Västerbottens läns landsting

VÄSTERBOTTENS LÄNS LANDSTING
Inkom 2018 -01- 31
Dnr:

MISSIV

2018-01-30

REV 46:3–2018

Landstingsstyrelsen
Hälso- och sjukvårdsnämnden

Förberedelser inför ny dataskyddsförordning

I maj 2018 ersätter den nya dataskyddsförordningen (GDPR) personuppgiftslagen. Förordningen innebär stärkta rättigheter och skydd för individen vad gäller information och samtycke samt ett ökat ansvar för personuppgiftsansvariga. De som behandlar personuppgifter ska inte bara följa lagen utan också kunna visa att lagens krav uppfylls.

Tidigare granskningar (rapport nr 20/2012, 25/2012, 22/2014, 13/2015, 18/2015) har visat på brister inom informationssäkerhetsområdet i landstinget. Viktiga funktioner så som informationssäkerhetsstrateg har saknats och det har funnits brister i personuppgiftshanteringen. Revisorerna har genomfört en förstudie med syfte att undersöka om en fördjupad granskning ska göras med anledning av den nya dataskyddsförordningen.

Förstudiens resultat

I förstudien har följande iakttagelser gjorts:

- Det saknas dokumenterade riskanalyser för landstingets arbete med att göra anpassningar till den nya dataskyddsförordningen.
- Det är otydligt på tjänstemannanivå i landstinget om vilka som har ansvar för vad i arbetet med att förbereda landstinget för den nya dataskyddsförordningen.
- Arbetet med förberedelser med anledning av dataskyddsförordningen kom igång sent. Först under hösten 2017 påbörjades vissa förberedelser. Den aktivitetsplan som är beslutad är inte heltäckande.

Förstudien visar att det ännu återstår mycket arbete innan landstingsstyrelsen och hälso- och sjukvårdsnämnden kan visa att kraven i dataskyddsförordningen uppfylls. Med anledning av förstudiens resultat bedömer revisorerna att det finns en risk att nödvändiga anpassningar inte hinner genomföras innan förordningen börjar gälla den 25 maj 2018. I februari år 2018 beslutar revisorerna om sin revisionsplan för året och vilka fördjupade granskningar som ska genomföras.

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

Vid revisorernas överläggning den 30 januari 2018 beslöt revisorerna enhälligt att ställa sig bakom slutsatser i detta missiv. Missiv och förstudie (nr 14/2017) lämnar revisorerna för kännedom till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

För landstingets revisorer

Christer Fessé
Ordförande

Bert Öhlund
Vice ordförande

LANDSTINGSREVISIONEN

Förstudie av förberedelser inför ny dataskyddsförordning (GDPR)

Rapport nr 14/2017

Västerbottens läns landsting

Januari 2018
Linda Marklund och Petra Nylander, Ernst & Young AB
Diarienummer: REV 46:2–2017

Revisionsrapport 2017
Genomförd på uppdrag av revisorerna
januari 2018

Västerbottens läns landsting

Förstudie av förberedelser inför införandet av dataskyddsförordningen (GDPR)

EY
Building a better working world

Building a better working world

Innehåll

1. Sammanfattning 2

2. Inledning 3

2.1. Bakgrund 3
2.2. Syfte och revisionsfrågor 4
2.3. Avgränsning och ansvarig nämnd 5
2.4. Genomförande 5

3. Revisionskriterier 5

3.1. Kommunallagen 5
3.2. Dataskyddsförordningen, samt styrande och stödjande material från Datainspektionen och SKL. 5

4. Granskningsresultat 9

4.1. Tidigare granskningar och vidtagna åtgärder 9
4.2. Organisation samt roll-, ansvars- och befogenhetsfördelning 10
4.3. Arbetet med anpassningar 11

5. Sammanfattning och förslag till granskningsområden 16

5.1. Sammanfattning 16
5.2. Förslag till fördjupad granskning 17
Bilaga 1: Källförteckning 18
Bilaga 2: Förslag till utformning av projektplan 19

Building a better working world

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Västerbottens läns landsting granskat landstingsstyrelsen och hälso- och sjukvårdsnämnden i syfte att ge revisorerna underlag för att kunna besluta om en fördjupad granskning med anledning av den nya dataskyddsförordningen.

I förstudien har följande iakttagelser gjorts:

- Vi kan inte styrka att någon organisation, med tydlig roll-, ansvars- och befogenhetsfördelning avseende införandet av GDPR, har beslutats på formellt sätt.
- Inga dokumenterade och landstingsövergripande riskanalyser har upprättats med anledning av den nya förordningen.
- Vi kan inte styrka att det inom landstinget pågår ett samordnat och heltäckande arbete med anpassningar inför GDPR. Vissa anpassningar har påbörjats under hösten men vår uppfattning är att det fortfarande återstår mycket arbete att genomföra innan landstingets verksamheter kan uppfylla samtliga krav som ställs i den nya dataskyddsförordningen.
- En aktivitetsplan har tagits fram. Denna plan är, enligt vår uppfattning, inte heltäckande för en fullständig implementering av GDPR inom landstingets verksamheter.
- Förslag till styrande dokument har tagits fram. Vid granskningstillfället är dessa dock fortfarande utkast och det finns ingen tidsplan för spridning och implementering av styrdokumenten.

Med anledning av förstudiens resultat är vår uppfattning att det finns en överhängande risk att nödvändiga anpassningar inte hinner genomföras i tid, innan förordningens ikraftträdande 25 maj 2018. Exempelvis behöver följande områden hanteras snarast:

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

Vi föreslår att en eventuell fördjupad granskning fokuseras på huruvida verksamheten lyckats genomföra anpassningarna i tid. Granskningen bör i så fall genomföras under hösten 2018 (augusti/september). För förslag på syfte, revisionsfrågor, metod, genomförande och avgränsningar se bilaga 2, *Förslag till utformning av projektplan.*

Building a better working world

2. Inledning

2.1. Bakgrund

I maj 2018 ersätter den nya dataskyddsförordningen (GDPR) personuppgiftslagen (PUL). Förordningen innebär stärkta rättigheter och skydd för individen vad gäller information och samtycke samt ett ökat ansvar för personuppgiftsansvariga. Med behandling av personuppgifter avses varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

De som behandlar personuppgifter ska inte bara följa den nya lagstiftningen utan ska också kunna visa att de har uppfyllt kraven. Det är en viktig och betydande förändring från passiv till aktiv efterlevnad som vårdgivare bör uppmärksamma. Ett sätt att säkerställa att personuppgiftsbehandlingen är i överensstämmelse med lagstiftningen kan vara att anta uppförandekoder, interna riktlinjer och förfaranden. De viktigaste principerna för skydd av personuppgifter är; laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet samt ansvarsskyldighet[1].

