LANDSTINGSREVISIONEN

Granskning av efterlevnad av dataskyddsförordningen

Rapport nr 03/2018

Västerbottens läns landsting

November 2018

Linda Marklund & Petra Nylander, EY

REV 25:2–2018

Revisionsrapport 2018
Genomförd på uppdrag av revisorerna
november 2018

Västerbottens läns landsting

Granskning av efterlevnad av GDPR

Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Västerbottens läns landsting granskat landstingsstyrelsen och hälso- och sjukvårdsnämnden i syfte att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att de krav som ställs i dataskyddsförordningen efterlevs på ett ändamålsenligt sätt.

Vår sammanfattande bedömning är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt att de krav som ställs i dataskyddsförordningen efterlevs på ett ändamålsenligt sätt.

Ett anpassningsarbete har nyligt påbörjats. Roller och ansvar har dokumenterats, ett antal styrande dokument har upprättats och ett inventeringsarbete av personuppgiftsbehandlingar har påbörjats i verksamheterna. Vi bedömer dock att det fortfarande kvarstår mycket arbete innan styrelsen och nämnden säkerställt och kan visa att samtliga verksamheter efterlever förordningens krav. En välfungerande dataskyddsorganisation samt samordning och kontroll av arbetet saknas. Vidare saknas tillräckligt stöd till verksamheterna, vilket är nödvändigt då verksamheterna inte har tillräcklig kunskap för att anpassningar ska kunna genomföras på ett effektivt och lagenligt sätt.

Vi uppmärksammar även att revisorernas Förstudie av förberedelserna inför GDPR (rapport nr 14/2017, januari 2018) inte har behandlats av landstingsstyrelsen.

För sammanfattning av våra iakttagelser och svar på uppställda kontrollmål se avsnitt 4; Sammanfattande bedömning.

Utifrån granskningsresultatet rekommenderar vi landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att:

- Det verkställs en välfungerande *dataskyddsorganisation* som:

  a) Ger verksamheterna tillräckligt *stöd* i anpassningsarbetet.

  b) Ser till att dataskyddsarbetet *samordnas och följs upp*. Detta är nödvändigt för att säkerställa att arbetet bedrivs effektivt och för att säkerställa att styrelsen och nämnden kan ha en tillräcklig kontroll över läget i organisationen.

- Nödvändiga *styrande dokument* (policy/strategi/riktlinjer) upprättas. Detta är nödvändigt eftersom styrelse och nämnd ska kunna visa att de efterlever förordningen samt på vilket sätt detta sker.

2. Inledning och bakgrund

Den nya dataskyddsförordningen, GDPR (The General Data Protection Regulation), ersatte personuppgiftslagen (PUL) den 25 maj 2018. Om verksamheterna brister i följsamheten till denna nya lag riskerar landstinget att drabbas av sanktionsavgifter i enlighet med bestämmelser i GDPR.

På uppdrag av de förtroendevalda revisorerna i Västerbottens läns landsting genomförde EY i januari 2018 en förstudie (rapport nr 14/2017) om arbetet med anpassningar inför GDPRs ikraftträdande. Syftet med förstudien var att ge revisorerna underlag för att kunna besluta om en eventuell fördjupad granskning. Förstudien var avgränsad till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

Förstudien visade på ett flertal brister; bland annat hade inte någon organisation, med tydlig roll-, ansvars- och befogenhetsfördelning avseende införandet av GDPR, formellt beslutats. Vidare framkom att det saknades ett samordnat och heltäckande arbete med anpassningar inför GDPR. Vissa anpassningar hade påbörjats under hösten 2017, men förstudien visade att det fortfarande återstod mycket anpassningar innan styrelsens och nämndens verksamheter kunde bedömas uppfylla de krav som ställs i dataskyddsförordningen.

Vid förstudiens genomförande hade förslag till styrande dokument tagits fram i verksamheten. Dessa var dock fortfarande utkast. Följaktligen fanns ingen tidplan för spridning och implementering av styrdokumenten. Vissa av dessa styrande dokument bedömdes i förstudien inte vara heltäckande för en fullständig implementering av GDPR inom landstingets verksamheter. Utöver detta framkom att inga dokumenterade och landstingsövergripande riskanalyser hade upprättats med anledning av nya förordningen.

Med anledning av förstudiens resultat bedömde revisorerna att det fanns en överhängande risk att nödvändiga anpassningar inte skulle hinna genomföras innan förordningens ikraftträdande. Revisorerna rekommenderade att följande områden skulle prioriteras:

- Ansvar och roller behöver tydliggöras.
- Tidigare identifierade brister i personuppgiftshantering behöver åtgärdas.
- Alla medarbetare behöver informeras om förändringen, och inse vikten av att genomföra anpassningar.
- IT-system som är kompatibla med GDPR behöver säkerställas.
- Att rutiner, som säkerställer den enskildes stärkta rättigheter, tas fram.

Revisorerna beslutade, mot bakgrund av ovanstående bedömning av risk och väsentlighet, att genomföra en fördjupad granskning av efterlevnaden av GDPR, efter lagens ikraftträdande.

Syfte, revisionsfrågor och avgränsning
Granskningens syfte är att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att de krav som ställs i dataskyddsförordningen efterlevs på ett ändamålsenligt sätt.

Granskningens revisionsfrågor beskrivs nedan i tre huvudsakliga områden; styrning, anpassningar i verksamheterna samt uppföljning och kontroll.

Styrning
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt;

- Att styrelsen och nämnden inom sina ansvarsområden säkerställt att det finns en ändamålsenlig roll- och ansvarsfördelning som möjliggör efterlevnad av förordningens krav? Exempelvis;
    - Har dataskyddsombud utsetts, med tydlig roll och uppgifter?
    - Har det tydliggjorts vilka personuppgiftsbehandlingar i IT-system som styrelsen och nämnden är personuppgiftsansvariga respektive personuppgiftsbiträde för?
- Att laganpassade styrande dokument inom området (policys, riktlinjer etc.) är antagna, och av behörig instans?
- Att resurser har avsatts för att kunna genomföra tekniska anpassningar, i enlighet med förordningens lagkrav?

Anpassningar i verksamheterna
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt;

- Att dokumenterade riskanalyser tagits fram med anledning av de förändringar som förordningen medför?
- Att det finns förutsättningar som möjliggjort att anställda tagit del av relevant information om dataskyddsförordningens krav?
- Att en inventering av personuppgifter genomförts i verksamheterna? Detta inkluderar även;
    - Att ett ändamålsenligt register över personuppgiftsbehandlingar har upprättats?
    - Att de personuppgifter som behandlas har en definierad och dokumenterad laglig grund?
- Att kartläggningar och analyser av anpassningsbehov inom IT-system gjorts?
- Att det finns dokumenterade rutiner som möjliggör för verksamheterna att efterleva lagkrav? Detta innefattar rutiner för att;
    - hantera utlämning av personuppgifter vid begäran (dvs rätten till registerutdrag),
    - inhämta och behandla samtycke där det är aktuellt
    - genomföra konsekvensbedömning där känsliga personuppgifter förekommer,
    - tillgodose dataportabilitet och överföra personuppgifter mellan myndigheter,
    - upptäcka, utreda och rapportera personuppgiftsincidenter,
    - genomföra systematisk genomgång och uppdatering av personuppgifter?

Uppföljning och kontroll
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt;

- Att styrelsen och nämnden får tillräcklig rapportering om arbetet med att uppfylla kraven i dataskyddsförordningen?
- Att tillräckliga åtgärder vidtagits med anledning av revisionens tidigare granskning inom området (Förstudie av förberedelser inför införandet av dataskyddsförordningen, 2017)?

