2018-11-19 REV 25:3–2018

Landstingsstyrelsen
Hälso- och sjukvårdsnämnden

Granskning av efterlevnad av dataskyddsförordningen

Granskningen visar att det nyligen påbörjats ett arbete i landstinget i syfte att uppfylla kraven i dataskyddsförordningen. Bland annat har landstingsdirektören godkänt en organisationsbeskrivning för dataskyddsarbetet och verksamheterna har påbörjat ett arbete med att inventera personuppgiftsbehandlingar. Ännu återstår dock mycket arbete för att uppfylla kraven i dataskyddsförordningen. Av granskningen framgår exempelvis följande:

- Det saknas politiskt beslutade styrdokument som tydliggör hur dataskyddsarbetet i landstinget strategiskt ska styras och följas upp.
- Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att riskanalyser tagits fram för dataskyddsarbetet inom sina ansvarsområden.
- Det saknas i landstinget en väl fungerande organisation för dataskyddsarbetet. Stödet till verksamheterna, samordningen och kontrollen över arbetet med att uppfylla kraven i dataskyddsförordningen är svagt utvecklad. Bland verksamheterna finns en generell brist på kunskap om vilka anpassningar som behöver genomföras för att uppfylla kraven i dataskyddsförordningen. Även personuppgiftshandläggare uppger att de behöver mer stöd i dataskyddsarbetet.
- Samtliga verksamheter som ingår i granskningen har inte upprättat register över sina personuppgiftsbehandlingar. Kvaliteten är generellt låg på de registerförteckningar som kontrollerats i granskningen.
- Landstingsstyrelsen och hälso- och sjukvårdsnämnden har hittills under år 2018 inte följt upp hur det går i arbetet med att uppfylla kraven i dataskyddsförordningen.

Vår samlade bedömning är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har haft en tillräcklig styrning och kontroll över dataskyddsarbetet. Med anledning av våra iakttagelser lämnar vi följande rekommendationer till landstingsstyrelsen och hälso- och sjukvårdsnämnden:

- Säkerställ att nödvändiga riskanalyser genomförs för arbetet med att uppfylla kraven i dataskyddsförordningen.

Västerbottens läns landsting
Landstingshuset, Köksvägen 11, 901 89 Umeå
Telefon: 090-785 00 00, telefax: 090-13 68 82
E-post: landstinget@vll.se Org.nr: 232100-0222
VAT-nr: SE232100022201 Bankgiro 5728-3061

- Se till att nödvändiga politiska styrdokument beslutas för dataskyddsarbetet.
- Säkerställ att det på tjänstemannanivå finns nödvändiga regler och rutiner för dataskyddsarbetet.
- Säkerställ att det för dataskyddsarbetet finns en väl fungerande organisation. Se bland annat till att verksamheterna och personuppgiftshandläggare får tillräckligt stöd.
- Säkerställ med hjälp av kontroller att kraven i dataskyddsförordningen efterlevs.
- Se till att dataskyddsarbetet följs upp och utvärderas.

Vid revisorernas överläggning den 19 november 2018 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 3/2018) lämnar revisorerna för yttrande till landstingsstyrelsen. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 4 april 2018.

För landstingets revisorer

Christer Fessé
Ordförande

Bert Öhlund
Vice ordförande

LANDSTINGSREVISIONEN

Granskning av efterlevnad av dataskyddsförordningen

Rapport nr 03/2018

Västerbottens läns landsting

November 2018
Linda Marklund & Petra Nylander, EY
REV 25:2–2018

Building a better working world

Innehåll

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;

- 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.

3.1.2. 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.

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

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.

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:

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.

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
	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 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

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.