Revisorerna har i upprepade granskningar åren 2012 – 2014 (rapport nr 20/12, 25/12, och 22/14) uppmärksammat brister i hantering av personuppgifter. Exempelvis framkom att anvisningar för behandling av personuppgifter inte fanns på intranätet, personuppgifter var inte åtkomstskyddade i Platina och hanterades inte korrekt. Uppföljningen var också svag samt att viktiga funktioner så som informationssäkerhetsansvarig och personuppgiftsombud var vakanta.

År 2015 genomförde revisorerna en uppföljande granskning som var inriktad mot om styrelser och nämnder vidtagit tillräckliga åtgärder för att säkra att inte obehöriga tog del av sekretessuppgifter i kund- och leverantörsfakturaprocessen (13/2015). Granskningen visade på brister i hanteringen och att utbildning i den inre sekretessen krävdes. I yttrandena från styrelsen och nämnder fick landstingsdirektören i uppdrag att hitta en lösning till en funktionalitet i Agresso för att kunna sekretessmarkera fakturor på ett annat sätt än idag. Ekonomienheten skulle också arbeta fram ett förslag till hur stickprov skulle tas samt uppdatera rutiner. I oktober 2016 återrapporterades att flera av uppdragen ännu inte hade genomförts. Arbeten var på gång som skulle vara klara under hösten 2016 och våren 2017.

Granskning av IT-behörigheter år 2015 (rapport nr 18/2015) visade att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt en tillräcklig kontroll av personalens behörigheter till journalsystemet. Av fyra kontrollerade basenheter saknade alla dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter till IT-system. I yttrande över granskningen medgav nämnderna att landstinget saknade en funktion i landstinget som samordnar frågor kring informationssäkerhet. Landstingsdirektören fick i uppdrag att genomföra en förstudie som skulle återrapporteras till landstingsstyrelsen februari 2017. I förstudien skulle den kommande dataskyddsförordningen beaktas.

[1] SKL:s informationsskrift; *Förändringar för hälso- och sjukvården genom EU: s dataskyddsförordningen GDPR.*

Rapporten om informationssäkerhet (genomförd av extern konsult) redovisades i november 2016 för exekutiv ledningsgrupp (ELG) och i februari 2017 för landstingsstyrelsen. Rapporten visade på stora brister i landstingets arbete med informationssäkerhet (VLL 2506:1–2016). Landstinget saknade en policy för informationssäkerhet och en ledning och organisation som håller ihop arbetet med informationssäkerheten. En slutsats i förstudien var att åtgärder måste vidtas och att landstinget måste påbörja förberedelserna inför den nya dataskyddsförordningen.

Landstingsdirektören beslutade 12 december 2016 att inleda rekrytering av en informationssäkerhetsstrateg. I samband med att rapporten redovisades för styrelsen i februari 2017 fick landstingsdirektören i uppdrag att i april 2017 återkomma till styrelsen med en handlingsplan utifrån vad som framkommit av rapporten. I april 2017 godkände landstingsstyrelsen redovisningen av handlingsplanen och begärde en lägesrapport av informationssäkerhetsarbetet i december 2017.

Hösten 2016 genomförde IVO en tillsyn av informationssäkerhetsarbetet vid Medicinskt centrum. Den samlade bedömningen var att vårdgivarens och verksamhetens systematiska informationssäkerhetsarbete inte fungerade fullt ut utifrån SOSFS 2008:14. IVO ställde krav på att vårdgivaren skulle utse minst en person som ansvarar för informations-säkerhetsarbetet och att den personen ska rapportera till vårdgivaren om granskningar, riskanalyser och förbättringsåtgärder (enligt SOSFS 2008:14). I yttrande över granskningen svarade landstinget att rekrytering av informationssäkerhetsstrateg pågick och vilket ansvar strategen skulle ha för uppföljning och rapportering. Vidare framfördes i patientsäkerhets-berättelsen vilka åtgärder och granskningar som genomförts inom informationssäkerhets-området under år 2016. I augusti 2017 började en ny informationssäkerhetsstrateg på ledningsstaben.

Revisorerna bedömer att det, mot bakgrund av ovanstående, finns en risk att verksamheten inte hinner genomföra alla nödvändiga förberedelser innan den nya dataskyddsförordningen träder i kraft.

2.2. Syfte och revisionsfrågor

Förstudien syftar till att ge revisorerna underlag för att kunna besluta om en fördjupad granskning med anledning av den nya dataskyddsförordningen. Förstudien ska innehålla:

- Identifierade risker för Västerbottens läns landsting med anledning av den nya dataskyddsförordningen
- Förslag på syfte och revisionsfrågor
- Förslag på metod, genomförande och avgränsningar

I förstudien besvaras följande frågor översiktligt utifrån syftet att identifiera angelägna områden för djupgranskning.

- Vilka riskanalyser är gjorda med anledning av den nya dataskyddsförordningen och vilka är de identifierade riskerna?
- Finns det en ändamålsenlig organisation med tydlig roll-, ansvars- och befogenhetsfördelning för att hantera införandet av den nya dataskyddsförordningen?
- Har styrdokument som t.ex. uppförandekoder, riktlinjer och rutiner upprättats?
- Finns det en plan för implementeringen av dataskyddsförordningen som inbegriper alla berörda verksamheter?

- Har nödvändiga anpassningar påbörjats i rimlig omfattning?

2.3. Avgränsning och ansvarig nämnd

I förstudien besvaras revisionsfrågorna översiktligt utifrån syftet att identifiera angelägna områden för djupgranskning.

Förstudien avser landstingsstyrelsen och hälso- och sjukvårdsnämnden.

2.4. Genomförande

Förstudien har genomförts genom analys av relevant dokumentation. För specifikation av dokumentation se Källförteckning, bilaga 1.