Granskningen avgränsas till landstingsstyrelsen (fokus på IT Västerbotten samt tre hälsocentraler) och hälso- och sjukvårdsnämnden (fokus på Psykiatricentrum Västerbotten samt barn- och ungdomscentrum vid Norrlands universitetssjukhus).

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder mot vilka resultatet i granskningen ställs. Följande revisionskriterier används i denna granskning:

- Kommunallagen 6 kap. § 6
- Dataskyddsförordningen/GDPR
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

- Eventuella landstingsinterna styrande dokument

En utförlig beskrivning av berörda delar i revisionskriterierna återfinns i bilaga 2.

Genomförande och urval
Granskningen har genomförts genom;

- insamling och analys av dokumentation från landstingsstyrelsens och hälso- och sjukvårdsnämndens verksamheter (se bilaga 1 Källförteckning)
- intervjuer med;
    - landstingsdirektören,
    - informationssäkerhetsstrateg,
    - jurist,
    - dataskyddsombud,
    - stabsdirektör,
    - verksamhetschefer,
    - projektledare för GDPR,
    - avvikelseutredare,
    - personuppgiftshandläggare,

En avstämning har även gjorts med digitaliserings- och teknikdirektören.

Inom styrelsens verksamheter har tre hälsocentraler och en basenhet ingått i urvalet:

- Tegs hälsocentral (ca 17 500 patienter, näst störst i länet sett till antalet patienter)
- Ersboda hälsocentral (ca 9 500 patienter, mellanstor sett till antalet patienter)
- Lövångers hälsocentral (ca 2 200 patienter, näst minst i länet sett till antalet patienter)

Urvalet av hälsocentraler baseras på antal patienter som är listade vid hälsocentralen. Oavsett storlek på hälsocentral anser vi att det är väsentligt att hälsocentralerna tillämpar GDPR-anpassade rutiner vid hantering av personuppgifter. Urvalet baseras även i till viss del på geografisk placering (stad/landsbygd).

Utöver hälsocentralerna ingår även länsövergripande IT Västerbotten i urvalet för landstingsstyrelsens verksamheter. IT Västerbotten ger stöd till landstingets samtliga verksamheter och ansvarar för drift, förvaltning, service och utveckling inom IT-området. Mot bakgrund av att många landstingsövergripande system driftas av IT Västerbotten är vår bedömning att IT Västerbotten har en särskild insyn i behov kring GDPR-relaterade anpassningar kopplade till IT-system.

Inom nämndens verksamheter har ett urval av två länsövergripande kliniker gjorts; Barn- och ungdomscentrum samt Psykiatricentrum. Urvalet baseras dels på att verksamheterna hanterar känsliga personuppgifter (uppgifter om hälsa samt i vissa fall även genetiska uppgifter). Vidare bedömer vi att verksamheternas målgrupper kan vara av skyddsvärd karaktär (till exempel barn och personer som inte har möjlighet att föra sin egen talan) och att det därmed kan vara aktuellt att upprätta särskilda rutiner för hantering av personuppgifter.

I granskningen har vi tagit del av en lista över systemägare för landstingsövergripande system. Systemägare har tilldelats särskilda uppgifter beträffande GDPR-anpassningar. Vi har kontaktat fyra slumpmässigt utvalda systemägare som är ägare för mellan ett till fem system och efterfrågat registerförteckning över personuppgiftsbehandling.

3. Granskningsresultat

3.1. Roller och ansvar inom dataskyddsorganisationen

I revisorernas förstudie (rapport nr 14/2017) konstaterade revisorerna att det inte fanns någon formellt beslutad organisation med tydlig roll-, ansvars-, och befogenhetsfördelning för införandet av GDPR. Revisorerna rekommenderade därför att ansvar och roller snarast skulle tydliggöras.

I avsnitten nedan beskrivs våra aktuella iakttagelser beträffande roller och ansvar i dataskyddsarbetet.

3.1.1. Dataskyddsorganisation

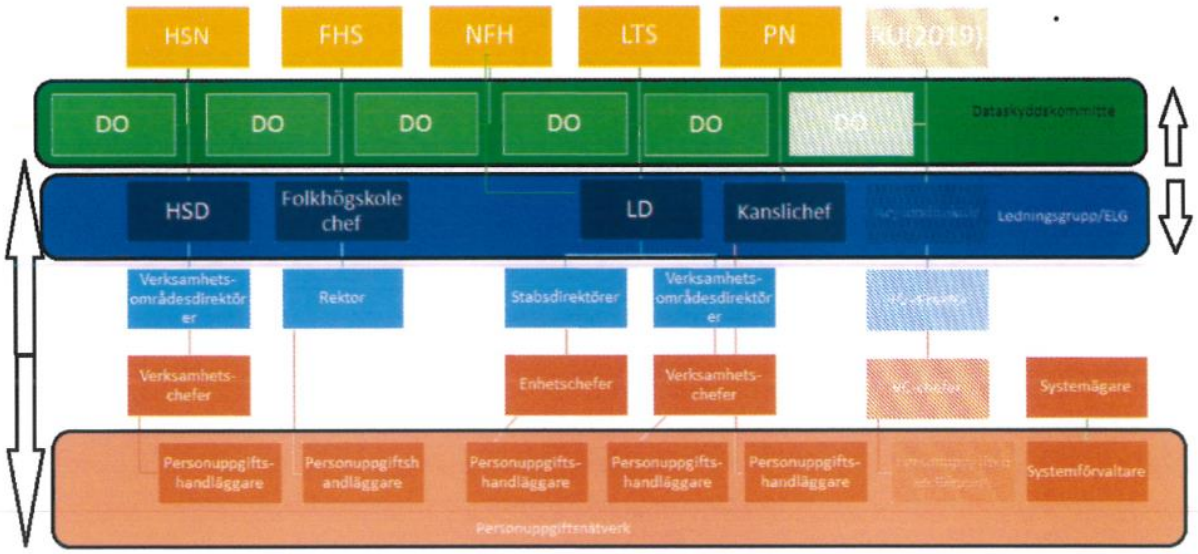
Vår granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har tagit del av information, eller fattat beslut, om en organisation för dataskyddsarbetet. Ett förslag till organisation har däremot behandlats på tjänstemannanivå.

Av ELGs[1] minnesanteckningar framgår att ELG i februari 2018 informerades om ett förslag till dataskyddsorganisation (2018-02-12, punkt 10). Landstingets jurist och informationssäkerhetsstrateg fick enligt anteckningarna vid detta tillfälle i uppdrag att återkomma med ett fördjupat förslag på intern dataskyddsorganisation.

Av senare minnesanteckningar från ELG (2018-03-26, punkt 21) framgår att landstingsjurist presenterat ett förslag till inriktningsbeslut avseende roller och ansvar i dataskyddsorganisationen. Enligt anteckningarna beslutade landstingsdirektören att principerna i organisationsförslaget tillstyrks.

Se bild över den tillstyrkta dataskyddsorganisationen (och dess kommunikationsvägar) nedan.

Figur 1. Organisations-/kommunikationsskiss Dataskyddsorganisation behandlad av ELG



[1] ELG = Landstingets Exekutiva Ledningsgrupp

3.1.2. Roll-, ansvars- och befogenhetsfördelning

I det förslag till dataskyddsorganisation som tillstyrkts av landstingsdirektören finns en beskrivning av olika funktioners roller och ansvar.

Vår granskning visar dock att den tillstyrkta organisationen ännu inte har verkställts till fullo. Enligt intervju med dataskyddsombud pågår fortfarande diskussioner om hur arbetet lämpligast ska organiseras och hur rapportering ska ske mellan olika nivåer i organisationen.

