Fördjupad granskning nr 2/2022

Efterlevnad av dataskyddsförordningen (GDPR)

September 2022
Max Wann Adebahr, EY
Diarienummer: REV 46-2021

region västerbotten

Revisionsrapport 2022
Genomförd på uppdrag av revisorerna
Juni 2022

Region Västerbotten

Granskning efterlevnad av dataskyddsförordningen (GDPR)

Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Region Västerbotten granskat regionstyrelsen och hälso- och sjukvårdsnämnden, hädanefter benämnt "de granskade nämnderna", i syfte att bedöma och kartlägga arbetet med personuppgiftshantering enligt dataskyddsförordningen (GDPR). Granskningens syfte har varit att bedöma om de granskade nämnderna har säkerställt att GDPR efterlevs på ett ändamålsenligt sätt samt om den interna kontrollen är tillräcklig inom området.

Baserat på den analys och granskning som genomförts bedöms mognadsgraden för regionstyrelsen samt hälso- och sjukvårdsnämnden vara förhållandevis låg på 1,80 av maximalt 5,00. Mognadsgrad 1 innebär begynnande, 3 bedöms vara god praxis (i relation till motsvarande organisationer), och 5 optimerad. Mognadsgraden bedöms vara något högre inom områdena riskhantering, incidenthantering och hantering av leverantörsrelationer. Lägst är mognadsgraden inom information till registrerade, inbyggt dataskydd och intern kontroll.

Den sammanfattade bedömningen är att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt att GDPR efterlevs på ett ändamålsenligt sätt samt att den interna kontrollen inom området ej är tillräcklig. Vidare bedömer vi att tillräckliga åtgärder ej har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018). Detta då det inte har verkställts en välfungerande dataskyddsorganisation, samt att nödvändiga styrande dokument inte har upprättats till en tillräcklig grad. För mer detaljerad information avseende bedömning av mognadsgrad, se bilaga 1.

De främsta förbättringspunkterna ligger i att:

- Definiera och implementera en tydlig och specifik organisation kopplat till arbetet med dataskydd inom de granskade nämnderna. Organisationen bör utgå från dokumenterade rollbeskrivningar, en tydlig ansvarsfördelning samt ett övergripande styrdokument för GDPR.
- Säkerställa att anställda besitter adekvat kunskap inom dataskyddsarbetet genom att fastställa en utbildningsplan med regelbundna och obligatoriska utbildningsinsatser.
- Formalisera arbetet med granskning och uppföljning genom att definiera och implementera en granskningsplan. Detta för att säkerställa efterlevnad av policyer, rutiner och riktlinjer kring personuppgiftshantering.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Innehåll

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

1 Inledning

1.1 Bakgrund

Regionstyrelsen och hälso- och sjukvårdsnämnden i Region Västerbotten, härefter benämnt "de granskade nämnderna", hanterar stora mängder personuppgifter i många olika delar av verksamheten. Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018 och ställer stora och ökade krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter. Avvikelser kan leda till sanktioner i form av bl.a. viten.

Ett av syftena med GDPR är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Rätten till privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). Förordningen baserat på Europaparlamentets och rådets förordning (EU) 2016/679 som gäller i hela EU.

Revisorerna har i tidigare granskningar (2018) identifierat brister i de granskade nämnderna arbete med GDPR. Bl.a. noterades att det inte fanns en fungerande dataskyddsorganisation eller tillräckliga styrdokument för arbetet. Vidare hade inte heller riskanalyser och inventering av personuppgifter genomförts på ett tillräckligt sätt. Regionstyrelsens och hälso- och sjukvårdsnämndens kontroll inom området bedömdes vara låg.

Mot bakgrund av ovanstående har revisorerna beslutat att genomföra en granskning av hur GDPR efterlevs.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden har säkerställt att GDPR efterlevs på ett ändamålsenligt sätt samt om den interna kontrollen är tillräcklig inom området. Granskningen ska svara på följande revisionsfrågor:

Styrning
Har styrelsen/nämnden säkerställt att:

- Det finns en välfungerande organisation för arbetet med GDPR? Med välfungerande avses bl.a. att nödvändiga roller och ansvar (inklusive DSO-rollen) är tydliga.
- Det finns ändamålsenliga styrdokument (tex policyer, riktlinjer, planer) och fungerande processer för att uppnå regelefterlevnad med avseende på GDPR? Tex;
    - Finns registerförteckning som uppfyller förordningens krav?
    - Finns en fungerande process för registervård?
    - Finns processer för hantering av dataöverträdelser inklusive handlingsplan, rutiner, rapportering och uppföljning av överträdelser?
    - Finns en dokumenthanteringsplan inklusive rutiner för bedömning av personuppgifter, identifiering av redundant data och radering av data?
    - Är det definierat när en konsekvensbedömning ska utföras och är dess process definierad?

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

    - Finns rutiner för personuppgiftsbiträdesavtal (PUB) inklusive register över avtal och vilken data som personuppgiftsbiträden hanterar/har åtkomst till?
- Tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018)?

I granskningen ingår även en kartläggning av i vilken grad de granskade nämnderna använder sig av molntjänster samt en kontroll av om styrelse och nämnd har säkerställt att hanteringen av dessa molntjänster är förenliga med GDPR.

Uppföljning och kontroll
Har styrelsen/nämnden säkerställt att:
- Det finns fungerande kontroller och rutiner för personuppgiftsbiträdesavtal (PUB) inklusive register över avtal, vilken data som personuppgiftsbiträden hanterar/har åtkomst till?
- Det sker en tillräcklig uppföljning och kontroll av arbetet med dataskyddsförordningen (GDPR)?

1.3 Avgränsningar

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policyer. Granskningen utgår från arbetet som regionstyrelsen bedriver samt arbetet som bedrivs inom hälso- och sjukvårdsnämnden. Ingen teknisk analys har genomförts, exempelvis penetrationtest/sårbarhetsanalys.

1.4 Metod

Granskningen har byggt på EY:s ramverk för granskning av personuppgiftshantering, särskilt framtagen för svensk offentlig sektor. Ramverket omfattar 12 områden, exempelvis personuppgiftsbehandling, incidenthantering och registrerades rättigheter, vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i personuppgiftshanteringen. Information kring de 12 områdena har insamlats både genom granskning av relevanta dokument, samt genom att EY:s specialister har genomfört intervjuer med relevanta personalkategorier i regionen. Vidare har de 12 områdena delats in i 2 huvudområden inom vilka iakttagelser och bedömningar har noterats.

Inledningsvis granskades relevant dokumentation kring rutiner och processer av EY. Därefter hölls intervjuer med de granskade nämndernas representanter kring arbetet med GDPR för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av dataskyddsförordningen i regioner. Slutligen analyserades och bedömdes den samlade bilden av dokumentation samt information inhämtad via intervjuer.

Under granskningen intervjuades följande funktioner:
- Dataskyddombud och informationssäkerhetsombud
- Verksamhetschef IT
- Dataskyddsombud
- Arkivarie
- Specialist Digitalisering

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

- Systemutvecklare

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta. Fullständig förteckning över intervjuade funktioner framgår av bilaga 2. Dokumentförteckning framgår av bilaga 3.

De 12 områdena som granskats inom uppdraget är:

1. Styrande dokument/styrning
2. Riskhantering
3. Kontroll
4. Organisation och ansvar
5. Behandling av personuppgifter
6. Val av skyddsåtgärder
7. Inbyggt dataskydd
8. Hantering av leverantörsrelationer
9. Hantering av incidenter
10. Information till registrerade
11. Begäran från registrerade
12. Profilering

1.5 Revisionskriterier

- Dataskyddsförordningen GDPR
- Regionsinterna policyer och riktlinjer på området
- Kommunallagen (kapitel 6)

1.6 Definitioner

Se Bilaga 4

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

2 Granskningsresultat

I detta kapitel presenteras de övergripande resultaten från genomförd granskning med utgångspunkt från revisionsfrågorna. Mognadsbedömningar och detaljerade granskningsresultat återfinns i bilaga 1.