Vidare har intervjuer genomförts med verksamhetschef för basenhet informatik, informationssäkerhetsstrateg, jurist, ledningsstabsdirektören, landstingsdirektör samt enterprisearkitekt.

3. Revisionskriterier

Med revisionskriterier avses de grunder mot vilka resultatet i förstudien ställs mot.

3.1. Kommunallagen

Av kommunallagens 6 kap. §7 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.

3.2. Dataskyddsförordningen, samt styrande och stödjande material från Datainspektionen och SKL.

Dataskyddsförordningen (GDPR) blir, efter beslut i Europeiska Unionen, svensk lag den 25 maj 2018 och ersätter 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.

Enligt Sveriges Kommuner och Landsting (SKL) är en viktig skillnad mellan PUL och GDPR att organisationer kommer att behöva förändra sitt arbetssätt från passiv till aktiv efterlevnad, vilket bör uppmärksammas av vårdgivare. Utöver att efterleva regelverket ställer förordningen krav på att en organisation aktivt ska kunna visa att regler efterlevs. Detta kan enligt SKL göras genom att anta uppförandekorder eller interna styrande dokument.

En stor del av bestämmelserna i dataskyddsförordningen överensstämmer med tidigare bestämmelser enligt PUL, men några viktiga förändringar finns. Nedan sammanfattas de huvudsakliga förändringarna för organisationer[2] i korthet.

- **Laglig behandling** - Enligt förordningen måste en organisation numera kunna ange en laglig grund för sin behandling. En viktig förändring är också att som laglig behandling

[2] Dataskyddsförordningen gäller i princip inom all slags verksamhet och oavsett vem som utför personuppgiftsbehandlingen. Den gäller således för företag, föreningar, organisationer, myndigheter och privatpersoner. I detta avsnitt används begreppet organisation, vilket även innefattar landsting.

räknas inte längre den intresseavvägning som myndigheter tidigare kunde åberopa som grund för sin behandling när de utför sina uppgifter. I Sverige finns den lagliga grunden för behandling av personuppgifter inom hälso- och sjukvården huvudsakligen i patientdatalagen. Andra grunder är avtal, samtycke, rättslig förpliktelse eller skydd av vitala intressen.

- **Regler om inbyggt dataskydd, och dataskydd som standard** – *Privacy by design,* samt *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.

- **Samtycke -** Dataskyddsförordningen bygger i stor utsträckning på att aktivt samtycke till registrering lämnas från den enskilde. I förordningen ställs särskilda krav på hur samtycke ska lämnas, i synnerhet vid behandling av känsliga personuppgifter (såsom uppgifter om hälsa eller religiös åskådning). Den som behandlar personuppgifter måste kunna visa att giltigt samtycke har lämnats av den som har registrerats.

- **Ökade rättigheter -** Enligt dataskyddsförordningen har den registrerade rätt att när som helst begära att få sina uppgifter raderade, med undantag för om det inte föreligger någon rättslig grund för behandlingen. Undantagsfall kan uppstå i de fall organisationen som hanterar personuppgifter behöver dessa för exempelvis bokföringsändamål. Med tanke på de ökade kraven som ställs på att de registrerade enkelt ska kunna få sina uppgifter raderade bör organisationen enligt Datainspektionen se över rutiner gällande hur en sådan begäran hanteras.

- **Dataportabilitet** – när uppgifter behandlas med stöd av samtycke eller för att uppfylla ett avtal, ska den registrerade ha rätt att få ut de uppgifter som lämnats för att överföra dem till en annan tjänst.

- **Konsekvensbedömning** – innan man planerar en ny personuppgiftsbehandling, vilken innebär särskilda risker för den registrerade, ska en bedömning göras av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska risker för den enskilde.

- **Anmälan om personuppgiftsincident**[3] – 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/DPO** – vissa organisationer som behandlar känsliga uppgifter, eller är involverade i särskilt riskfylld behandling av personuppgifter, måste utse en person i organisationen som har som särskild uppgift att bevaka dataskyddsfrågor – ett dataskyddsombud. Ombudet har bland annat till uppgift att utföra kontroller och informationsinsatser. Ombudet ska vara väl insatt i de lagar som gäller för personuppgiftsbehandling.

[3]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

- **"Missbruksregeln" försvinner** – När dataskyddsförordningen träder ikraft kommer den så kallade missbruksregeln inte längre finnas kvar. Missbruksregeln innebär att det idag är 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. När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på webbplatser. Det kommer att innebära krav på att bland annat ha en rättslig grund för hantering av personuppgifter, krav på att informera de registrerade samt föra register över sina behandlingar.

- **Sanktionsavgift** – vid brytande mot förordningens regler kan Datainspektionen ålägga en sanktionsavgift. 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.

- **Nya definitioner för personuppgifter** – I dataskyddsförordningen anges tre nya definitioner av personuppgifter med stark koppling till hälso- och sjukvården; uppgifter om hälsa, genetiska uppgifter samt biometriska personuppgifter. Uppgifter om hälsa avser enligt SKL personuppgifter som rör en fysisk persons fysiska/psykiska hälsa eller information om tillhandahållandet av hälso- och sjukvårdstjänster. SKL uppger vidare att samtliga personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, som framför allt härrör från analys av biologiskt prov är att betrakta som personuppgifter.

3.2.1. Datainspektionens vägledning

Datainspektionen är tillsynsmyndighet när det gäller landstingens hantering av personuppgifter. Enligt Datainspektionens vägledning behöver landstingen bl.a. förbereda sig inför Dataskyddsförordningens ikraftträdande på följande vis:

- Försäkra sig om att beslutsfattare och nyckelpersoner inom organisationen är medvetna om att personuppgiftslagen kommer att ersättas av dataskyddsförordningen. Således krävs att organisationen undersöker hur GDPR kommer att påverka organisationen, för att därefter identifiera de områden som måste arbetas särskilt med.

- Inventera och dokumentera vilka personuppgifter som hanteras, hur de samlas in och till vem uppgifterna lämnas ut. Datainspektionen rekommenderar en bred översyn för att ta reda på vilka uppgifter som behandlas och hanteras inom de olika delarna av organisationen.