I nedanstående tabell beskrivs ett urval av roller, uppgifter och ansvar i den beslutade organisationen, tillsammans med våra iakttagelser från dokumentation och intervjuer.

Beskrivning enligt den dokumenterade dataskyddsorganisationen	**Våra iakttagelser**
Varje nämnd är personuppgiftsansvarig för sina personuppgiftsbehandlingar och är skyldig att *utse ett dataskyddsombud.*	Såväl landstingsstyrelsen som hälso- och sjukvårdsnämnden har utsett ett dataskyddsombud. Styrelsens ordförande har genom ett delegationsbeslut i maj 2018 (2018-05-22, dnr VLL 1226-2018) utsett ett dataskyddombud för styrelsen. Ordförandebeslutet har enligt protokoll anmälts som delegationsbeslut till styrelsen (2018-06-07, § 172). Nämnden har i maj 2018 utsett ett dataskyddsombud (2018-05-23, § 62). Vidare framgår av intervju att nämnden ska utse ett nytt dataskyddsombud i samband med regionbildningen 1 januari 2019.
Dataskyddsombudens *uppgift* är bla att informera och ge råd till den personuppgiftsansvarige (nämnderna) och de anställda om deras skyldigheter enligt förordningen. Vidare ska ombuden bla övervaka efterlevnaden av dataskyddsförordningen. I organisationsbeskrivningen anges att organisationen måste bedriva ett *självständigt och aktivt dataskyddsarbete som inte leds av dataskyddsombuden.*	Intervjuade dataskyddsombud uppger att de försöker informera och stödja verksamheterna, exempelvis via personuppgiftsnätverket, mail och telefon. Av våra intervjuer med verksamheterna (bland annat verksamhetschefer och personuppgiftshandläggare) framkommer följande: ▸ Verksamheterna uttrycker ett stort behov av stöd i form av konkreta råd i sina anpassningsarbeten och de flesta verksamheterna upplever att de inte får det stöd de behöver, exempelvis i tillämpning av befintliga riktlinjer och mallar. ▸ Verksamheterna upplever inte att de informerats om att de själva måste bedriva ett självständigt dataskyddsarbete. Samtliga verksamheter vi intervjuat upplever att de inte har tillräcklig kunskap och stöd för att kunna genomföra ett självständigt dataskyddsarbete.

En *dataskyddskommitté* vars syfte är att utgöra en expertgrupp för dataskyddsfrågor ska inrättas. Enligt organisationsbeskrivningen ska kommittén utgöras av ansvariga chefer på landstingsledningsnivå. Vidare ska kommittén ha i uppgift att besluta kring prioritering och organisering av dataskyddsaktiviteter.	Vår granskning visar att det ännu inte finns en aktiv dataskyddskommitté i organisationen. Landstingsdirektör och stabsdirektör uppger att kommittén är under uppbyggnad. Anledningarna att avvakta uppges vara att landstingets högsta ledning byts under hösten samt den kommande regionbildningen.
Verksamhetschefen ska *utse personuppgiftshandläggare.* Enhetens *dataskyddsteam* ska utgöras av; verksamhetschef, avdelningschef, systemägare, avvikelsehandläggare och personuppgiftshandläggare.	Samtliga verksamhetschefer som omfattas av vårt urval har utsett minst en personuppgiftshandläggare i sin verksamhet. Vi har, från dataskyddsombuden, erhållit en samlad lista på samtliga utsedda personuppgiftshandläggare. Det finns dock ingen information om huruvida samtliga verksamheter har utsett personuppgiftshandläggare. Av våra intervjuer med dataskyddsombud framgår att det ännu inte är helt bestämt att dataskyddsteam ska inrättas.
Personuppgiftshandläggare ska fungera som verksamhetschefernas förlängda arm. Handläggaren ska utreda personuppgiftsincidenter som inträffar på enheten, bistå verksamheten i att registerförteckna personuppgiftsbehandlingar, ta fram enhetsspecifika rutiner om det är nödvändigt, kontakta dataskyddsombudet i frågor om laglighet och dataskydd samt ingå i personuppgiftsnätverket som dataskyddsombudet leder.	De personuppgiftshandläggare (inom både styrelsens och nämndens ansvarsområde) vi intervjuat upplever att rollen som personuppgiftshandläggare i stora drag är tydlig. Dock upplever en majoritet av handläggarna att de inte har tillräcklig kunskap för att utföra sina uppgifter.
Ett *personuppgiftsnätverk* ska inrättas med syfte att skapa ett forum för dataskyddsfrågor.	Vid granskningens genomförande har personuppgiftsnätverket, bestående av samtliga utsedda personuppgiftshandläggare, sammanträtt vid ett tillfälle (september 2018). I november 2018 planerar dataskyddsombuden en till träff med en workshop runt personuppgiftsincidenter.

Av våra intervjuer framgår att dataskyddsombud i september 2018 informerat personuppgiftsnätverket om personuppgiftshandläggarnas roll, nätverkets roll samt dataskyddsombudens roll. Hur övriga delar av dataskyddsorganisationen ska se ut diskuteras ännu.

3.2. Resurser

Landstingsstyrelsen och hälso- och sjukvårdsnämnden har avsatt resurser i form av *dataskyddsombud*. Enligt den av landstingsdirektören tillstyrkta dataskyddsorganisationen beräknas dataskyddsombuden för styrelsen och nämnden avsätta 50 % av sina tjänster till denna uppgift.

Varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har i övrigt avsatt några särskilda resurser för att genomföra anpassningar i verksamheten eller uppdateringar i IT-system.

Ingen av de utsedda *personuppgiftshandläggarna* som intervjuats i granskningen har i sina tjänster formellt avsatt tid för rollen som personuppgiftshandläggare.

Vi uppmärksammar vidare att varje systemägare, enligt dataskyddsorganisationen, ansvarar för att säkerställa att IT-systemen är anpassade efter gällande lagar. Dock har systemägarna inte budgetansvar för de system som de ansvarar för. Brist på resurser för anpassningar av befintliga IT-system framförs också som ett generellt bekymmer vid våra intervjuer med IT Västerbotten.

3.3. Styrande dokument

I revisorernas förstudie av arbetet inför GDPR (rapport nr 14/2017) framkom att landstingets jurist och informationssäkerhetsstrateg hade upprättat förslag till ett antal vägledande dokument för arbetet[2]. Vid intervjuer med dataskyddsombuden framkommer nu att dokumenten som nämns i förstudien i stor utsträckning endast var arbetsdokument för det interna arbetet med införandet av förordningen, och de används inte i organisationen efter lagens ikraftträdande.

Vår granskning visar att varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har beslutat om några GDPR-specifika styrande dokument sedan förstudiens genomförande (januari 2018).

Landstingsjurist och informationssäkerhetsstrateg har under innevarande år upprättat ett antal landstingsövergripande stödjande dokument:

- Riktlinje för personuppgiftshandläggare (saknar datum för fastställande, dokumentansvarig är landstingsdirektören)
- Riktlinje för e-post (2018-06-19, digitaliserings- och teknikdirektören)
- Riktlinje för hur registerförteckning över personuppgiftsbehandlingar ska göras (2018-04-03, landstingsdirektören)
- Rutin för rapportering och utredning av personuppgiftsincident (saknar datum, fastställt av landstingsdirektören)
- Mall för utredning av personuppgiftsincident (saknar uppgifter om fastställande)
- Mall för inhämtande av samtycke allmänt samt för bilder, ljud och video (saknar uppgifter om fastställande)
- Mall för upprättande av personuppgiftsbiträdesavtal (saknar uppgifter om fastställande)

Samtliga ovanstående dokument finns tillgängliga för alla medarbetare på landstingets intranät.