2.1 Organisation

I detta delkapitel besvaras följande revisionsfråga:

- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att det finns en välfungerande organisation för arbetet med GDPR? Med välfungerande avses bl.a. att nödvändiga roller och ansvar (inklusive DSO-rollen) är tydliga.

2.1.1 Iakttagelser

De granskade nämnderna ansvarar för att kraven avseende GDPR uppfylls inom respektive nämnd och för att resurser och kompetens är tillräcklig för att uppfylla kraven i dataskyddsförordningen. Enligt dokumenterade rollbeskrivningar utser granskade nämnderna dataskyddsombud för sin verksamhet medan verksamhetschefen för respektive verksamhet utser personuppgiftshandläggare. Rollbeskrivningar för Dataskyddsombud och Personuppgiftshandläggare finns dokumenterade och uppdaterades i januari 2021. Det saknas däremot en övergripande dataskyddsorganisation med ytterligare definierade roller och ansvarsbeskrivningar kopplade till dataskyddsarbetet, samt en tydlig beskrivning av hur dataskyddsarbetet koordineras. Enligt uppgift bedrivs det i dagsläget ett arbete för att ta fram en dataskyddsorganisation där rollbeskrivningar och ansvarsområden kopplade till dataskydd och personuppgiftshantering ska vara tydligt definierade.

De granskade nämnderna ställer krav vid rekryteringstillfället att dataskyddsombudet besitter relevant och tillräcklig kunskap för att leva upp till kraven i dataskyddsförordningen. Däremot finns det ingen rutin för att kontinuerligt säkerställa att dataskyddsombudets kunskap förblir riktig och aktuell över tid. Det har inte heller säkerställts att dataskyddsombudet får allt stöd som krävs för att kunna utföra sina uppgifter enligt dataskyddsförordningen. Vid tid för granskning, vinter/vår 2022, är dataskyddsombudet och informationssäkerhetssamordnaren för de granskade nämnderna samma person. Det har inte genomförts en dokumenterad analys för att säkerställa att det inte finns några intressekonflikter mellan dataskyddsombud och övriga arbetsuppgifter.

2.1.2 Bedömning

Vår bedömning är att de granskade nämnderna inte har säkerställt att det finns en välfungerande organisation för arbetet med GDPR. Detta då det vid tid för granskning saknas en upprättad dataskyddsorganisation med tydligt definierad koordinering och roll- och ansvarsfördelning avseende arbetet med GDPR. Därtill anser vi att de granskade nämnderna inte har säkerställt att dataskyddsombudet ges det stöd som krävs och besitter en tillräcklig kompetens för att leva upp till kraven i dataskyddsförordningen. Vidare anser vi att de granskade nämnderna inte har säkerställt att dataskyddsombudet tillåts arbeta utan intressekonflikter då dataskyddsombudet och informationssäkerhetssamordnaren vid tid för granskning är samma person.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

2.2 Styrning

I detta delkapitel besvaras följande revisionsfrågor:

- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att det finns ändamålsenliga styrdokument (tex policyer, riktlinjer, planer) och fungerande processer för att uppnå regelefterlevnad med avseende på GDPR?
- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att hanteringen av personuppgifter i molntjänster är förenliga med GDPR?

2.2.1 Iakttagelser

De granskade nämndernas dataskyddsarbete grundar sig främst i Informationssäkerhetspolicyn som är fastställd av landstingsfullmäktige under 2018 och uppföljd under 2020. Till informationssäkerhetspolicyn finns övergripande styrdokument beslutade av regionstyrelsen. I vissa fall förekommer också lokala riktlinjer för nämnder/verksamheter inom regionen. I dagsläget saknas ett styrdokument som på övergripande nivå beskriver hur de granskade nämndernas dataskyddsarbete ska organiseras, styras samt genomföras för att uppfylla kraven i dataskyddsförordningen. Det finns en dokumenterad riktlinje avseende hur ofta styrdokument ska granskas eller revideras, men flertalet styrande dokument har inte uppdaterats i enlighet med riktlinjen.

De gemensamma styrdokumenten avseende GDPR inkluderar bland annat samtyckeshantering, incidenthantering, arkivering av allmänna handlingar och informationslagring i molntjänsten Microsoft Office 365. I styrdokument för Microsoft Office 365 är det beskrivet att känsliga personuppgifter eller information som omfattas av offentlighets- och sekretesslagen inte får hanteras i Microsoft Office 365.

I dagsläget finns det ingen dokumenterad process avseende vilken information som ska lämnas till registrerade vid insamling av personuppgifter. Det finns inte heller en dokumenterad rutin för hantering av registrerade som begär ut personuppgifter. Det saknas även ett dokumenterat dataflöde av personuppgifter mellan de granskade nämndernas IT-system. Vidare har en rutin för att säkerställa att ostrukturerad information blir klassificerad inte implementerats.

Vid tid för granskning finns ingen dokumenterad process för utbildning avseende personuppgiftsbehandling. I samband med införandet av dataskyddsförordningen 2018 genomfördes GDPR-utbildningar, men dessa har inte följts upp sedan 2018. Utbildningar sker i dagsläget på efterfrågan. Viss utbildning gällande dataskydd finns på regionens intranät som är tillgängligt för samtliga anställda. Det pågår i nuläget ett arbete med att ta fram en utbildningsplan inom GDPR för att kontinuerligt säkerställa anställdas kunskap inom området.

De granskade nämnderna har i enlighet med kraven i dataskyddsförordningen ett dokumenterat register över alla personuppgiftsbehandlingar. Det har dock inte säkerställts att registerförteckningen är, samt förblir, komplett och riktig över tid. Vidare har de granskade nämnderna inte kontrollerat och säkerställt att personuppgifter endast används till de ändamål de var insamlade för.

2.2.2 Bedömning

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Det är vår bedömning att de granskade nämnderna delvis har säkerställt att det finns ändamålsenliga styrdokument och fungerande processer avseende GDPR. Bedömningen grundar sig i att det finns flertalet ändamålsenliga styrdokument kopplat till GDPR. Dock saknas exempelvis ett styrdokument som på övergripande nivå beskriver hur dataskyddsarbetet ska organiseras, styras samt genomföras. Därtill anser vi att de granskade nämnderna saknar vissa centrala styrdokument och processer kopplat till dataskyddsarbetet. Bland annat saknas rutiner och riktlinjer för hur anställda ska hantera registrerade som begär ut personuppgifter och hur anställda ska informera registrerade vid insamling av personuppgifter. Det är därtill vår bedömning att de granskade nämndernas styrdokument inte är uppdaterade med tillräckligt hög frekvens för att säkerställa att dokumenten förhåller sig till aktuella lagar och krav. De granskade nämnderna anses inte heller ha tillsett att utbildning av samtliga anställda sker systematiskt och i nödvändig utsträckning. För att kunna säkerställa nödvändig kunskap enligt krav i dataskyddsförordningen ser vi ett behov av en strukturerad utbildningsplan med regelbundna insatser.

Det är vår bedömning att de granskade nämndernas riktlinjer avseende hantering av molntjänster är ändamålsenliga. Styrelsen och nämnden har dock inte säkerställt genom kontroll eller uppföljning att riktlinjerna efterlevs i praktiken.

2.3 Åtgärder

I detta delkapitel besvaras följande revisionsfråga:

- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018)?

2.3.1 Iakttagelser

Tidigare granskning år 2018 visade att styrelsen och nämnden inte hade en ändamålsenlig dataskyddsorganisation samt att styrdokument avseende personuppgiftshantering saknades. Revisorerna rekommenderade då att regionstyrelsen och hälso- och sjukvårdsnämnden bör verkställa en välfungerande dataskyddsorganisation, samt upprätta nödvändiga styrdokument. Se avsnitt 2.1 och 2.2 för iakttagelser och nulägesbedömning avseende organisation och styrning.