- Undersök om verksamheten har utnyttjat personuppgiftslagens undantag för att behandla personuppgifter i ostrukturerat material, den så kallade missbruksregeln, då denna regel inte kommer att finnas kvar när förordningen träder i kraft. Undersök särskilt om behandling som idag stödjer sig på missbruksregeln är förenlig med dataskyddsförordningens bestämmelser.

- Granska den information som lämnas till enskilda vars personuppgifter registreras, och fundera över vilka förändringar av den informationen som kan bli nödvändig att göra.

Building a better working world

- Se över rutiner för att säkerställa att alla rättigheter som de registrerade har enligt dataskyddsförordningen kan uppfyllas, som exempelvis hur personuppgifter raderas och hur uppgifter lämnas ut elektroniskt i ett allmänt använt format.
- Undersök vilka olika typer av uppgifter som behandlas och med vilket rättsligt stöd detta görs. Dokumentera slutsatserna.
- Undersök på vilket sätt samtycke inhämtas, vilken information som lämnas och hur uppgiften om att samtycke har lämnats av den registrerade sparas och dokumenteras.
- Fundera på hur kontroll av en persons ålder ska göras och hur vårdnadshavares samtycke inhämtas i samband med behandling av barns personuppgifter online.
- Säkerställ att det finns tillräckliga rutiner för att upptäcka, rapportera och utreda personuppgiftsincidenter.
- Analysera om personuppgiftsbehandling är förenad med särskilda risker för enskildas stärkta fri- och rättigheter, och om det i så fall behöver göras en konsekvensbedömning avseende dataskydd.
- Ta hänsyn till dataskyddsförordningens regler när nya IT-system tas fram eller befintliga förändras. Det ger en större möjlighet att följa reglerna, höja säkerheten och förhindra onödiga framtida kostnader.
- Fastställ var i organisationen som ansvaret för dataskyddsfrågor ska ligga. Utse ett dataskyddsombud.

4. Granskningsresultat

4.1. Tidigare granskningar och vidtagna åtgärder

Revisionen har, vid ett flertal tidigare tillfällen, granskat olika delar av landstingets hantering av personuppgifter. Granskningen visar att endast ett fåtal åtgärder vidtagits med anledning av revisorernas iakttagelser i dessa granskningar.

Granskning av *vårdgivarens informationssäkerhet* (rapport nr 20/2012) genomfördes med syfte att bedöma om ansvarig vårdgivare i landstinget har säkerställt att landstinget har rutiner och kontroller som innebär att patientdata hanteras på korrekt sätt i förhållande till Socialstyrelsens föreskrifter och patientdatalagen. Granskningen resulterade i bedömningen att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte i tillräcklig utsträckning säkerställt rutiner och kontroller som innebär att patientuppgifter behandlas på ett korrekt sätt, i förhållande till tidigare nämnda krav. I granskningen framkom brister i form av avsaknad av arbetsbeskrivning för dåvarande informationssäkerhetsansvarig och avsaknad av årlig rapportering av relevanta förbättringsåtgärder. Granskningen visade även att anvisningar för loggkontroller inte följdes. Ytterligare en brist var att periodisk granskning av behörigheter inte utfördes på samtliga enheter.

År 2012 granskades landstingets *hantering av personuppgifter* (rapport nr 25/2012) av landstingsrevisionen. I granskningen gjordes bedömningen att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte hade en tillfredsställande styrning och uppföljning av att landstingets hantering personuppgifter var förenlig med gällande lagstiftning. I granskningen framkom bland annat att ansvarsfördelningen mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden inte var definierad. Vidare framkom att personuppgiftsombudet för VLL saknade ett skriftligt uppdrag som specificerade uppdragets omfattning, eller vilka nämnder som företräds av ombudet. Utöver detta framgår av granskningen ett behov av att se över riktlinjer och hantering, då det saknades förutsättningar för personuppgiftsbiträdesavtal. Slutligen uppdagades brister i styrelsens och nämndens uppföljning och kontroll.

År 2014 genomfördes en uppföljande granskning av de ovan nämnda rapporterna *informationssäkerhet och hantering av personuppgifter* (rapport nr 22/2014). Granskningen visade att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit åtgärder med anledning av tidigare identifierade brister. Bland annat framkom att varken styrelsen, nämnden eller landstingsdirektören under de senaste åren före granskningstillfället fått rapporteringar av betydelse för informationssäkerhetsarbetet i landstinget. Enligt uppgift fanns ej heller uppföljning att tillgå, som visar i vilken utsträckning verksamheterna efterlever riktlinjer för informationssäkerhet. Ej heller genomfördes någon uppföljning av hur hantering av personuppgifter görs, enligt granskningsrapporten. Stickprov visade enligt rapporten fortsatta brister i genomförande av loggkontroller för behörigheter.

Landstingets revisorer genomförde en uppföljande granskning av *sekretess i leverantörs- och faktureringsrutinen* i januari 2016 (rapport nr 13/2015). I granskningen uppmärksammades *fortsatta brister* i sekretessmarkering på fakturor, i synnerhet inom hjälpmedelsverksamhet, samt fakturor med koppling till laboratorieverksamhet. Enligt granskningen hade de granskade nämnderna och styrelsen inte tillräcklig kontroll över hur verksamheter hanterade känsliga personuppgifter. Bland annat framkom att personer som avslutat sin anställning fortfarande hade tillgång till journalsystemet.

I rapport nr 18/2015 granskades *behörigheter till journalsystemet*. Granskningen visade att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt en tillräcklig kontroll av

personalens behörigheter till journalsystemet. Samtliga kontrollerade basenheter saknade dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter.

I revisorernas granskning av *IT-systemens robusthet* (rapport nr 03/2017) bedömde revisorerna att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt en tillräcklig styrning, uppföljning och kontroll av IT-systemen. När det gäller informationssäkerhet och skydd av personuppgifter identifierades följande brister:

- tillräcklig styrning, uppföljning och kontroll av informationsarbetet har inte säkerställts
- ändamålsenlig rapportering för arbetet med informationssäkerhet har inte säkerställts
- ändamålsenlig kommunikation och utbildning gällande riktlinjer för informationssäkerhet har inte säkerställts
- dokumenterade uppdragsbeskrivningar för personuppgiftsombud och informationssäkerhetsstrateg har inte säkerställts
- övergripande informationssäkerhetspolicy har inte fastställts

Landstingsstyrelsen har ännu inte avlämnat något svar på denna granskning.