Utöver de ovan nämnda dokumenten uppger dataskyddsombuden att följande landstingsövergripande riktlinjer/rutiner är under framtagande:

- Riktlinje om hur rätten till registerutdrag ska hanteras
- Riktlinje om hur konsekvensbedömningar ska göras

En stor del av de personuppgiftshandläggare vi intervjuat i såväl styrelsens som nämndens verksamheter upplever de befintliga riktlinjerna och mallarna som svårbegripliga och att de behöver vägledning och förtydliganden för att använda dessa.

[2] GDPR-aktivitetsplan (antagen i ELG 2017-10-21, punkt 61), GDPR-strategi, Checklista för lagkrav, checklista för informationssäkerhet samt rutin för personuppgiftsincidenter, Ledning och styrmodell för informationssäkerhet, Säkerhetsanalys av informationstillgångar

3.4. Verksamheternas genomförda anpassningar

Av våra intervjuer framgår att arbetet med anpassningar i verksamheterna nyligt har påbörjats och att verksamheterna generellt upplever att de saknar tillräcklig kunskap och ett konkret stöd i sitt anpassningsarbete.

3.4.1. Riskanalyser

I revisorernas förstudie av arbetet med GDPR konstaterades att verksamheten inte upprättat några dokumenterade landstingsövergripande riskanalyser med anledning av GDPR. Vår granskning visar att det fortsatt saknas dokumenterade landstingsövergripande riskanalyser som ligger till grund för verksamheternas prioriteringar i anpassningsarbetet.

3.4.2. Verksamhetens rutiner

Av riktlinjen för personuppgiftshandläggare (se avsnitt 3.3.1) framgår att verksamhetens personuppgiftshandläggare, i samråd med dataskyddsombudet, ska ta fram de rutiner för dataskyddsfrågor som behövs vid respektive enhet. Vi noterar att endast två av de granskade verksamheterna (Psykiatricentrum och IT-Västerbotten) har tagit fram en kompletterande lokal rutin.

Vi har i granskningen inte erhållit någon centralt eller lokalt upprättad riktlinje/rutinbeskrivning för följande moment i arbetet:

- Hantera utlämning av personuppgifter vid begäran (rätt till registerutdrag),
- Tillgodose dataportabilitet och överföra personuppgifter mellan myndigheter (här noterar vi dock att information om rätten till dataportabilitet har lämnats via Linda)
- Eventuella anpassningar i IT-system
- Systematisk genomgång och uppdatering av personuppgiftsbehandlingar/registerförteckningar
- Hantera rätten till registerutdrag (uppges vara under upprättande på central nivå)
- Göra konsekvensbedömningar (uppges vara under upprättande på central nivå)

Av våra intervjuer framgår att det inte är helt tydligt i alla verksamheter hur ovanstående moment ska genomföras.

Vad beträffar samtycke framkommer vid intervjuer att verksamheter inom styrelsens ansvarsområde (i synnerhet hälsocentralerna) samt nämndens ansvarsområde (Barn- och ungdomscentrum) sedan tidigare inhämtar *samtycke* då det behövs. Detta sker till exempel vid överföring av uppgifter till andra kommuner och myndigheter eller vid forskningsändamål. Enligt uppgift hanteras samtycket nu som tidigare i det befintliga system som används, och inte på den mall för inhämtande av samtycke som upprättats efter förordningens ikraftträdande.

Psykiatricentrum upplever att det är otydligt på vilket sätt begäran om utlämnande av handlingar med personuppgifter ska hanteras. Otydligheten rör hur utlämning av handlingar ska göras samtidigt som kraven i GDPR, offentlighets- och sekretesslagen och tryckfrihetsförordningen ska uppfyllas. När det gäller hantering av *dataportabilitet* (rätten för en registrerad att få ut sina uppgifter och/eller överföra dem till annan aktör) framgår av intervjuer att detta sällan är aktuellt i landstingets verksamheter. Det saknas dock en rutin för hur verksamheten ska hantera eventuella förfrågningar.

Vidare framgår av våra intervjuer att det i flera av de granskade verksamheterna, i synnerhet vid hälsocentralerna, råder oklarhet kring hur, av vem samt på vilket sätt *personuppgiftsincidenter* ska hanteras. Flera verksamheter har utsedda avvikelsehanterare som rapporterar andra typer av avvikelser/incidenter i Platina. Några intervjuade har lyft möjligheten att använda Platina även för hantering av personuppgiftsincidenter.

3.4.3. Registerförteckningar och inventering av personuppgifter

I revisorernas förstudie (rapport nr 14/2017) fanns ingen samlad landstingsövergripande bild av verksamheternas arbete med inventering av personuppgiftsbehandlingar. Vidare konstaterades att endast ett av landstingets IT-system hade inventerats i sin helhet. Inventering av personuppgifter pågick för två andra system. En förteckning från IT-Västerbotten visade att där fanns minst 38 system.

Dataskyddsombuden har, efter förstudiens genomförande, upprättat en mall (Excel-fil) som verksamheterna ska använda för att registerförteckna sina personuppgiftsbehandlingar. Samtliga verksamheter är ålagda att inventera sina personuppgiftsbehandlingar och översända en kopia på förteckningen till dataskyddsombudens gemensamma myndighetsbrevlåda. Enligt information på intranätet ska registerförteckningar ha tagits fram och översänts till dataskyddsombudens gemensamma funktionsbrevlåda för kännedom senast 15 maj 2018.

Samtliga registerförteckningar som skickats in till dataskyddsombuden, via funktionsbrevlådan, har sammanställts i en excelfil. Vår granskning visar dock att det fortfarande saknas registerförteckningar från ett flertal verksamheter. Vissa personuppgiftsbehandlingar kan även vara dubbelförtecknade. Således finns ännu ingen heltäckande information om vilka personuppgiftsbehandlingar som finns i landstinget. Vidare uppmärksammar vi att det inte genomförts någon kontroll eller kvalitetssäkring av innehållet i de registerförteckningar som skickas in till dataskyddsombudens gemensamma myndighetsbrevlåda.

Vi har tagit del av registerförteckningar från fem av de sex verksamheter som ingått i vårt urval. Vår granskning av de förteckningar vi erhållit visar följande:

- Ett flertal inventeringar och förteckningar är inte heltäckande eller kompletta.
- Laglig grund saknas för flera personuppgiftsbehandlingar.
- Verksamheterna har i vissa fall gjort olika tolkningar om vad som utgör känsliga personuppgifter. Exempelvis har patienters diagnoser tolkats som känsliga personuppgifter av en verksamhet men inte av en annan.

Av våra intervjuer framgår att ett flertal verksamheter upplever det svårt att genomföra inventeringen och att upprätta registerförteckningen. Otydligheter i vad som ska förtecknas och hur detta ska ske har inneburit att flera verksamheter ägnat tid till att klargöra vad som gäller kring registerförteckningsarbetet, vilket upplevts som mycket ineffektivt. Några verksamheter uppger att de har efterfrågat synpunkter på de förteckningar som de skickat in till dataskyddsombudens gemensamma myndighetsbrevlåda men att de inte erhållit någon återkoppling.

I nedanstående stycken beskrivs inventeringsarbetet i verksamheterna samt våra iakttagelser närmare.

3.4.3.1 Inventering i landstingsstyrelsens verksamheter

IT Västerbotten har tillhandahållit en registerförteckning över personuppgiftsbehandlingar med dokumenterad laglig grund för samtliga personuppgiftsbehandlingar. Förteckningen har enligt intervjuade tagits fram under september månad. Detta efter att personuppgiftshandläggare deltagit i utbildning (tillhandahållen av dataskyddsombud) i början på september.