2.3.2 Bedömning

Med grund i de granskade nämndernas nuvarande arbete avseende organisation och styrning anser vi att det inte har vidtagits tillräckliga åtgärder med anledning av revisionens tidigare granskningar inom GDPR (3/2018). Det saknas ännu en definierad och välfungerande dataskyddsorganisation samt vissa styrande dokument avseende arbetet med GPDR.

2.4 Tredjepartshantering/leverantörsrelationer

I detta delkapitel besvaras följande revisionsfråga:

- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att det finns fungerande kontroller och rutiner för personuppgiftsbiträdesavtal (PUB) inklusive

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

register över avtal, vilken data som personuppgiftsbiträden hanterar/har åtkomst till?

2.4.1 Iakttagelser

Enligt dokumenterade riktlinjer ska personuppgiftsbiträdesavtal som bygger på SKR:s avtalsmall tecknas med samtliga leverantörer, och kraven på biträden följer därefter. De granskade nämnderna har däremot inte någon dokumenterad rutin på plats för att bedöma hur leverantörer förhåller sig till krav och förväntningar. Granskningen visar att det inte finns ett register över leverantörer med PUB-avtal, vilket betyder att det inte går att säkerställa att avtal är tecknade för samtliga leverantörer. Intervjuade uppger att det pågår ett arbete kring utveckling och förbättring av leverantörsbedömning.

Dataöverföring av personuppgifter utanför Europeiska ekonomiska samarbetsområdet (EES) och Europeiska Unionen (EU) förekommer inom de granskade nämnderna, och det finns en dokumenterad vägledning för tredjelandsöverföring. Däremot finns ingen rutin för att säkerställa att vägledningen efterlevs.

2.4.2 Bedömning

Det är vår bedömning att de granskade nämnderna devis har säkerställt att det finns fungerande kontroller och rutiner för personuppgiftsbiträdesavtal. Detta då personuppgiftsbiträdesavtal, enligt SKR:s avtalsmall, ska tecknas med samtliga personuppgiftsbiträden. Vi bedömer dock att det inte har säkerställts att personuppgiftsavtal har tecknats för samtliga leverantörer i enlighet med dokumenterad riktlinje. Vi bedömer även att det inte säkerställts att pub-avtal med leverantörer uppdateras vid behov, exempelvis vid förändringar i regelverk, samt att leverantörer och tredjeparter följer dataskyddsförordningen över tid. Därtill är det vår bedömning att de granskade nämnderna inte har säkerställt att dataöverföring utanför Europeiska ekonomiska samarbetsområdet (EES) och Europeiska Unionen (EU) sker enligt dokumenterad rutin.

2.5 Uppföljning och kontroll

I detta delkapitel besvaras följande revisionsfråga:

- Har regionstyrelsen/hälso- och sjukvårdsnämnden säkerställt att det sker en tillräcklig uppföljning och kontroll av arbetet med dataskyddsförordningen (GDPR)?

2.5.1 Iakttagelser

De granskade nämnderna har i dagsläget ingen rutin för att kontrollera och säkerställa efterlevnad av riktlinjer och policyer. Efterlevnadsrapportering har förekommit sporadiskt, men det finns ingen dokumenterad process eller rutin för hur efterlevnad av riktlinjer och regelverk ska granskas och rapporteras. Vidare finns det i nuläget ingen naturlig rapporteringsväg för dataskyddsarbetet från verksamheterna till regionstyrelsen, och det saknas dokumenterade krav på rapportering mellan dataskyddsombud och regionstyrelse.

Det finns vid tid för granskning inte någon fastslagen granskningsplan eller internkontrollfunktion med fokus på att säkerställa att dataskyddsarbetet är i enlighet med

dataskyddsförordningens krav. Det bedrivs inte heller något strukturerat arbete med inbyggt dataskydd för att ta hänsyn till integritetsskyddsreglerna i utvecklingsfasen av internutvecklade IT-system. Det genomförs riskanalys, och vid behov konsekvensbedömning, av system i samband med ändringsbegäran. En sådan riskanalys görs på en övergripande nivå och GDPR är en del av denna. En dokumenterad riskanalys har däremot inte genomförts för samtliga system. Vid tid för granskning kan det således inte säkerställas att riskanalyser och konsekvensbedömningar har genomförts enligt dokumenterad rutin för alla relevanta system som hanterar personuppgifter.

De granskade nämnderna har definierad ett antal olika behörighets- och loggkontroller för att förbättra dataskyddet inom verksamheternas IT-system. Exempelvis finns det riktlinjer kring loggkontroller som beskriver att en systematisk stickprovskontroll av loggverktyget ska genomföras. De granskade nämnderna har däremot inte följt upp och säkerställt att riktlinjerna för behörighets- och loggkontroller efterlevs i praktiken. Vidare finns det inte heller någon dokumenterad process som säkerställer att integritetsrisker inkluderas i utformningen av behörighetskontroller.

Internkontrollplanen för 2021 från regionstyrelsen inkluderar en kontrollpunkt avseende GDPR som kontrollerar risken att personuppgifter behandlas i strid med dataskyddsförordningen. Bedömningen av kontrollpunkten var att det finns fortsatt behov av att utveckla dataskyddsarbetet. Internkontrollplanen för 2022 från regionstyrelsen inkluderar inga kontrollpunkter avseende GDPR.

Internkontrollplanen för 2021 från hälso- och sjukvårdsnämnden inkluderar en kontroll avseende GDPR som kontrollerar risken att personuppgifter behandlas i strid med dataskyddsförordningen. Kontrollen består av kontrollpunkter kring organisation, samordning och styrning av dataskyddsarbetet. Bedömningen av kontrollen var att kontrollpunkterna delvis uppfylldes. Kontrollen identifierade behov av åtgärder avseende GDPR, såsom att fastställa den framtagna dataskyddsorganisationen och att förbättra samordningen av dataskyddsarbetet.

2.5.2 Bedömning

Det är vår bedömning att de granskade nämnderna inte har säkerställt att det sker en tillräcklig uppföljning och kontroll av arbetet med dataskyddsförordningen. Detta då det saknas rutiner för att regelbundet kontrollera och säkerställa att riktlinjer, processbeskrivningar och kontroller efterlevs i praktiken. Vi bedömer att de granskade nämnderna inte har säkerställt att riktlinjer avseende samtyckeshantering, incidenthantering och informationslagring i Microsoft Office 365 efterlevs i praktiken. Därtill bedömer vi att det inte har säkerställts att personuppgifter gallras enligt aktuella gallringsfrister.

De granskade nämnderna saknar gransknings- och rapporteringskrav, vilket är nödvändigt för att kontrollera att verksamheterna förhåller sig till kraven i dataskyddsförordningen. Kontroll och uppföljning sker i dagsläget sporadiskt och utan grund i dokumenterad plan. Det saknas således en dedikerad granskningsplan för GDPR som säkerställer att efterlevnad, utförande och kunskap om relevanta styrdokument, processbeskrivningar och kontroller regelbundet granskas och kontrollers.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Det är vår bedömning att det inte genomförs tillräcklig löpande kontroll och uppföljning av regionstyrelsens eller hälso- och sjukvårdsnämndens dataskyddsarbete. Detta då att internkontrollplanen för 2022 från regionstyrelsen inte innefattar kontroll av dataskyddsarbetet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

3 Samlad bedömning

Granskningen syfte har varit att bedöma om regionstyrelsen och hälso- och sjukvårdsnämnden har säkerställt att GDPR efterlevs på ett ändamålsenligt sätt samt om interna kontroller är tillräckligt inom området. Den sammanfattade bedömningen är att regionstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt att GDPR efterlevs på ett ändamålsenligt sätt samt att den interna kontrollen inom området ej är tillräcklig. Det är vår bedömning att de granskade nämnderna har något högre mognadsgrad inom:

- Riskhantering
- Incidenthantering
- Hantering av leverantörsrelationer

Lägst bedöms mognadsgraden vara inom:

- Information till registrerade
- Inbyggt dataskydd
- Intern kontroll

Vidare bedömer vi att tillräckliga åtgärder ej har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018). Detta då det inte har verkställts en välfungerande dataskyddsorganisation, samt att nödvändiga styrande dokument inte har upprättats till en tillräcklig grad. För mer detaljerad information avseende bedömning av mognadsgrad, se bilaga 1.