I februari 2017 presenterades en *förstudie om informationssäkerhet* för landstingsstyrelsen som genomförts av en extern konsult. Den sammantagna bedömningen var att det *saknades en sammanhållen strategisk bild av arbetet med informationssäkerhet* inom landstinget. Förstudien berörde även den nya dataskyddsförordningen och bland annat lämnades följande rekommendationer med anledning av denna:

- förbered organisationen på kommande förändringar
- vidta åtgärder som visar strukturer för att kommande regelverk efterlevs i praktiken
- analysera dataskyddsförordningens påverkan på verksamheterna
- analysera var ett dataskyddsombud ska tillsättas
- informera hela organisationen om vad förändringen innebär

Landstingsstyrelsen beslutade utifrån förstudien att ge landstingsdirektören i uppdrag att utarbeta en handlingsplan (2017-02-02, § 17). Landstingsstyrelsen godkände 2017-04-04, § 52) handlingsplan för informationssäkerhetsarbete (se avsnitt 4.3.2). Vidare fick landstingsdirektören i uppdrag att lämna en lägesbeskrivning av informationssäkerhetsarbetet vid landstingsstyrelsens sammanträde i december 2017.

4.2. Organisation samt roll-, ansvars- och befogenhetsfördelning

4.2.1. Organisation, ansvar och roller

Politisk nivå

Av landstingsstyrelsens reglemente (reviderat av fullmäktige 2015-06-16, § 93) framgår att styrelsen leder och samordnar förvaltningen av landstingets angelägenheter och har uppsikt för hela landstingets utveckling och ekonomiska ställning. Vidare anges att styrelsen har ett övergripande ansvar att tillse att verksamheten bedrivs i enlighet med de mål, riktlinjer och uppdrag som landstingsfullmäktige har bestämt, gällande lagstiftning och reglementet.

Styrelsens reglemente anger vidare att styrelsen ansvarar för de informationssystem som stödjer landstingets verksamhet. Utöver detta framgår att styrelsen ska utarbeta risk- och sårbarhetsanalyser för sitt ansvarsområde. Styrelsen är även personuppgiftsansvarig för de personuppgifter styrelsen behandlar, enligt personuppgiftslagen. Enligt reglementet är styrelsens arbetsutskott beredningsorgan för åtgärder inom IT.

Av hälso- och sjukvårdsnämndens reglemente (reviderat av fullmäktige 2016-02-16, § 25) framgår att nämnden är verksamhetsansvarig för den verksamhet som bedrivs inom områdena Sjukhusvård och Tandvård. I uppdraget ligger ansvar för att tillse att den interna kontrollen är tillräcklig, samt att säkerställa att verksamheterna bedrivs i enlighet med lag och av fullmäktige beslutade mål och riktlinjer. I reglementet anges vidare att nämnden är personuppgiftsansvarig för de personuppgifter som nämnden behandlar, enligt personuppgiftslagen.

Tjänstemannanivå
Granskningen visar att landstingsstyrelsen i april 2015 (2015-04-07, § 66) har tillsatt ett *personuppgiftsombud* för styrelsen. Även nämnden för funktionshinder och habilitering har utsett samma personuppgiftsombud (2015-02-15, § 34), likväl som hälso- och sjukvårdsnämnden (2017-04-15, § 69). Av intervjuer framgår vidare att landstingsdirektören i augusti 2017 har tillsatt en *informationssäkerhetsstrateg*.

I den handlingsplan (LST 2017-04-04 § 52) som upprättats med anledning av förstudie av informationssäkerhet anges att *informationssäkerhetsstrateg mfl* är ansvarig för arbetet med att upprätta en handlingsplan för införandet av GDPR.

Personuppgiftsombud och informationssäkerhetsstrateg uppger vid intervjuer att de fått ett muntligt uppdrag av en enhetschef inom ledningsstaben att påbörja ett arbete med förberedelser inför GDPR. Enligt personuppgiftsombudet ska denne och informationssäkerhetsstrategen fungera som stödfunktioner i verksamheternas arbete med införandet av GDPR. De intervjuade uttrycker inga oklarheter när det gäller befogenheter. Dock har arbetet relativt nyligt påbörjats och de upplever uppdraget när det gäller arbetet med förberedelserna som otydligt. Främst upplevs följande som otydligt:

- Det har inte kommunicerats eller tydliggjorts hur respektive verksamhet ska arbeta med området.
- Det är inte tydligt samordnat var ansvaret för förberedelserna ligger, eller vilka förväntningar som finns på verksamheterna.

Även av intervjuer med basenhet Informatik framgår att det finns en upplevelse av att uppdraget och ansvarsfördelningen inför införandet av dataskyddsförordningen är otydlig på övergripande nivå, samt även mellan verksamheter inom basenheten.

Av intervjuer med personuppgiftsombud (tillika jurist), genomförda i november 2017, framgår att det pågår ett arbete med att ta fram underlag för hur rollen som dataskyddsombud ska fungera, samt utses av nämnder. Tidsplanen för arbetet är, enligt intervjuad, oklar.

4.3. Arbetet med anpassningar

Av intervjuer framgår att arbetet med anpassningar inför den nya dataskyddsförordningen har påbörjats först under hösten 2017. Vid intervjuer framkommer vidare att det inte finns en samsyn i hur anpassningar som tar hänsyn till alla perspektiv i GDPR ska genomföras inför att dataskyddsförordningen träder i kraft. Bland annat råder delade meningar kring hur olika perspektiv (såsom informationssäkerhet, digital säkerhet och dataskydd) ska inkluderas i förberedelsearbetet. Intervjuade beskriver även en viss oro över att förberedelsearbetet inte genomförs med ett helhetsperspektiv.

Enligt uppgift från förvaltningen kommer det vara svårt att säkerställa att samtliga IT-system har systemuppdateringar som är kompatibla och anpassade efter GDPR. GDPRs regler

kring inbyggt dataskydd och dataskydd som standard (privacy by design samt privacy by default) uppges vara svårt att uppnå inom angiven tidsram.

Intervjuade vid basenhet Informatik uppger att det finns en stor medvetenhet inom basenheten om att dataskyddsförordningen innebär stora utmaningar avseende IT-system. En brist som uppges är att det inte finns resurser att genomföra nödvändiga förändringar inom verksamheterna.