Företrädare för Lövångers hälsocentral beskriver i intervjuer att de har arbetat fram en registerförteckning över personuppgiftsbehandlingar. I granskningen har vi tagit del av den. Vi har även tagit del av muntliga uppgifter som beskriver att den registerförteckning som tagits fram ska kompletteras, vilket är ett pågående arbete vid granskningstillfället (oktober 2018). Den lagliga grunden finns i stor utsträckning dokumenterad.

Företrädare för Ersboda hälsocentral beskriver att de påbörjat ett inventeringsarbete i sin verksamhet. Enligt uppgift har ett arbete för att rensa servrar genomförts. Dock framkommer att det inte är tydligt vad som ska ingå i registerförteckningen, ej heller vilken detaljeringsnivå personuppgiftsbehandlingarna i förteckningen ska ha. Vi har därmed inte tagit del av någon framtagen registerförteckning.

Företrädare för Tegs hälsocentral har översänt en registerförteckning. Enligt uppgift pågår fortfarande inventeringen av personuppgiftsbehandlingar, och förteckningsarbetet beskrivs därför som fortlöpande. Ett antal lagliga grunder finns dokumenterade men inte för samtliga personuppgiftsbehandlingar.

3.4.3.2 Inventering i hälso- och sjukvårdsnämndens verksamheter

För länskliniken Psykiatricentrum har vi tagit emot tre registerförteckningar. Dessa förteckningar är framtagna utifrån geografisk indelning (Umeå, Skellefteå och Södra Lappland). Vi har även tagit emot en lokalt framtagen rutin för hantering av GDPR.

Samtliga förteckningar har en kolumn för angivande av laglig grund. En genomgång av de personuppgiftsbehandlingar som anges i registerförteckningarna för kliniken visar att den lagliga grunden i stor utsträckning inte dokumenterats. Hur den lagliga grunden för behandling av personuppgifter ska dokumenteras är tydligare sedan personuppgiftshandläggare deltagit i den utbildning som tillhandahållits av dataskyddsombuden.

Personuppgiftshandläggare för Psykiatricentrum beskriver vid intervjuer att arbetet med att ta fram registerförteckningar pågår fortlöpande. Vidare uppger intervjuade att det är otydligt vilken detaljeringsnivå personuppgiftsbehandlingarna ska ha i förteckningen.

Personuppgiftshandläggare inom kliniken beskriver att de efterfrågat återkoppling på innehållet i registerförteckningen från dataskyddsombuden utan resultat.

För barn- och ungdomscentrum har vi tagit emot en registerförteckning. En genomgång av de personuppgiftsbehandlingar som anges i registerförteckningen visar att den lagliga grunden inte dokumenterats. Vid intervjuer framkommer att registerförteckningen togs fram när verksamheten fortfarande saknade utbildning och kunskap om hur förteckningen skulle fyllas i. Personuppgiftshandläggare vid barn- och ungdomscentrum upplever att det inte är klargjort vilken detaljeringsnivå som registerförteckningarna ska ha.

Personuppgiftshandläggare inom centrat beskriver att de efterfrågat återkoppling på innehållet i registerförteckningen från dataskyddsombuden utan resultat.

Inom barn- och ungdomscentrums registerförteckning framgår att det förekommer personuppgiftsbehandlingar som innehåller patienters diagnoser. I registerförteckningen anges att dessa behandlingar inte innehåller känsliga personuppgifter. I registerförteckningar som Psykiatricentrum tillhandahållit har patienters diagnoser klassats som känsliga personuppgifter.

3.4.4. IT-system anpassning och personuppgiftsbiträdesavtal

3.4.4.1 Kartläggning och analys av anpassningsbehov

I revisorernas förstudie av förberedelserna inför GDPR framkom att:

- GDPRs regler kring inbyggt dataskydd och dataskydd som standard (GDPR artikel 25) upplevdes av IT Västerbotten (dåvarande Informatik) vara svåra att uppnå innan förordningen skulle träda i kraft.
- Upplevelsen var att det saknades resurser för att genomföra nödvändiga förändringar beträffande IT-system i verksamheterna.

Med anledning av ovanstående iakttagelser rekommenderade revisorerna styrelsen och nämnden att säkerställa att IT-systemen görs kompatibla med GDPRs bestämmelser.

Av rollbeskrivning för systemägare samt den beskrivning av dataskyddsorganisationen som tillstyrkts av landstingsdirektören framgår att det är varje systemägares uppgift att säkerställa att systemen stödjer verksamheten och följer tillämpliga lagar och förordningar.

Granskningen visar att det inte finns någon samlad information om huruvida landstingets IT-system kartlagts och vilka systemanpassningar som i så fall är nödvändiga. Det finns inte heller, som tidigare nämnts, någon dokumenterad rutin för hur eventuella anpassningar eller nyinvesteringar i IT-system ska hanteras.

3.4.4.2 IT-system och personuppgiftsbiträdesavtal

Av den beskrivning av dataskyddsorganisationen som tillstyrkts av landstingsdirektören framgår att varje systemägare ska se till att upprätta en förteckning över sitt/sina system, och rapportera in en kopia av förteckningen till dataskyddsombudet. Enligt mallen för registerförteckning ska den förteckning som upprättas också innehålla information om huruvida personuppgiftsbiträden används.

Landstingets jurist har upprättat en mall som ska användas vid upprättande av personuppgiftsbiträdesavtal. Mallen reglerar ansvarsfördelningen i personuppgiftshantering mellan personuppgiftsansvarig (styrelse/nämnd) och personuppgiftsbiträdet (extern leverantör). Enligt dataskyddsombuden ska mallen användas för samtliga personuppgiftsbiträdesavtal som upprättas inom landstinget.

Vi har från IT Västerbotten erhållit en förteckning över 51 landstingsövergripande IT-system. Förteckningen uppges vara komplett och innehålla samtliga landstingets IT-system. Utifrån listan har vi gjort en stickprovskontroll. Från fyra systemägare har vi efterfrågat:

- Registerförteckning över personuppgiftsbehandlingar där systemägarens system ingår.
- Personuppgiftsbiträdesavtal (om systemet behandlar personuppgifter).

Vi har erhållit svar från tre systemägare. Resultatet av vår stickprovskontroll visar följande:

Systemägare	*Registerförteckning har översänts*	*Systemet behandlar personuppgifter*	*Personuppgiftsbiträdesavtal finns*
Systemägare 1 (ansvarig för ett system)	Ja.	Ja.	Nej. Enligt registerförteckningen används inte biträden för systemet.
Systemägare 2 (ansvarig för två system)	Ja.	Ja.	Nej. Enligt registerförteckningarna används inte biträden för dessa två system.
Systemägare 3 (ansvarig för två system)	Nej, men uppger att det ska finnas.	Ja.	Ja. Personuppgiftsbiträdesavtal för ett system har översänts. Upprättat enligt leverantörens mall.
Systemägare 4 (ansvarig för fem system)	*Ej återkopplat trots upprepade påminnelser.*	*Ej återkopplat trots upprepade påminnelser.*	*Ej återkopplat trots upprepade påminnelser.*

3.4.5. Information till anställda

På landstingets intranät har dataskyddsombuden publicerat information om GDPR som samtliga anställda har tillgång till. Informationen beskriver bland annat lagens syfte, roller och ansvar kring GDPR, viss hantering av personuppgifter samt skyldigheten att registerförteckna.

Vi har i granskningen inte haft möjlighet att kontrollera hur många anställda som i praktiken nåtts av informationen på intranätet. Denna typ av kontroll har heller inte gjorts inom landstinget.

Samtliga intervjuade upplever att den information som finns att tillgå på intranätet är informativ. Ett antal personuppgiftshandläggare har dock beskrivit informationen som svår att tillgodogöra sig. Detta då språkbruket upplevs som formellt och akademiskt.