3.1 Svar på revisionsfrågor

Revisionsfrågorna besvaras utifrån granskningen som helhet, det vill säga regionstyrelsen och hälso- och sjukvårdsnämnden, i en sammanvägd bedömning.

3.1.1 Styrning

Tabell 2: Svar på revisionsfrågor avseende styrning.

Revisionsfråga	Svar
Har styrelsen/nämnden säkerställt att det finns en välfungerande organisation för arbetet med GDPR? Med välfungerande avses bl.a. att nödvändiga roller och ansvar (inklusive DSO-rollen) är tydliga.	De granskade nämnderna bedöms *inte* ha säkerställt en välfungerande organisation för arbetet med GDPR. Svaret grundar sig i att det saknas en övergripande dokumenterad roll- och ansvarsfördelning kring arbetet med GDPR. Det saknas även en rutin för att kontinuerligt säkerställa att dataskyddsombudets kunskap förblir riktig och aktuell över tid. Därtill är de granskade nämndernas dataskyddsombud och informationssäkerhetssamordnare samma person, vilket innebär en risk för intressekonflikt och avsaknad av objektivitet.
Har styrelsen/nämnden säkerställt att det finns ändamålsenliga styrdokument (tex policyer, riktlinjer, planer) och	De granskade nämnderna bedöms *delvis* ha säkerställt att det finns ändamålsenliga styrdokument och fungerande processer för

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

fungerande processer för att uppnå regelefterlevnad med avseende på GDPR? Tex; ▸ Finns registerförteckning som uppfyller förordningens krav? ▸ Finns en fungerande process för registervård? ▸ Finns processer för hantering av dataöverträdelser inklusive handlingsplan, rutiner, rapportering och uppföljning av överträdelser? ▸ Finns en dokumenthanteringsplan inklusive rutiner för bedömning av personuppgifter, identifiering av redundant data och radering av data? ▸ Är det definierat när en konsekvensbedömning ska utföras och är dess process definierad? ▸ Finns rutiner för personuppgiftsbiträdesavtal (PUB) inklusive register över avtal och vilken data som personuppgiftsbiträden hanterar/har åtkomst till?	att uppnå regelefterlevnad med avseende på GDPR. Svaret grundar sig i att det finns flertalet ändamålsenliga styrdokument för delar av dataskyddsarbetet bl.a. registerförteckning, dokumenthanteringsplan och enskildas rättigheter enligt GDPR. Det finns även styrdokument för hantering av personuppgiftsincidenter samt riskanalys och konsekvensbedömning av personuppgiftsbehandling. Revisionsfrågan bedöms inte ha uppfyllts fullständigt då det saknas ett styrdokument för GDPR-arbetet som på övergripande nivå beskriver de riktlinjer som arbetas utefter för att förhålla sig till kraven i dataskyddsförordningen, exempelvis en policy för dataskydd. Vidare saknas riktlinje för bland annat utbildning kring dataskydd, hantering av registrerade vid begäran av uppgifter, samt hur information ska lämnas till registrerade vid insamling av data. Det saknas genomgående dokumenterade rutiner och processer för uppföljning och kontroll av samtliga områden, och därmed säkerställs inte efterlevnad av riktlinjerna.
Har styrelsen/nämnden säkerställt att hanteringen av personuppgifter i molntjänster är förenliga med GDPR?	De granskade nämnderna bedöms *delvis* ha säkerställt att hanteringen av personuppgifter i molntjänster är förenliga med GDPR. Svaret grundar sig i att det finns ett upprättat styrdokument kring hantering av personuppgifter i molntjänsten Microsoft Office 365. Revisionsfrågan bedöms inte ha uppfyllts fullständigt då det inte finns någon granskningsplan eller rutin för att kontrollera och säkerställa att riktlinjen kring personuppgiftshantering i Microsoft Office 365 efterlevs.
Har styrelsen/nämnden säkerställt att tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018)?	De granskade nämnderna bedöms *inte* ha säkerställt att tillräckliga åtgärder har vidtagits med anledning av revisionens tidigare granskningar och väsentliga iakttagelser inom GDPR (3/2018).

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	Svaret grundar sig i att det inte har verkställts en välfungerande dataskyddsorganisation som ger verksamheterna tillräckligt stöd i anpassningsarbetet och ser till att dataskyddsarbetet samordnas och följs upp. Svaret grundar sig också i att nödvändiga styrande dokument inte har upprättats till en tillräcklig grad, då det saknas styrande dokument som på övergripande nivå beskriver dataskyddsarbetet, samt att det saknas rutiner för säkerställande av efterlevnad.

3.1.2 Uppföljning och kontroll

Tabell 3: Svar på revisionsfrågor avseende uppföljning och kontroll.

Revisionsfråga	Svar
Har styrelsen/nämnden säkerställt att det finns fungerande kontroller och rutiner för personuppgiftsbiträdesavtal (PUB) inklusive register över avtal, vilken data som personuppgiftsbiträden hanterar/har åtkomst till?	De granskade nämnderna bedöms *delvis* ha säkerställt att det finns fungerande kontroller och rutiner för personuppgiftsbiträdesavtal. Svaret grundar sig i att regionen har dokumenterade riktlinjer som beskriver att personuppgiftsbiträdesavtal ska tecknas för samtliga personuppgiftsbiträden, med grund i SKR:s avtalsmall. Ur SKR:s avtalsmall följer krav på biträden att efterleva relevant lagstiftning gällande GDPR. Revisionsfrågan bedöms inte ha uppfyllts fullständigt då det saknas kontroll eller en rutin för att säkerställa att personuppgiftsbiträden lever upp till krav ställda i personuppgiftsbiträdesavtal. Därtill har de granskade nämnderna inte fört register över personuppgiftsbiträdesavtal med leverantörer, varvid det inte har säkerställts att personuppgiftsbiträdesavtal enligt SKR:s mall har tecknats för samtliga personuppgiftsbiträden.
Har styrelsen/nämnden säkerställt att det sker en tillräcklig uppföljning och kontroll av arbetet med dataskyddsförordningen (GDPR)?	De granskade nämnderna bedöms *inte* ha säkerställt en tillräcklig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR).

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	Svaret grundar sig i att internkontrollplanen för 2022 från regionstyrelsen inte innefattar kontroll av dataskyddsarbetet. Därtill saknas en dedikerad granskningsplan för dataskyddsarbetet. De granskade nämnderna har inte heller upprättat dokumenterade rutiner för uppföljning på verksamhetsnivå och således sker ingen strukturerad rapportering kring uppföljning och efterlevnad av riktlinjer kring dataskyddsarbetet.

3.2 Övergripande rekommendationer

Då flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera de mest relevanta övergripande rekommendationer och förslag på åtgärder för de främsta riskerna avseende personuppgiftshantering. För mer information om respektive rekommendation, se bilaga 1.

Regionstyrelsen och hälso- och sjukvårdsnämnden rekommenderas att:

Inledningsvis:

- Säkerställa att en välfungerande dataskyddsorganisation, med tydlig roll- och ansvarsfördelning kring dataskyddsarbete, är implementerad.
- Säkerställa att relevanta styrdokument och rutinbeskrivningar finns på plats, samt att de förblir riktiga och uppdaterade över tid genom att implementera en process för att regelbundet granska och uppdatera styrdokument.
- Säkerställa att medarbetare som behandlar personuppgifter får relevant utbildning utifrån roll och ansvar samt att utbildning genomförs, och följs upp, utefter en dokumenterad utbildningsplan.
- Utarbeta och dokumentera riktlinjer för uppföljning av registerförteckningens riktighet och fullständighet över tid.