I kommande avsnitt beskrivs de insatser/aktiviteter som hittills genomförts.

4.3.1. Inventering av informationstillgångar

Vi har tagit del av underlag som styrker att en säkerhetsanalys har genomförts för ett system. Enligt förvaltningen pågår arbete med säkerhetsanalys för två andra system, som enligt uppgift ska vara genomförda innan årsskiftet 2017/2018. Enligt en förteckning över förvaltningsobjekt (system) inom basenhet Informatik finns minst 38 system. I granskningen har vi inte undersökt hur många system som totalt finns inom landstinget.

4.3.2. Genomförda informationsinsatser

Politisk nivå
Granskningen visar att landstingsstyrelsen i december 2017 (2017-12-12, § 255) av landstingsdirektören har fått en uppdatering av genomförda åtgärder med anledning av dataskyddsförordningen. Detta i samband med återrapportering av handlingsplan för informationssäkerhet (se avsnitt 4.1). Av återrapporteringen framgår bl.a. att det inom förvaltningen har förts diskussioner om att ta fram en områdesövergripande GDPR-strategi. Vidare anges att en handlingsplan för arbetet med dataskyddsförordningen har kommunicerats med ELG och att det pågår en utredning för hur en övergripande GDPR-process med ansvar ska utformas.
Av protokollet framgår även att bland annat följande informationsinsatser har genomförts i organisationen:

- Notis har publicerats på LINDA
- Kort film om vad personuppgiftsbehandling innebär har publicerats på Lärande landsting
- Flera nyckelfunktioner har informerats. Enligt underlaget ges information löpande, till personer ute i verksamheterna.
- Chefläkare har informerats.

Förutom ovanstående noterar vi att styrelsen uppmärksammats på förestående förändringar i september 2017, i samband med behandling av följande ärenden:

- Landstingsstyrelsens yttrande över remissen SOU 2017:49 *EUs dataskyddsförordning och utbildningsväsende* (2017-09-12, § 168). Av yttrandet framgår att styrelsen inte hade synpunkter på SOU 2017:49.
- Landstingsstyrelsens yttrande över remissen *Personuppgiftsbehandling för forskningsändamål SOU 2017:50* (2017-09-12, § 170). I yttrandet efterfrågar styrelsen vägledning för att ytterligare analysera enskildas möjligheter att motsätta sig behandling av personuppgifter.

Verksamhetsnivå
Av våra intervjuer framgår att informationssäkerhetsstrateg och personuppgiftsombud har genomfört informationssatsningar till verksamheter som efterfrågat utbildning med koppling till GDPR. Bland annat uppges rutinen för personuppgiftsincidenter behandlats vid dessa

tillfällen. De intervjuade upplever att det finns ett generellt behov av att bredda kunskapen i organisationen, för att kompetensen i personuppgiftsrelaterade frågor ska öka i verksamheterna.

Informationssäkerhetsstrateg och personuppgiftsombud har vid ovan nämnda informationstillfällen även informerat verksamheterna om vikten av att påbörja inventering av vilka personuppgifter som behandlas i respektive verksamhet. Personuppgiftsombudet har publicerat en blankett på blanketthotellet för inrapportering av personuppgifter, som riktar sig till verksamheterna. Vidare uppges att kontakt har tagits med samtliga systemägare och forskningsenheten, i syfte att informera om kommande lagkrav.

4.3.3. Upprättade styrdokument

I den handlingsplan för informationssäkerhet som godkänts av landstingsstyrelsen 2017-04-04 §52 anges att en tidsplan för införandet av GDPR ska upprättas efter rekryteringen av informationssäkerhetsstrateg. Kontroll av arbetet ska, enligt handlingsplanen, genomföras i maj 2018.

GDPR-aktivitetsplan
Granskningen visar att GDPR-aktivitetsplan har upprättats och behandlats vid ELGs sammanträde 2017-10-21 (punkt 61).

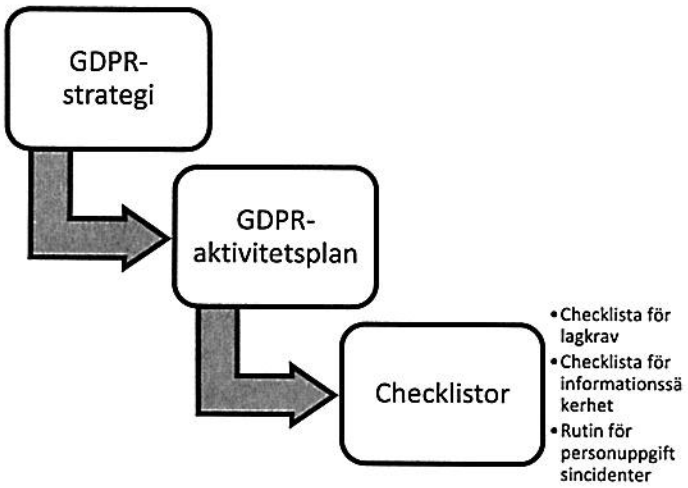
I aktivitetsplanen anges några huvudsakliga förändringar som landstinget kommer att behöva hantera. För varje förändring anges nuläge, vilka som berörs, vilka aktiviteter som krävs, vem som ska genomföra aktiviteterna samt en tidsplan.

Av planen framgår att det i dagsläget saknas en dataskyddsorganisation. Enligt planen är det i dagsläget oklart om rutiner och system för personuppgiftsincidenter finns, vilket enligt planen är ett område som omfattar alla medarbetare. Vidare uppges det även vara oklart hur det inbyggda dataskyddet ska uppnås, vilket bland annat innefattar uppgifts- och lagringsminimering, gallring och behandling.

Enligt planen är en angelägen aktivitet att kontrollera på vilken laglig grund som personuppgifter behandlas. I nuläget uppges inte ändamålen för personuppgiftshantering vara fastställd, trots att laglig grund oftast finns, dock ej dokumenterad eller definierad.