Utöver informationen på intranätet har en utbildning för personuppgiftshandläggare, med fokus på kartläggning av laglig grund och personuppgiftsincidenter, genomförts i september 2018. Utbildningen anordnades av dataskyddsombuden. I underlaget som användes vid träffen framgår att personuppgiftshandläggarna fick information om sin roll med tillhörande uppgifter, samt instruktioner om vilka uppgifter som ska ingå i en registerförteckning.

Av intervjuer framgår att dataskyddsombuden planerar en workshop i november 2018 för personuppgiftshandläggare med fokus på handläggning av incidenter.

De personuppgiftshandläggare vi intervjuat uppger att de arbetar med att informera sina medarbetare i respektive verksamhet om kraven i GDPR. Några personuppgiftshandläggare upplever dock svårigheter i att föra informationen vidare då de inte själv har tillräcklig kunskap inom området.

3.5. Uppföljning av förstudie och rapportering till styrelse och nämnd

Revisorerna bedömde i förstudien av arbetet med GDPR bla att det fanns en överhängande risk att nödvändiga anpassningar inte skulle hinna genomföras innan förordningens ikraftträdande. Revisorerna lämnade därför ett antal rekommendationer till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

Granskningen visar att landstingsstyrelsen inte har behandlat revisorernas förstudie. Förstudien har inte heller behandlats i ELG. Vi har efterfrågat information om anledningen till detta

och det svar som lämnats från ledningsstabens kanslichef är att rapporten inte blivit anmäld till styrelsen pga. en miss i hanteringen.

Hälso- och sjukvårdsnämnden har i maj 2018 (2018-05-23, § 62) behandlat revisorernas förstudie. Nämnden beslutade att *notera informationen till protokollet och revisionens synpunkter beaktas i det kommande planeringsarbetet.*

Utöver ovanstående kan vi inte styrka att styrelsen eller nämnden fått någon information om det pågående arbetet med GDPR i organisationen.

4. Sammanfattande bedömning

Vår sammanfattande bedömning är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt att de krav som ställs i dataskyddsförordningen efterlevs på ett ändamålsenligt sätt. Den sammanfattande bedömningen baseras på nedanstående iakttagelser och bedömningar.

Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt:	**Svar**
Att styrelsen och nämnden inom sina ansvarsområden säkerställt att det finns en ändamålsenlig roll- och ansvarsfördelning som möjliggör efterlevnad av förordningens krav? Tex; ▸ Har dataskyddsombud utsetts, med tydlig roll och uppgifter? ▸ Har det tydliggjorts vilka personuppgiftsbehandlingar i IT-system som styrelsen och nämnden är personuppgiftsansvariga respektive personuppgiftsbiträde för?	Nej. Vår bedömning är att styrelsen och nämnden ännu inte har säkerställt en ändamålsenlig roll- och ansvarsfördelning. Styrelsen och nämnden har utsett dataskyddsombud för sina respektive ansvarsområden, vilket är i enlighet med förordningens krav. I verksamheterna som ingått i vårt urval har även personuppgiftshandläggare utsetts. Vidare har en organisationsbeskrivning upprättats och tillstyrkts av landstingsdirektören. I beskrivningen framgår roller, ansvar och uppgifter för olika funktioner och grupperingar i dataskyddsorganisationen. Vi uppmärksammar dock följande brister när det gäller dataskyddsorganisationen: ▸ Organisationen är ännu *inte fullt implementerad*. Diskussioner pågår fortfarande om hur arbetet lämpligast ska organiseras och hur rapportering ska ske mellan olika nivåer i organisationen. ▸ Det saknas tillräcklig *samordning och kontroll* av arbetet. Det finns i nuläget ingen tydligt samordnande funktion och ingen samlad information om hur personuppgifter behandlas i organisationen. Vår uppfattning är att arbetet inte bedrivs på effektivt sätt då samordning saknas. ▸ Det framkommer med stor tydlighet i granskningen att det saknas tillräcklig kunskap hos de som utsetts i verksamheterna, för att arbetet ska kunna genomföras på ett effektivt och lagenligt sätt. Vår bedömning är vidare att det ännu inte har tydliggjorts vilka personuppgiftsbehandlingar i IT-system som styrelsen och nämnden är ansvariga samt vilka de anlitar biträden för. Det finns en rutin för att dokumentera och samla in information om personuppgiftsbiträdesavtal. Dock saknas kontroll av om det upprättats aktuella avtal för samtliga system som behandlar personuppgifter inom styrelsens respektive nämndens verksamheter. Vår stickprovskontroll bland fyra systemägare med ansvar för sammanlagt 10 IT-system gav oss tillgång till ett upprättat personuppgiftsbiträdesavtal.
Att laganpassade styrande dokument inom området (policys, riktlinjer etc) är antagna, och av behörig instans?	Nej. Vi bedömer att styrelsen och nämnden inte säkerställt att tillräckliga laganpassade styrande dokument har tagits fram.

Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt:	Svar
	Ett antal riktlinjer har tagits fram inom förvaltningen. Det saknas dock ett sammanhållet övergripande och politiskt fastställt styrdokument (policy/strategi el motsvarande) som tydliggör hur dataskyddsarbetet ska styras, organiseras och följas upp.
Att kartläggningar och analyser av anpassningsbehov inom IT-system gjorts? Att resurser har avsatts för att kunna genomföra tekniska anpassningar, i enlighet med förordningens lagkrav?	Nej. Vår bedömning är att styrelsen och nämnden inte säkerställt att kartläggningar och analyser av anpassningsbehov inom IT-system har genomförts i tillräcklig omfattning. Det är, enligt den beskrivna dataskyddsorganisationen, varje systemägares uppgift att säkerställa att systemen stödjer verksamheten och följer tillämpliga lagar och förordningar. Vi noterar att det saknas landstingsövergripande information om vilka eventuella anpassningar som är nödvändiga att göra för att säkerställa att landstingets IT-system är kompatibla med GDPRs bestämmelser. Det finns inte heller någon rutin för hur eventuella anpassningar eller nyinvesteringar av IT-system ska hanteras. Varken styrelsen eller nämnden har heller säkerställt att ekonomiska resurser har avsatts för att genomföra de eventuella anpassningar som behövs i IT-systemen.
Att dokumenterade riskanalyser tagits fram med anledning av de förändringar som förordningen medför?	Nej. Vi bedömer att styrelsen och nämnden inte har säkerställt att dokumenterade riskanalyser har tagits fram. Enligt vår bedömning är det en väsentlig del i anpassningsarbetet att identifiera risker i landstingets personuppgiftsbehandlingar. En riskanalys är också nödvändig för att veta om en konsekvensbedömning behöver utföras för att förebygga riskerna.
Att det finns förutsättningar som möjliggjort att anställda tagit del av relevant information om dataskyddsförordningens krav?	Ja. Vi bedömer att styrelsen och nämnden har skapat förutsättningar för anställda att ta del av relevant information om dataskyddsförordningens krav. Information har publicerats på landstingets intranät. Vidare har personuppgiftshandläggarna i viss utsträckning informerat sina kollegor vid arbetsplatsträffar. Vi vill dock uppmärksamma styrelsen och nämnden på att en generell brist på tillräcklig kunskap i verksamheterna samt personuppgiftshandläggarnas upplevelse av att det saknas tillräckligt stöd, medför att verksamheterna i praktiken har svårigheter att tillgodogöra sig den information som finns.
Att en inventering av personuppgifter genomförts i verksamheterna? Detta inkluderar även;	Nej.

Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt:	Svar
▸ Att ett ändamålsenligt register över personuppgiftsbehandlingar har upprättats? ▸ Att de personuppgifter som behandlas har en definierad och dokumenterad laglig grund?	Vi bedömer att varken styrelsen eller nämnden säkerställt att en heltäckande inventering av personuppgifter ännu genomförts i verksamheterna. Enligt GDPR artikel 30 ska samtliga personuppgiftsbehandlingar ingå i en registerförteckning. Granskningen visar att det i den sammanställda informationen över verksamhetens registerförteckningar inte går att få en heltäckande bild över vilka personuppgiftsbehandlingar som finns i landstinget. Samtliga verksamheter som ingått i vårt urval har inte upprättat register över sina personuppgiftsbehandlingar och vi bedömer att kvaliteten på de registerförteckningar vi erhållit varierar men är generellt låg. Exempelvis har majoriteten av verksamheterna inte dokumenterat laglig grund för behandling av personuppgifter och vi konstaterar att utan en angiven rättslig grund är personuppgiftsbehandlingen inte laglig. Vi vill även uppmärksamma hälso- och sjukvårdsnämnden på att det inom organisationen råder en okunskap kring vad som utgör känsliga personuppgifter. Exempelvis har patienters diagnoser tolkats som känsliga personuppgifter av en verksamhet men inte av en annan.
Att det finns dokumenterade rutiner som möjliggör för verksamheterna att efterleva lagkrav? Detta innefattar rutiner för att; ▸ hantera utlämning av personuppgifter vid begäran, ▸ inhämta och behandla samtycke där det är aktuellt ▸ genomföra konsekvensbedömning där känsliga personuppgifter förekommer, ▸ tillgodose dataportabilitet och överföra personuppgifter mellan myndigheter, ▸ upptäcka, utreda och rapportera personuppgiftsincidenter, ▸ genomföra systematisk genomgång och uppdatering av personuppgiftsbehandlingar?	Nej. Vi bedömer att styrelsen och nämnden inte säkerställt att det i tillräcklig omfattning finns dokumenterade rutiner som möjliggör för verksamheterna att efterleva lagens krav. På landstingsövergripande nivå har ett antal riktlinjer och mallar upprättats. Exempelvis finns: ▸ Mall för inhämtande av samtycke ▸ Riktlinjer och mallar för hantering av personuppgiftsincidenter. ▸ Mall för upprättande av personuppgiftsbiträdesavtal Vår uppfattning är dock att det saknas ett flertal riktlinjer och rutiner som är av vikt för att tydliggöra hur verksamheten ska säkerställa en lagenlig personuppgiftshantering. Exempelvis saknas dokumentation för följande moment: ▸ hantera utlämning av personuppgifter vid begäran (rätten till registerutdrag), ▸ genomföra konsekvensbedömning där känsliga personuppgifter förekommer, ▸ tillgodose dataportabilitet och överföra personuppgifter mellan myndigheter, ▸ eventuella anpassningar i IT-system, ▸ genomföra systematisk genomgång och uppdatering av personuppgiftsbehandlingar/registerförteckningar

Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt:	Svar
	Vi har i granskningen också sett ett flertal exempel på att verksamheterna behöver kompletterande information och stöd i hur förordningens krav ska efterlevas.
Att styrelsen och nämnden får tillräcklig rapportering om arbetet med att uppfylla kraven i dataskyddsförordningen?	Nej. Vi bedömer att styrelsen och nämnden inte säkerställt att de fått tillräcklig rapportering om arbetet med att uppfylla kraven i dataskyddsförordningen. Bedömningen baseras på att varken styrelsen eller nämnden under året efterfrågat eller erhållit någon information om organisationens anpassningsarbete eller hur förordningens krav efterlevs.
Att tillräckliga åtgärder vidtagits med anledning av revisionens tidigare granskning inom området (rapport nr 14/2017 - Förstudie av förberedelser inför införandet av dataskyddsförordningen)?	Nej. Vi bedömer att styrelsen och nämnden inte säkerställt att tillräckliga åtgärder vidtagits med anledning av revisionens tidigare granskning. Vi uppmärksammar dessutom att revisorernas rapport ännu inte har behandlats av landstingsstyrelsen. Revisorerna bedömde med anledning av förstudiens resultat att det fanns en överhängande risk att nödvändiga anpassningar inte skulle hinna genomföras innan förordningens ikraftträdande 25 maj 2018. Anpassningsarbetet har förvisso nu påbörjats så till vida att roller och ansvar har dokumenterats, ett antal styrande dokument har upprättats och ett inventeringsarbete har påbörjats. Vi bedömer dock att det fortfarande kvarstår mycket arbete innan styrelsen och nämnden har säkerställt och kan visa att samtliga verksamheter efterlever förordningens krav.

Utifrån granskningsresultatet rekommenderar vi landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att:

- Det verkställs en välfungerande *dataskyddsorganisation* som:

  a) Ger verksamheterna tillräckligt *stöd* i anpassningsarbetet.

  b) Ser till att dataskyddsarbetet *samordnas och följs upp*. Detta är nödvändigt för att säkerställa att arbetet bedrivs effektivt och för att säkerställa att styrelsen och nämnden kan ha en tillräcklig kontroll över läget i organisationen.

- Nödvändiga *styrande dokument* (policy/strategi/riktlinjer) upprättas. Detta är nödvändigt eftersom styrelse och nämnd ska kunna visa att de efterlever förordningen samt på vilket sätt detta sker.

Umeå den 5 november 2018

Linda Marklund
Certifierad kommunal revisor
EY

Petra Nylander
Verksamhetsrevisor
EY

Bilaga 1: Källförteckning

Intervjuade funktioner

- Landstingsdirektör
- Stabsdirektör
- Jurist/Dataskyddsombud
- Informationssäkerhetsstrateg/Dataskyddsombud
- Sekreterare och utredare för CSG/Dataskyddsombud
- Projektledare för GDPR inom Folktandvården
- Systemsamordnare/personuppgiftshandläggare inom Barn- och ungdomscentrum
- Verksamhetschef, biträdande verksamhetschef, avdelningschef för medicinsk administration/personuppgiftshandläggare samt tre personuppgiftshandläggare inom Psykiatricentrum
- Verksamhetschef samt kvalitetsansvarig/personuppgiftshandläggare inom IT Västerbotten
- Tillförordnad verksamhetschef och medicinsk sekreterare/personuppgiftshandläggare vid Tegs hälsocentral
- Verksamhetschef och medicinsk administratör/personuppgiftshandläggare vid Ersboda hälsocentral
- Avdelningschef/personuppgiftshandläggare för Lövångers hälsocentral, tillika avvikelseutredare inom Skellefteå-området

Dokumentation

- Förstudie om dataskyddsförordningen (rapport nr 14/2017)
- Landstingsstyrelsens delegationsordning (2017-04-40, § 61)
- Protokoll från landstingsstyrelsen och hälso- och sjukvårdsnämndens sammanträden (2018)
- Minnesanteckningar från ELG (2017-10- 2018-09)
- Förslag till dataskyddsorganisation
- Riktlinje för e-post (2018-06-19, digitaliserings- och teknikdirektören)
- Riktlinje för hur registerförteckning över personuppgiftsbehandlingar ska göras (2018-04-03, landstingsdirektören)
- Riktlinje för personuppgiftshandläggare
- Mall för utredning av personuppgiftsincident
- Rutin för rapportering och utredning av personuppgiftsincident
- Mall för inhämtande av samtycke för bilder, ljud och video
- Mall för upprättande av personuppgiftsbiträdesavtal
- Registerförteckningar från barn- och ungdomscentrum, psykiatricentrum, Lövångers hälsocentral, Tegs hälsocentral samt IT Västerbotten
- Dataskyddsorganisation för IT Västerbotten
- Lista över systemägare och förvaltningsobjekt
- Underlag från systemägare kring personuppgiftsbiträdesavtal samt registerförteckningar
- Lokalt framtagen rutin för GDPR från Psykiatricentrum

Bilaga 2: Revisionskriterier

Kommunallagen

Av kommunallagens 6 kap. § 6 framgår att nämnder och styrelser ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de föreskrifter som gäller för verksamheten. Nämnder och styrelser ska också se till att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Dataskyddsförordningen/GDPR

Dataskyddsförordningen (GDPR) är, efter beslut i Europeiska Unionen (EU), svensk lag den 25 maj 2018 och ersatte därmed personuppgiftslagen (PUL) i Sverige.