Därefter:

- Implementera en granskningsplan för att utvärdera och säkerställa att relevanta krav på hantering av personlig information uppfylls av chefer, medarbetare och leverantörer.
- Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med regionens krav och dataskyddsförordningen över tid.

Regionstyrelsen rekommenderas att:

Inledningsvis:

- Upprätta ett övergripande styrdokument för GDPR som på en hög nivå beskriver regionens riktlinjer kopplat till arbetet med personuppgiftshantering.
- Definiera rapporteringskrav och rapporteringsvägar för dataskyddsarbetet inom regionens nämnder och förvaltningar.

Därefter:

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

- Implementera en formell rutin för att dokumentera och rapportera granskningsresultat till ledningsnivå.

Hälso- och sjukvårdsnämnden rekommenderas att:

Inledningsvis:

- Tillse att policyer, rutiner och riktlinjer kommuniceras aktivt till nämndens medarbetare med en bestämd frekvens.
- Säkerställa att centralt framtagna styrdokument kontinuerligt anpassas utefter den egna verksamheten.

Därefter:

- Säkerställa att obligatorisk utbildning genomförs för samtliga anställda inom verksamheten samt införa uppföljning av deltagande och effekt.
- Definiera och dokumentera riktlinjer som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

4 Bilaga 1: Detaljerade granskningsresultat

Baserat på den analys och granskning som genomförts bedöms regionstyrelsen och hälso- och sjukvårdsnämnden i Region Västerbotten, hädanefter benämnt "regionen", ha en genomsnittlig mognadsgrad på 1,80 av maximalt 5,00 inom de 12 granskningsområdena. Detta är en lägre mognadsgrad än vad EY rekommenderar för en region som Västerbotten, givet den mängd personuppgifter, och andel av känslig karaktär, som hanteras.

Regionen saknar övergripande styrdokument kring GDPR som på en hög nivå beskriver samtliga regionens riktlinjer kopplat till arbetet med personuppgiftshantering. I nuläget bedöms strategier såsom processer och instruktioner för personuppgiftshantering vara bristfälliga jämfört med kraven i dataskyddsförordningen. Regionen saknar i nuläget även en tydlig dataskyddsorganisation och ansvarsfördelning gällande personuppgiftshantering. Det finns ett behov av en behovsanpassad organisation med tillräckliga resurser för att lösa de uppgifter som krävs för att öka mognadsgraden och därmed adekvat hantera dagens risker. Regionens största förbättringsområden ligger i att definiera policyer, rutiner och riktlinjer i övergripande styrdokument samt att fastställa en tydlig organisation kring arbetet med GDPR.

Översiktsbilden nedan (*Figur 1. Mognadsgrad per område*) redovisar regionens mognadsgrad för de 12 områden som granskats.

Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad. Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

Tabell 4: Skala för bedömning av regionens mognadsgrad inom dataskyddsområden

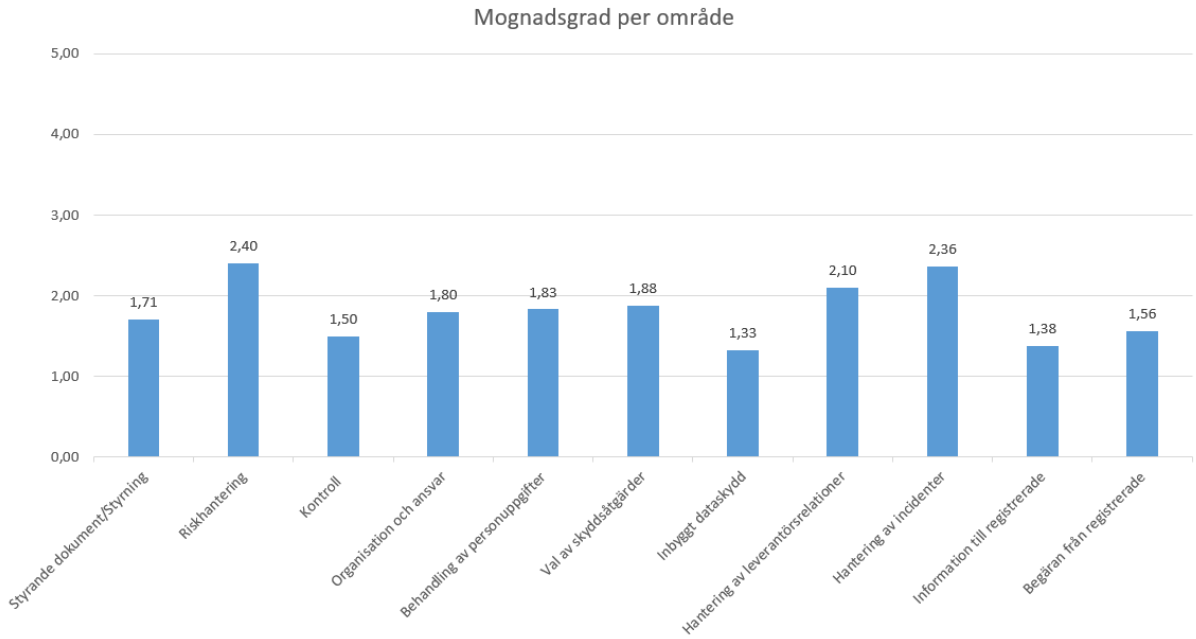
1	Saknas helt / fungerar mycket bristfälligt utan rutiner
2	Existerar men har inte formellt definierats / fungerar bristfälligt utifrån begränsade rutiner
3	Har definierats med delvis efterlevnad / fungerar godtagbart utifrån definierade rutiner
4	Har definierats och förvaltas med god efterlevnad / fungerar väl utifrån definierade rutiner
5	Har definierats och förvaltas med mycket god efterlevnad / fungerar optimalt utifrån mycket väl definierade rutiner

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan t.ex. ett område med grön färgkod ändå sakna viktiga kontroller. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Figur 1: Mognadsgrad per område.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873



Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Tabell 5: Detaljerad nulägesanalys och iakttagelser.

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/Styrning	Region Västerbottens styrande dokument är samlade i regionens ledningssystem. Styrdokumenten gäller för samtliga verksamheter men det förekommer också lokala riktlinjer. En policy som på övergripande nivå beskriver regionens arbete med GDPR finns inte i dagsläget. Regionen har en dokumenterad riktlinje avseende styrande dokument som beskriver att uppföljning ska ske enligt tidsperioden vartannat år om inget annat angivits. Det framgår även ur riktlinjen att styrande dokument ska granskas och godkännas av bäst lämpade avseende innehåll och format innan de upprättas eller uppdateras i ledningssystemet. EY har vid tid för granskning noterat att flertalet styrdokument inte har uppdaterats under de senaste två åren, och kan därmed inte säkerställa att riktlinjen för styrande dokument har efterlevts i praktiken. Det framkom i intervjuer med sakkunniga att regionen i dagsläget inte har en rutin för att kontrollera och säkerställa efterlevnad av riktlinjer och policyer. Efterlevnadsrapportering har förekommit sporadiskt, men det finns ingen dokumenterad process eller rutin för att säkerställa efterlevnad av riktlinjer och regelverk. Det framgick vidare att det inte finns en rutin för genomförande av gap-analyser för GDPR, men det har genomförts visst arbete i regionen för att undersöka hur arbetet kring GDPR kan utvecklas.	Det saknas ett övergripande styrdokument som definierar hur arbetet med dataskyddsförordningen ska organiseras, styras samt genomföras. Styrande dokument har inte uppdaterats i enlighet med regionens riktlinje. Regionen saknar en rutin för att säkerställa efterlevnad av rutiner och regelverk.	1,71

