliseringsstöd (2022)*
- *Mall IT-incidentrapport FOA (2022)*
- *It-säkerhet i drift och förvaltning (2018)*
- *För inköp (utbildningsmaterial)*
- *Mall för lösningsbeskrivning*
- *Skyddsnivåer Kravkatalog*
- *Behandling av personuppgifter (2019)*
- *Hantering av personuppgiftsincidenter (2019)*
- *Behörighetsbeställning i HSA (2021)*
- *Åtkomst till patientuppgift i journal (2020)*
- *Krav för åtkomst till uppgifter i regionens huvudjournalsystem (2020)*
- *Sekretess och tystnadsplikt i region Västmanland (2017)*
- *Utlämnande av journalanteckningar (2016)*
- *Loggranskning (2020)*
- *Loggkoll - genomförande av loggranskningar (2020)*
- *Utbildningar-informationssäkerhet (1 jan-20 jun 2022)*

2022-09-09

Tobias Bjöörn

Uppdragsledare

Marie Lindblad

Projektledare