Övriga styrdokument
Utkast för arbetet med GDPR
I granskningen har vi, utöver ovanstående handlingsplaner, tagit del av ett antal dokument som framtagits av informationssäkerhetsstrateg och personuppgiftsombud i syfte att förbereda organisationen på förändringar i och med GDPR. Av intervjuer framgår dock att dessa dokument fortfarande är att betrakta som utkast och de har inte börjat tillämpas i organisationen.

Enligt intervjuade ska arbetet med införandet av GDPR fortlöpa genom att styrande dokument enligt figur 1, upprättas och följs.



Samtliga dokument i figur 1, förutom GDPR-aktivitetsplan, är enligt förvaltningen utkast och därmed arbetsmaterial.

Figur 1. Schematisk bild över processen för dataskyddsförordningen inom VLL

Ledning och styrmodell för informationssäkerhet samt säkerhetsanalys av informationstillgångar.
Förvaltningen uppger att även dokumenten Ledning och styrmodell för informationssäkerhet samt säkerhetsanalys av informationstillgångar är relevanta för arbetet med GDPR. Av dokumenten framgår inte till vilka dessa riktas, när de har tagits fram eller hur dessa ska spridas.

Ledning och styrmodell för informationssäkerhet syftar till att säkerställa systematisk och effektiv styrning av informationssäkerhet i landstingets verksamheter och informationssystem. Vidare framgår att målet med modellen är att förebygga kända risker och minimera skador vid säkerhetshändelser. Ansvar och befogenheter för styrelse och nämnder, informationsägare, systemägare och informationssäkerhetsstrateg beskrivs.

I säkerhetsanalys av informationstillgångar (ännu utkast) anges hur säkerhetsanalys av informationstillgångar ska genomföras, med stöd i form av checklistor och mallar. Riskanalyser är enligt förvaltningen en del i genomförandet av säkerhetsanalys för informationstillgångar.

Riktlinjer för informationssäkerhet
Inom landstinget finns två *riktlinjer för informationssäkerhet* (Användare och Förvaltning och drift) som reglerar personuppgiftsombudets uppdrag samt i viss utsträckning reglerar hantering av personuppgifter. Dessa omfattar dock inte specifikt arbetet med anpassningar inför GDPR.

Riktlinjer – Användare har fastställts av styrelsen 2016-10-25 § 204 och Hälso- och sjukvårdsnämnden har informerats om riktlinjerna 2016-02-10, § 16. Dokumentet omfattar samtliga anställda i landstinget. Av riktlinjen framgår att dokumentet tydligt ska definiera informationssäkerhetsorganisationen, samt utgöra ett stöd i utformandet av rutiner på informationssäkerhetsarbetet. Bland annat uppges i riktlinjen att samtliga personuppgiftsbehandlingar inom landstinget skall föras in i en förteckning.

Riktlinjer – Förvaltning och drift har fastställts av styrelsen 2015-11-18, § 259 och Hälso- och sjukvårdsnämnden har informerats om riktlinjerna 2016-02-10, § 16. Dokumentet omfattar landstingets ledning samt förvaltningsorganisationen av informationssäkerhetsarbetet. Av dokumentet framgår att syftet med riktlinjerna är att säkra hantering och bearbetning av information för att uppnå önskad tillgänglighet, riktighet, sekretess och spårbarhet. Vidare uppges syftet vara att information skyddas mot obehörig åtkomst. Riktlinjen redogör för ansvar och befogenheter för landstingsfullmäktige, styrelse och nämnder, verksamhetschef, systemförvaltning samt personuppgiftsombud.

Building a better working world

5. Sammanfattning och förslag till granskningsområden

5.1. Sammanfattning

Revisionsfråga	Svar
Finns det en ändamålsenlig organisation med tydlig roll-, ansvars- och befogenhetsfördelning för att hantera införandet av den nya dataskyddsförordningen?	Nej. Av våra intervjuer med personuppgiftsombud och informationssäkerhetsstrateg framkommer att de har fått ett muntligt uppdrag av en enhetschef inom ledningsstaben att påbörja förberedelser inför GDPR. Uppdraget upplevs dock som otydligt. Vi noterar även att de vi intervjuat vid basenhet Informatik upplever att det inte är tydligt vilka förväntningar som finns på verksamheterna att påbörja egna arbeten. Vi kan inte styrka att någon organisation, med tydlig roll-, ansvars- och befogenhetsfördelning avseende införandet av GDPR, har beslutats på formellt sätt.
Vilka riskanalyser är gjorda med anledning av den nya dataskyddsförordningen och vilka är de identifierade riskerna?	Inga dokumenterade och landstingsövergripande riskanalyser har upprättats med anledning av den nya förordningen. Vi ser dock att nödvändiga förändringar har identifierats, bl.a. följande: ► Landstinget behöver kontrollera på vilken laglig grund personuppgifter behandlas samt hur landstinget ska uppnå en dataskyddsorganisation. ► Landstinget behöver analysera hur personuppgiftsincidenter ska hanteras och hantera den utökade förteckningsskyldigheten.
Finns det en plan för implementeringen av dataskyddsförordningen som inbegriper alla berörda verksamheter?	Nej. En aktivitetsplan för införandet av GDPR har upprättats. I denna anges bl.a. vilka förändringar som kommer att behöva genomföras med anledning av GDPR. Enligt intervjuade har planen inte ännu kommunicerats till samtliga berörda i verksamheterna och har inte heller börjat tillämpas. Denna plan är, enligt vår uppfattning, inte heller heltäckande för en fullständig implementering av GDPR inom landstingets verksamheter.
Har styrdokument som t.ex. uppförandekoder, riktlinjer och rutiner upprättats?	Nej. Förutom GDPR-aktivitetsplan har ett antal styrdokument upprättats. Som exempel kan nämnas GDPR-strategi och checklista för GDPR-förberedelser. Dessa är dock fortfarande utkast och det finns vid förstudiens genomförande ingen tidsplan för spridning och implementering av styrdokumenten.
Har nödvändiga anpassningar påbörjats i rimlig omfattning?	Nej. Vi kan inte styrka att det inom landstinget ännu pågår ett samordnat och heltäckande arbete med anpassningar.