Dataskyddsförordningen reglerar, i likhet med PUL, grundläggande bestämmelser om enskildas rätt till skydd av personuppgifter. Att skydda enskildas grundläggande rättigheter och friheter kopplat till personuppgiftshantering är således ett av syftena med dataskyddsförordningen.

Nedan finns en redogörelse av de artiklar i lagstiftningen som utgör revisionskriterier för granskningen.

Principer för behandling av personuppgifter

För landstingets behandling av personuppgifter ska, enligt artikel 5 punkt 1, följande gälla för behandling av personuppgifter:

- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
- Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.
- Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).
- Uppgifterna ska vara korrekta och om nödvändigt uppdaterade.
- Uppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas
- Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).
- Enligt artikel 5 punkt 2 har den personuppgiftsansvarige (ansvarig styrelse eller nämnd) ansvarsskyldighet för att kunna visa att ovanstående punkter efterlevs.

Laglig behandling av personuppgifter

Landstingets behandling av personuppgifter är enligt artikel 6 punkt 1 endast laglig om åtminstone ett av följande villkor är uppfyllt för behandlingen:

a) Den registrerade har lämnat sitt samtycke till behandlingen.

b) Nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade

c) Nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige

d) Nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person

e) Nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning

f) Nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighets utövning. I Sverige finns den lagliga grunden för behandling av personuppgifter inom hälso- och sjukvården huvudsakligen i patientdatalagen.

Missbruksregeln, som fanns i personuppgiftslagen, innebar att det var möjligt att använda enklare regler för personuppgifter i ostrukturerat material, exempelvis information om personer i e-post, på internet eller i en enkel lista som man har i datorn. Samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem gäller i dagsläget också för det som skrivs om personer i exempelvis enklare listor, e-post och på webbplatser.

Villkor för samtycke

I de fall landstinget behandlar personuppgifter som grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter, enligt artikel 7 punkt 1. Enligt artikel 7 punkt 2 ska det tydligt framgå vad den registrerade samtycker till i begriplig och lättillgänglig form. Av artikel 7 punkt 3 framgår att den registrerade när som helst kan återkalla sitt samtycke.

Särskilda kategorier av personuppgifter

Artikel 9 punkt 1 anger att behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

Punkt 1 är inte tillämplig i de fall den registrerade samtyckt till behandling, eller om uppgifterna krävs för att landstinget ska kunna fullgöra sina skyldigheter. I artikel 9 anges även följande undantag som kan beröra landstingets verksamhet:

- Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke
- Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system
- Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits. Artikel 13 reglerar på vilket sätt den registrerade ska informeras om de personuppgifter som samlas in.

Den registrerades rättigheter stärks även enligt följande:

- Rätt att tillgå information om behandlingen (artikel 15)
- Rätt till rättelse (artikel 16)
- Rätt till radering (artikel 17)
- Rätt till begränsning av behandling (artikel 18)
- Rätt till dataportabilitet (artikel 20)
- Rätt att göra invändningar (artikel 21)

Personuppgiftsansvariges ansvar

Enligt artikel 25 ska styrelse och nämnd (i egenskap av personuppgiftsansvarig) genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning.

Artikel 25 reglerar utformningen av inbyggt dataskydd *(privacy by design)*, samt dataskydd som standard (*privacy by default*) är en skyldighet som innebär att hänsyn till integritetsskydd och dataskydd tas i samband med utformandet av system. Denna skyldighet är ett viktigt nytt krav för registeransvariga, som kommer att behöva visa överensstämmelse med förordningen. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

Register över behandling

Enligt artikel 30 ska varje personuppgiftsansvarig föra ett register över behandling som utförts under dess ansvar. Registret ska enligt förordningen innehålla:

- Kontaktuppgifter till den personuppgiftsansvarige
- Syftet med behandlingen
- Beskrivning av kategorierna av registrerade och kategori av personuppgifter
- Kategori av mottagare om uppgifterna lämnats ut, eller ska lämnas ut
- Ev. överföring av personuppgifter till tredje land
- Ev. tidsfrister för radering
- Ev. beskrivning av tekniska och organisatoriska säkerhetsåtgärder

Anmälan av personuppgiftsincident

Enligt SKL är en personuppgiftsincident en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Detta enligt artikel 33.

Vid händelse av säkerhetsincident, exempelvis dataintrång eller oavsiktlig förlust av uppgifter, måste det anmälas till Datainspektionen inom 72 timmar. Vid risk för exempelvis id-stöld eller bedrägeri kan de personer vars personuppgifter berörs behöva informeras.

Dataskyddsombud

Enligt artikel 37 ska den personuppgiftsansvarige och personuppgiftsbiträde under alla omständigheter utnämna ett dataskyddsombud om behandling av personuppgifter genomförts av en myndighet eller offentligt organ. Norstedts handbok i GDPR (*Juridik, organisation och säkerhet enligt Dataskyddsförordningen, 2018)* skriver att beslutet att utse dataskyddsombud av bevisskäl bör dokumenteras skriftligen, samt att dataskyddsombud ska registreras hos tillsynsmyndigheten, Datainspektionen.

Ombudet ska informera och ge råd till den personuppgiftsansvarige och de anställda. Enligt artikel ska ombudet minst ha följande uppgifter:
a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt förordningen.
b) Att övervaka efterlevnaden av förordningen och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.

Utöver detta ska dataskyddsombudet även fungera som kontaktperson för tillsynsmyndigheten, Datainspektionen.

En handbok i GDPR (utgiven av Norstedts juridik, 2018) beskriver att dataskyddsombudet har en särställning inom den organisation som denne är satt att övervaka och stödja. Enligt skriften ska dataskyddsombudet rapportera direkt till organisationens högsta förvaltningsnivå (styrelse och högsta ledning) (s102).

Sanktionsavgift

Vid brytande mot förordningens regler kan Datainspektionen ålägga en sanktionsavgift enligt artikel 83. Avgiftens storlek är bland annat beroende av hur allvarlig överträdelsen är, om det skett avsiktligt eller inte samt vilka åtgärder som vidtagits för att minska skadan. Vid mindre förseelser riskerar den som bryter mot förordningen ett påpekande eller föreläggande om eventuella brister. Anses brottet däremot vara allvarligare, eller om organisationen anses ovillig att vidta nödvändiga åtgärder, riskeras böter upp till 20 miljoner euro eller 4 % av organisationens globala omsättning.

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Lagen med kompletterande bestämmelser till dataskyddsförordningen reglerar att känsliga personuppgifter får behandlas om behandlingen är nödvändig för förebyggande hälso- och sjukvård och yrkesmedicin, medicinska diagnoser, tillhandahållande av hälso- och sjukvård eller behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster, social omsorg samt deras system.

Denna behandling får ske under förutsättning att kravet på tystnadsplikt är uppfyllt.

Landstingsinterna styrande dokument

Vår granskning visar att det inte finns något politiskt antaget styrande dokument som är relevant att göra avstämningar mot, dvs använda som revisionskriterium för denna granskning.