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Riskhantering	Regionen har dokumenterade riktlinjer kring konsekvensbedömning avseende dataskydd. Vid ny eller förändring av personuppgiftsbehandling ska en tröskelanalys genomföras för att bedöma risk och avgöra ifall en konsekvensbedömning bör genomföras. Tröskelanalysen utgår från Integritetsskydds-myndighetens förteckning som fastställts i enlighet med artikel 35.4 i dataskyddsförordningen. Enligt styrdokumentet för konsekvensbedömning avseende dataskydd framgår det att dataskyddssamordnare ska ha rådfrågats eller medverkat vid genomförande av konsekvensbedömning. Styrdokumentet för konsekvensbedömning avseende dataskydd uppdaterades senast i januari 2022. Regionen har ingen rutin på plats för att säkerställa efterlevnad av riskanalys och konsekvensbedömning i praktiken. Enligt intervjuade nyckelpersoner har flera av regionens system använts sedan innan GDPR-kraven infördes i maj 2018. Regionen genomför i nuläget riskanalys och vid behov konsekvensbedömning av system i samband med ändringsbegäran. En sådan riskanalys görs på en övergripande nivå och GDPR är en del av denna. En dokumenterad riskanalys har däremot inte genomförts för samtliga system. Vid tid för granskning kan EY därmed inte säkerställa att riskanalyser och konsekvensbedömningar har genomförts för alla relevanta system som hanterar personuppgifter.	Regionen har inte säkerställt att riskanalyser och konsekvensbedömningar har genomförts enligt dokumenterad rutin. Det har ej säkerställts att riskanalys och konsekvensbedömning genomförts för alla relevanta system som hanterar personuppgifter.	2,40
Kontroll	Enligt intervjuade nyckelpersoner för regionens personuppgiftshantering ska dataskyddsarbetet i verksamheterna rapporteras till regionstyrelsen årligen. Däremot har årliga dataskyddsrapporter inte presenterats. Regionen har i nuläget ingen naturlig rapporteringsväg för dataskyddsarbetet från verksamheterna till regionstyrelsen. Regionens dataskyddsombud är utsedd kontaktperson för förfrågningar från Integritetsskyddsmyndigheten (IMY) och förväntas därmed hantera och bistå IMY med den information som begärs. Regionen har i nuläget ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att regionens dataskyddsarbete är i enlighet med dataskyddsförordningens krav. Enligt intervjuande nyckelpersoner kring regionens dataskyddsarbete genomfördes en intern kontroll under 2021, men kontrollen hanterade inte specifikt personuppgifter.	Det saknas dokumenterade krav på rapportering mellan dataskyddsombud och regionstyrelse. Det saknas en granskningsplan för att säkerställa att regionen uppfyller krav kring personuppgiftshantering enligt dataskyddsförordningen.	1,50
Organisation och ansvar	Regionen har tydligt definierade roller för Dataskyddsombud och Personuppgiftshandläggare, varvid rollbeskrivningarna uppdaterades i januari 2021. Övriga roller kopplade till dataskyddsarbetet saknar däremot roll- och ansvarsbeskrivning. Enligt intervjuade personer specifikt kopplade till dataskyddsarbetet pågår det ett arbete från regionens sida att ta fram en dataskyddsorganisation där	Övergripande beskrivning av roller och ansvarsområden kopplade till dataskydd och personuppgiftshantering har inte definierats.	1,80

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	rollbeskrivningar och ansvarsområden kopplade till dataskydd och personuppgiftshantering ska vara tydligt definierade. Dataskyddsorganisationen är ännu inte fastställd och har därmed inte blivit implementerad. Enligt intervjuade nyckelpersoner inom regionens dataskyddsarbete ställer regionen krav vid rekryteringstillfället att dataskyddsombudet besitter relevant och tillräcklig kunskap för att leva upp till kraven i dataskyddsförordningen. Däremot har regionen ingen rutin för att kontinuerligt säkerställa att dataskyddsombudets kunskap förblir riktig och aktuell över tid. Regionen har inte heller någon rutin för att säkerställa att dataskyddsombudet får allt stöd som krävs för att kunna utföra sina uppgifter enligt dataskyddsförordningen. I nuläget är regionens dataskyddsombud och informationssäkerhets-samordnare samma person, vilket innebär en risk för intressekonflikt och avsaknad av objektivitet.	Regionen har ingen rutin för att kontinuerligt säkerställa att dataskyddsombudets kunskap förblir riktig och aktuell över tid. Det har inte genomförts en dokumenterad analys för att säkerställa att det inte finns några intressekonflikter mellan dataskyddsombud och övriga arbetsuppgifter.	
Behandling av personuppgifter	Det framgick under intervjuer att både regionstyrelsen och hälso- och sjukvårdsnämnden hanterar känsliga personuppgifter. Vidare framkom det att insamlande av samtycke inte är vanligt förekommande eftersom en majoritet av behandlade personuppgifter är av allmänintresse. Exempelvis är regionen skyldig att dokumentera personuppgifter inom sjukvården. Regionen har dock en dokumenterad riktlinje för hur insamlande av samtycke ska ske, bl.a. att den registrerade måste ha samtyckt aktivt. Riktlinjen för samtyckeshantering är inte uppdaterad sedan 2018 och det har inte säkerställts att den förhåller sig till krav i dataskyddsförordningen. Efterlevnad av rutin kring samtyckesinsamling säkerställs genom att laglig grund för personuppgiftsbehandling registreras i registerförteckning av personuppgiftsbehandlingar. Både regionstyrelsen och hälso- och sjukvårdsnämnden har i enlighet med kraven i dataskyddsförordningen ett dokumenterat register över alla personuppgiftsbehandlingar. Det finns även en dokumenterad riktlinje som beskriver hur registret ska föras. Enligt riktlinjen skall respektive verksamhetschef inventera samtliga personuppgifts-behandlingar som verksamheten utför och registerföra dessa. Verksamheten skall kvalitetsgranska registerförteckningen årligen. Det saknas dock dokumenterad uppföljning avseende efterlevnad av riktlinjen avseende registerförteckning över personuppgiftsbehandlingar. Riktlinjen beskriver även att samtliga personuppgiftsbehandlingar är ändamålsbegränsade och att inga ändringar ska ske utan den registrerades vetskap. Enligt intervjuade nyckelperson i arbetet med GDPR skapas en incident ifall personuppgifter används till inkorrekt ändamål. I nuläget saknar regionen dock en process för att säkerställa att riktlinjerna kring ändamålsbegränsning	Regionen har inte säkerställt att riktlinjen för samtyckeshantering förhåller sig till uppdaterade krav i dataskyddsförordningen. Regionen har inte kontrollerat och säkerställt att personuppgifter endast används till de ändamål de var insamlade för. Regionen har inte säkerställt att registerförteckningen är, samt förblir, komplett och riktig över tid. Det har inte säkerställts att regionen förhåller sig till uppdaterade sektorspecifika	1,83