	Vi noterar att arbetet med förberedelserna har påbörjats först under hösten 2017, efter rekrytering av informationssäkerhetsstrateg. Som exempel på anpassningar som påbörjats kan nämnas: ► Säkerhetsanalyser av landstingets system (för närvarande endast ett system). ► Utkast till styrdokument har upprättats. ► Blankett för inrapportering av personuppgifter har lagts ut på blanketthotellet. Vi noterar dock att det fortfarande återstår mycket arbete att genomföra innan landstingets verksamheter kan uppfylla samtliga krav som ställs i den nya dataskyddsförordningen.

5.2. Förslag till fördjupad granskning

Med anledning av förstudiens resultat är vår uppfattning att det finns en överhängande risk att nödvändiga anpassningar inte hinner genomföras i tid, innan förordningens ikraftträdande 25 maj 2018. Exempelvis behöver följande områden hanteras snarast:

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

Vi föreslår att en eventuell fördjupad granskning fokuseras på huruvida verksamheten lyckats genomföra anpassningarna i tid. Granskningen bör i så fall genomföras under hösten 2018 (augusti/september). För förslag på syfte, revisionsfrågor, metod, genomförande och avgränsningar se bilaga 2, *Förslag till utformning av projektplan.*

Umeå den 30 januari 2017

Linda Marklund
Certifierad kommunal revisor
EY

Petra Nylander
Verksamhetsrevisor
EY

Building a better working world

Bilaga 1: **Källförteckning**

Intervjuade funktioner:

- Ledningsstabsdirektör
- Informationssäkerhetsstrateg
- Jurist, personuppgiftsombud
- Enterprisearkitekt
- Verksamhetschef för basenhet Informatik
- Landstingsdirektör

Dokument:

- Landstingsstyrelsens reglemente
- Hälso- och sjukvårdsnämndens reglemente
- Landstingsstyrelsens delegationsordning
- Hälso- och sjukvårdsnämndens delegationsordning
- Landstingsdirektörens vidaredelegationsordning
- Hälso- och sjukvårdsdirektörens vidaredelegationsordning
- GDPR-strategi (utkast)
- GDPR aktivitetsplan (utkast)
- GDPR Checklista för lagkrav avseende personuppgiftsbehandling (utkast)
- GDPR Checklista anpassningar informationssäkerhet (utkast)
- Rutin för personuppgiftsincidenter (utkast)
- ATEA: Slutrapport Informationssäkerhet (2017-02)
- Ledning- och styrmodell för informationssäkerhet (ej fastställd)
- Mall Säkerhetsanalys av informationstillgångar (ej fastställd)
- Protokoll från landstingsstyrelsen (2017)
- Sammanträdesanteckningar för ELG (augusti-december 2017)
- Återrapport om informationssäkerhetsarbete

Building a better working world

Bilaga 2: **Förslag till utformning av projektplan**

Bakgrund
EY har på uppdrag av de förtroendevalda revisorerna i Västerbottens läns landsting granskat landstingsstyrelsen och hälso- och sjukvårdsnämnden i syfte att ge revisorerna underlag för att kunna besluta om en fördjupad granskning med anledning av den nya dataskyddsförordningen.

I förstudien gjordes följande iakttagelser:

- Vi kan inte styrka att någon organisation, med tydlig roll-, ansvars- och befogenhetsfördelning avseende införandet av GDPR, har beslutats på formellt sätt.
- Inga dokumenterade och landstingsövergripande riskanalyser har upprättats med anledning av den nya förordningen.
- Vi kan inte styrka att det inom landstinget pågår ett samordnat och heltäckande arbete med anpassningar inför GDPR. Vissa anpassningar har påbörjats under hösten men vår uppfattning är att det fortfarande återstår mycket arbete att genomföra innan landstingets verksamheter kan uppfylla samtliga krav som ställs i den nya dataskyddsförordningen.
- En aktivitetsplan har tagits fram. Denna plan är, enligt vår uppfattning, inte heltäckande för en fullständig implementering av GDPR inom landstingets verksamheter.
- Förslag till styrande dokument har tagits fram. Vid granskningstillfället är dessa dock fortfarande utkast och det finns ingen tidsplan för spridning och implementering av styrdokumenten.

Med anledning av förstudiens resultat är vår uppfattning att det finns en överhängande risk att nödvändiga anpassningar inte hinner genomföras i tid.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden efterlever de krav som ställs i dataskyddsförordningen.

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

Styrning
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt;

- att det finns en ändamålsenlig organisation som möjliggör för att efterleva förordningens krav? Har tex dataskyddsombud utsetts? Är dennes roll och uppgifter är tydliga?
- att områdesspecifika styrande dokument är antagna, och av behörig instans?
- att det finns laganpassade och ändamålsenliga rutinbeskrivningar för hur personuppgifter hanteras i verksamheterna?
- att tillräckliga resurser har budgeterats för att kunna genomföra förändringar i enlighet med lagkrav?

Praktiskt arbete i verksamheterna
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt;

- att en heltäckande inventering av personuppgifter genomförts i organisationen?
- att det finns rutiner och system för hur den enskildes stärkta rättigheter kan tillgodoses?

- exempelvis rutiner för att; kartlägga laglig grund, hämta in samtycke, genomföra konsekvensbedömning, tillgodose dataportabilitet, hur uppgifter lämnas ut
- att IT-system uppdaterats och anpassats efter förordningens krav?
- att anställda får nödvändig information sina skyldigheter enligt förordningens krav

Uppföljning och kontroll
Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt

- att det finns en plan för systematisk genomgång och uppdatering av personuppgifter som finns i organisationen?
- att det finns tillförlitliga rutiner för att upptäcka, utreda och rapportera personuppgiftsincidenter?
- att styrelsen och nämnden får tillräcklig rapportering om arbetet med att uppfylla kraven i dataskyddsförordningen?

Revisionskriterier

- Kommunallagen
- Dataskyddsförordningen
- Interna styrande dokument

Metod, genomförande och avgränsningar

Granskningen genomförs genom insamling och analys av dokumentation inom området samt intervjuer med landstingsdirektören, digitaliserings- och teknikdirektören, informationssäkerhetsstrateg, jurist, dataskyddsombud, stabschefer och verksamhetschefer.

Granskningen omfattar landstingsstyrelsen (fokus på basenhet Informatik samt ett urval hälsocentraler) och hälso- och sjukvårdsnämnden (fokus på basenhet barn- och ungdomscentrum).

Tidplan

Granskningen inleds under augusti/september 2018 och avrapporteras i november/december 2018.