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	efterlevs. Vidare saknas dokumenterad riktlinje för att hålla sig kontinuerligt uppdaterad kring sektorspecifika lagar avseende personuppgifter. Enligt dokumenterad riktlinje avseende arkivering sker gallring av personuppgifter enligt dokumenthanteringsplaner för den enskilda verksamheten. I dokumenthanteringsplanen ska tidsgräns för arkivering och gallring av olika typer av personuppgifter framgå. I vissa fall krävs ett särskilt beslut angående gallring. Dokumenthanteringsplaner för regionstyrelsen samt hälso- och sjukvårdsnämnden har ej blivit uppdaterade i enlighet med regionens dagliga rutiner och informationen är i vissa fall felaktig och utdaterad. Vidare har regionen inte säkerställt att dokumenthanteringsplaner förhåller sig till aktuella gallringsfrister. Enligt intervjuad nyckelperson har regionen kontroller på plats för att säkerställa att anställda har korrekta behörigheter, såsom upplägg av ny behörighet och periodisk genomgång av behörigheter. Däremot finns inga dokumenterade riktlinjer för behörighetskontroll kopplat till riskbedömning utifrån personuppgiftsbehandling för respektive system och behörighet. Regionen har även dokumenterade riktlinjer kring loggkontroller där det i riktlinjen framgår att verksamhetscheferna ansvarar för att sätta upp lokala rutiner för loggkontroller, samt rutiner för att säkerställa efterlevnad. Riktlinjen beskriver även att en systematisk stickprovskontroll av loggverktyget ska genomföras, i syfte att kontrollera efterlevnad. Regionen har däremot inte följt upp och kontrollerat att riktlinjerna efterlevs för samtliga behörighets- och loggkontroller. EY har tagit del av en överblick av regionens systemlandskap som beskriver vilka typer av system som hanterar personuppgifter. Däremot framgår inte regionens samtliga system som hanterar personuppgifter. Regionen har inte heller dokumenterat hur personuppgifter flödar mellan system som hanterar personuppgifter.	lagar avseende personuppgifter. Det har inte säkerställts att personuppgifter gallras enligt aktuella gallringsfrister. Behörighetskontroller är inte anpassade utefter riskbedömning av personuppgiftshantering. Regionen har inte säkerställt att behörighet- och loggkontroller genomförs i praktiken enligt riktlinjer. Det saknas dokumenterat dataflöde av personuppgifter mellan systemen.	
Val av skyddsåtgärder	Enligt intervjuade nyckelpersoner inom regionens arbete med GDPR sker klassificering av strukturerad information i KLASSA enligt SKR:s verktyg för klassificering. Däremot har regionen i nuläget ingen rutin för klassificering av ostrukturerad information. Vidare har regionen definierat vad som klassas som känslig personuppgift, och dessa klassningar överensstämmer med definitioner i dataskyddsförordningen. I samband med införandet av dataskyddsförordningen 2018 genomförde regionen GDPR-utbildningar. Enligt intervjuade nyckelpersoner är denna utbildning inte något som strukturerat har följts upp och utbildningar	En rutin för att säkerställa att ostrukturerad information blir klassificerad har inte implementerats. Regionen har inte etablerat en process som säkerställer att utbildningar om dataskyddsförordningen	1,88

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	sker just nu på efterfrågan. Även om det pågår ett arbete för att ta fram en strukturerad utbildningsplan så har regionen i dagsläget ingen kontinuerlig uppföljning av utbildning för att säkerställa anställdas kunskap inom området. Viss utbildning gällande dataskydd finns på regionens intranät vilket är tillgängligt för samtliga medarbetare inom regionen.	uppdateras och genomförs regelbundet av nyanställda såväl som av befintliga anställda.	
Inbyggt dataskydd	Regionen har genomfört vissa åtgärder för att minska risken att regionen tar del av information som inte är nödvändig för definierat ändamål. Vidare arbetar regionen utefter riktlinjer och arbetssätt för säker hantering av patientuppgifter. Däremot har regionen i nuläget ingen rutin eller strukturerat arbete på plats för att ta specifik hänsyn till integritetsskyddsreglerna redan vid utvecklande av interna system. Därmed är inte inbyggt dataskydd en metod som regionen systematiskt använder för att säkerställa att man lever upp till dataskyddsförordningens krav i sin databehandling. Vidare har regionen ingen rutin på plats för att uppfylla kravet på lagrings- och uppgiftsminimering.	Regionen tar inte hänsyn till integritetsskyddsreglerna angående dataskydd i utvecklingsfasen av internutvecklade IT-system.	1,33
Hantering av leverantörsrelationer	Enligt dokumenterad riktlinje ska biträdesavtal som bygger på SKR:s avtalsmall tecknas med samtliga leverantörer, och kraven på personuppgiftsbiträden följer därefter. Ur SKR:s mall för biträdesavtal följer krav på att personuppgiftsbiträden ska följa patientdatalagen och relevant lagstiftning gällande GDPR. Det finns däremot ingen rutin på plats för att säkerställa att detta efterlevs för samtliga leverantörer. Regionen har inte någon dokumenterad rutin på plats för att bedöma om leverantörer lever upp till regionens krav och förväntningar, men enligt intervju med nyckelperson inom regionens dataskyddsarbete sker det i nuläget ett arbete kring utveckling och förbättring av regionens leverantörsbedömning. Personuppgifter som är tillgängliga för leverantörer är registerförda. Enligt biträdesavtal tecknade med leverantören ska incidenter kopplade till personuppgifter hanteras enligt regionens interna incidenthanteringsriktlinjer. Eventuella underleverantörer framkommer vid upphandling av biträde. Vid förändring av underleverantör ska regionen enligt biträdesavtalet meddelas. Dataöverföring av personuppgifter utanför Europeiska ekonomiska samarbetsområdet (EES) och Europeiska Unionen (EU) förekommer inom regionen. Inventering och konsekvensbedömning har genomförts för tredjelandsöverföring för att säkerställa att kraven i dataskyddsförordningen följs, samt för att bedöma risk. Det finns även dokumenterad vägledning för tredjelandsöverföring. Däremot finns ingen rutin för att säkerställa att vägledningen efterlevs.	Regionen har inte säkerställt att pub-avtal med leverantörer uppdateras vid behov, exempelvis vid förändringar i regelverk. Regionen har inte säkerställt att leverantörer och tredjeparter följer dataskyddsförordningen över tid. Regionen har inte säkerställt att dataöverföring utanför Europeiska ekonomiska samarbetsområdet (EES) och Europeiska Unionen (EU) sker enligt dokumenterad rutin.	2,10

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	Enligt intervjuade nyckelpersoner inom regionens arbete med dataskydd hanteras personuppgifter i mindre utsträckning i molntjänsten Microsoft Office 365. I en dokumenterad riktlinje har regionen beskrivit att känsliga personuppgifter eller information som omfattas av offentlighets- och sekretesslagen inte får hanteras i Microsoft Office 365. Ur riktlinjen framkommer även att det ska genomföras riskbedömning vid osäkerhet kring vilken information som får lov att lagras i molntjänsten Microsoft Office 365. I nuläget finns det däremot ingen rutin på plats för att kontrollera och säkerställa att personuppgifter i molnet hanteras enligt riktlinjer.	Regionen har inte säkerställt att riktlinje kring personuppgiftshantering i molntjänster efterlevs.	
Hantering av incidenter	Regionen har en dokumenterad riktlinje för rapportering och utredning av personuppgiftsincidenter. Riktlinjen beskriver hur varje säkerhetsincident som rör personuppgifter ska dokumenteras och att alla allvarliga personuppgiftsincidenter ska anmälas till IMY samt att de registrerade ska informeras vid allvarlig personuppgiftsincident. Riktlinjerna för hantering av personuppgiftsincidenter avseende den information som ska lämnas till de registrerade vid incident uppfyller kraven enligt dataskyddsförordningen. Regionen registrerar samtliga personuppgiftsincidenter som rapporteras, med en efterföljande utredning. Enligt riktlinjen bedöms allvarlighet av incidenten samt att det genomförs uppföljning av varje personuppgiftsincident för att bedöma om ytterligare åtgärder behöver vidtas. Regionen har däremot ingen dokumenterad rutin som säkerställer att ledning, anställda och leverantörer är medvetna om lagar och förpliktelser i samband med personuppgiftsincidenter, samt ifall samtliga personuppgiftsincidenter rapporteras enligt riktlinjer. Det finns i nuläget ingen formell process för att följa förändringar i lagkrav gällande personuppgiftsincidenter.	Regionen har inte säkerställt att rutinen kring incidenthantering efterlevs i praktiken.	2,36
Information till registrerade	Information kring hur den registrerades personuppgift kommer användas samt hur den registrerade kommer åt sin personuppgift finns på regionens hemsida, vilket innebär att den registrerade på eget initiativ behöver uppsöka informationen. Regionen har i nuläget ingen strukturerad process avseende vilken information som ska lämnas till registrerade vid insamling av personuppgifter. För information till allmänheten så har regionen en utsedd kommunikatör är kopplad till regionens ledningsstab. Dock är det inte formaliserat att denne specifikt ansvarar för information gällande personuppgiftsincidenter.	Regionen saknar generell rutin för vilken information som ska lämnas till den registrerade vid insamling av personuppgifter. Ansvarig för information till allmänhet gällande personuppgifter har inte formaliserats.	1,38
Begäran från registrerade	Regionen har en dokumenterad riktlinje för enskildas rättigheter enligt GDPR i vilket det beskrivs vilka rättigheter den registrerade har samt att information ska skickas inom en månad av mottagen begäran i ett	Det har inte säkerställts att verksamheterna har utvecklat rutiner för att efterleva den	1,56

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

	format som den registrerade kan tillgodogöra sig. Respektive verksamhetschef ansvarar för att skapa rutiner för att efterleva den enskildas rättigheter enligt GDPR. Dessa rutiner har dock inte kunnat uppvisats vid tiden för granskning. Registrerade kommer i kontakt med regionen genom dataskyddsmejlen (vilken hänvisas till på regionens hemsida), men det finns ingen rutin på plats för att hantera begäran av personuppgifter från registrerade.	enskildas rättigheter enligt GDPR. Regionen saknar rutin för hur verksamheten hanterar registrerade som begär ut personuppgifter.	
Profilering	Profilering förekommer inte i regionen.	-	-

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

5 Bilaga 2: Förteckning över intervjuade funktioner

- Dataskyddombud och informationssäkerhetssamordnare, 2022-02-07
- Dataskyddsombud, 2022-02-07
- Arkivarie, 2022-02-07
- Verksamhetschef IT, 2022-02-22
- Specialist Digitalisering, 2022-02-24
- Systemutvecklare, 2022-02-25

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

6 Bilaga 3: Dokumentförteckning

- Arkivering av allmänna handlingar(163750)
- Att lämna ut allmän handling(423630)
- Behörighetsflöde NCS Cross 1.0
- Dataskyddsombud(304761)
- Diarieföring av allmänna handlingar(165680)
- Dokumenthanteringsplan för forskningsverksamhet_forskningsprojekt(370552)
- Dokumenthanteringsplan för hälso- och sjukvårdförvaltningens stab(247683)
- Dokumenthanteringsplan för patientinformation och övrig medicinsk dokumentation(370559)
- Dokumenthanteringsplan för personal- och lönehantering(380274)
- Dokumenthanteringsplan för sociala medier(194696)
- Dokumenthanteringsplan Hälso- och sjukvårdsnämnden
- Dokumenthanteringsplan Regionstyrelsen
- Enskildas rättigheter enligt GDPR(348203)
- Hälso- och sjukvårdsnämndens nämndprotokoll för 2021 (10 stycken)
- Hälso- och sjukvårdsnämndens internkontrollplan 2021
- Implementationsbeskrivning - BizTalk X-Ray Referrals - SCN-0075
- Informationssäkerhet(288601)
- Integrationsöverenskommelse - BizTalk X-Ray Referrals - SCN-0075
- IT-säkerhetsstrategi Region Västerbotten(356724)
- Kartläggning personuppgiftsöverföring tredje land
- Konsekvensbedömning avseende dataskydd
- Lagring av information i Microsoft Office 365(295593)
- Manual Journallogg reviderad 220202(442653)
- NCS Cross - Loggkontroller(236461)
- NCS Cross - Patienter med skyddade personuppgifter, sekretesskyddad(237649)
- Personuppgiftsbiträdesavtal med leverantörer, vägledning(315221)
- Personuppgiftshandläggare(292852)
- Personuppgiftsincidenter 2018
- Personuppgiftsincidenter 2019-2022
- Rapportering och utredning av personuppgiftsincidenter(289408)
- Regionstyrelsens nämndprotokoll för 2021 (9 stycken)
- Regionstyrelsens internkontrollplan 2021 & 2022
- Regionstyrelsens tillsynsrapport 2021
- Registerförteckning 2022
- Registerförteckning över personuppgiftsbehandlingar(286796)
- Samtyckesformulär_2021
- Samtyckeshantering
- Styrande dokument(188192)
- Superanvändare i ledningssystemet(414534)
- Systemberoenden Region Västerbotten
- Systemlandskap Region Västerbotten
- Systemutveckling där personuppgifter förekommer(286579)
- Uppdrag för att utveckla leverantörsbedömningen
- Vägledning tredjelandsöverföringar(441969)

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

7 Bilaga 4: Definitioner

Behandling: Med behandling menas varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Dataskyddsombud (DSO): Myndigheter och offentliga organ är skyldiga att utse dataskyddsombud. Dataskyddsombudets uppgifter är bland annat att informera och ge råd inom den egna organisationen om vilka skyldigheter som gäller enligt såväl förordningen som nationella bestämmelser. Ombudet ska också bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen. Slutligen ska ombudet fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna.
EU/EES: EU står för den Europeiska unionen och EES för Europeiska Ekonomiska Samarbetsområdet. I EU ingår följande länder Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Förenade Kungariket, Grekland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern, Österrike. I EES ingår utöver länderna i EU även Island, Liechtenstein och Norge.

Förhandssamråd: Om man vid en konsekvensbedömning bedömer att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken måste man samråda med Integritetsskyddsmyndigheten.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Informationssäkerhet: Berör i huvudsak säkerhetsfrågor som berör information, oberoende av system, eller plattformar.

Konsekvensanalys: Innan man inleder en behandling av personuppgifter som kan leda till en hög risk för integritetsintrång till exempel ett omfattande register med känsliga personuppgifter, måste man bedöma konsekvenserna för de registrerade (konsekvensbedömning).

Känslig personuppgift: Exempel på känsliga personuppgifter är ras och etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, biometriska och genetiska data, medlemskap i fackförening, hälsa eller uppgifter om fysisk persons sexualliv eller sexuell läggning.

Personuppgift: Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk levande person, d.v.s. medborgare, anställda m.fl. Exempel på personuppgifter är namn, personnummer, telefonnummer, bank- och kontouppgifter, IP-adress, försäkringsnummer m.m.

Personuppgiftsansvarig: Med personuppgiftsansvarig avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org. nr 556053-5873

Personuppgiftsbiträde: Med personuppgiftsbiträde avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för personuppgiftsansvarigs räkning.

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.

Policy och instruktion: Avser dokumentation av rutiner på ett eller annat sätt. I denna rapporten görs ingen skillnad på om dokumentationen är antagen på politisk eller tjänstemannanivå.

Profilering: Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Pseudonymisering: Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. De kompletterande uppgifterna ska förvaras separat och vara föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Register: En strukturerad samling av samtliga personuppgiftsbehandlingar som företas inom verksamheten.

Registrerad: Med registrerad avses den enskilde vars personuppgifter behandlas.

Samtycke: Med samtycke avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring från den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Tillsynsmyndighet: En oberoende offentlig myndighet som är utsedd av en medlemsstat. I Sverige är Integritetsskyddsmyndigheten tillsynsmyndighet.

Tredje land: Med tredje land avses ett land som inte är medlem i EU eller EES. En överföring till tredje land är när personuppgifter som behandlas i ett EU- eller EES-land görs tillgängliga i ett land utanför EU/EES-området. Exempelvis när personuppgifter i ett datoriserat register skrivs ut och skickas i pappersform eller när personuppgifter skickas via e-post. Personuppgifter får föras över endast om det finns en adekvat skyddsnivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de registrerades rättigheter skyddas.

Tredje part: Med tredje part avses en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.