Granskning av dataskyddsarbetet

Rapport

Västra Götalandsregionen

KPMG AB

Datum 2022-12-14

Antal sidor 30

Västra Götalandsregionen
Granskning av dataskyddsarbetet

2022-12-14

Innehållsförteckning

1 Sammanfattning

KPMG har av Västra Götalandsregionens revisorer fått i uppdrag att granska efterlevnad av dataskyddsförordningen inom koncernkontoret vilket ingår i regionstyrelsens personuppgiftsansvar. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen inte säkerställt att den inom sitt personuppgiftsansvar bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Vi baserar vår bedömning på följande iakttagelser:

- Roller och ansvar är otydliga och det har inte etablerats en dataskyddsorganisation som motsvarar behov och omfattning av dataskyddsfrågorna.
- Dataskyddsarbetet är inte integrerat i regionens ledningssystem för informationssäkerhet.
- Registerförteckning är inte komplett och i vissa delar inaktuell och i behov av översyn och revidering.
- Utbildningsinsatser är inte obligatoriska och har inte genomförts med en tillräcklig regelbundenhet för att etablera tillräckliga kunskaper och medvetenhet vid hantering av personuppgifter.
- Det saknas etablerad kontroll och uppföljning av regionstyrelsens dataskyddsarbete och efterlevnad av dataskyddsförordningen.

Granskningens resultat visar att regionstyrelsen har en bristande efterlevnad av dataskyddsförordningen. Detta medför bland annat risk för skada för de registrerade men även risk för regionen i form av förtroendeskada eller ekonomisk skada om en bristande efterlevnad av dataskyddsförordningen medför sanktionsavgifter eller skadestånd.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen att:

— Etablera en dataskyddsorganisation med tillräckliga resurser att stödja dataskyddsombud i utförande av de uppgifter som dataskyddsförordningen ställer krav på.

— Komplettera nuvarande riktlinje och rutiner med ansvarsbeskrivningar för nyckelroller.

— Integrera dataskyddsarbetet i ledningssystemet för informationssäkerhet genom att komplettera styrdokument med krav avseende personuppgiftshanteringen.

— Upprätta registerförteckning för samtliga personuppgiftsbehandlingar inom regionstyrelsens personuppgiftsansvar.

— Erbjuda regelbunden utbildning till samtliga medarbetare som hanterar personuppgifter, samt avväga vilka kompletterande utbildningar som bör erbjudas nyckelfunktioner och ansvariga i dataskyddsarbetet.

— Tydliggöra incidenthanteringsrutiner med instruktioner om när personuppgiftsansvariga ska informeras.

— Tillse att dataskyddsombud genomför årlig granskning av dataskyddsarbetet med bedömning av efterlevnad av dataskyddsförordningen och att uppföljning rapporteras till regionstyrelsen.

2 Bakgrund

Västra Götalandsregionen hanterar en stor mängd personuppgifter där flertalet är att klassa som känsliga. Det ställer höga krav på att hanteringen av dessa så att den sker utifrån de krav som dataskyddsförordningen stipulerar. Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679 gäller i hela EU och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998.

Det främsta syftet med dataskyddsförordningen är skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället. I jämförelse med PUL ställer Dataskyddsförordningen högre krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter. Vid överträdelse av förordningens artiklar föreligger skärpta sanktioner.

Med utgångspunkt från ovan har regionens revisorer bedömt att efterlevnad och mognad avseende koncernkontorets dataskyddsarbete bör granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om regionstyrelsen bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Granskningen har besvarat följande revisionsfrågor:

- Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade för att uppnå regelefterlevnad av dataskyddsförordningen?
- Har styrelsen genom beslut fastställt en arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningens krav?
- Finns registerförteckning upprättad för de personuppgiftsbehandlingar där styrelsen är personuppgiftsansvarig?

- Har konsekvensbedömningar gjorts på personuppgiftsbehandlingar som kan bedömas ha en påverkan på den registrerades rättigheter och friheter?
- Har åtgärder vidtagits för att säkerställa en tillräcklig kunskap hos medarbetarna om de krav som ställs på personuppgiftshanteringen?
- Finns etablerade rutiner och en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav?
- Har regionstyrelsen en ändamålsenlig kontroll och uppföljning av arbetet utifrån dataskyddsförordningen?

Granskningen avser Regionstyrelsen och avgränsas till dataskyddsarbetet inom koncernkontorets verksamheter.

2.2 Revisionskriterier

Vi har bedömt om regionstyrelsen bedriver dataskyddsarbete i enlighet med:

- Kommunallagen (2017:725) kap. 6 § 6 kap
- Dataskyddsförordningen
- Policy för styrning i Västra Götalandsregionen (RS 2019–02491)

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Ledningssystem för informationssäkerhet
- Riktlinje behandling av personuppgifter i Västra Götalandsregionen
- Rutin Rapportering vid personuppgiftsincident
- Rapport från Dataskyddsombud, 2021

Intervjuer har genomförts med:

- Regionjurist
- Funktionsansvarig informationssäkerhet och dataskydd
- Regionutvecklare informationssäkerhet och dataskydd

Dataskyddsombud för regionstyrelsen saknades vid tiden för granskningen.

Rapporten är faktakontrollerad av samtliga intervjupersoner.

3 Dataskyddsförordningen

Dataskyddsförordningen trädde i kraft den 25 maj 2018. Lagstiftningen syftar bland annat till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för dataskyddsförordningen. Tillsynsmyndighet ska säkerställa påförande av administrativa sanktionsavgifter för överträdelser av förordningen. Sanktioner ska vara i nivåer för att fungera effektivt, proportionellt och avskräckande.

Hantering av personuppgifter ska ske utifrån förordningens grundläggande principer enligt följande:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”rättslig grund”. Utan en rättslig grund är personuppgiftsbehandling ej laglig.

4 Resultat av granskningen

4.1 Styrning av dataskyddsarbetet

4.1.1 Ledningssystem för informationssäkerhet

Regionstyrelsen har etablerat ett ledningssystem för informationssäkerhet, ett så kallat LIS. LIS utgörs främst av en fastställd Riktlinje för informationssäkerhet[1] med en indelning i olika avsnitt och mer detaljerade riktlinjer och rutiner som syftar till att etablera en styrning av det övergripande informationssäkerhetsarbetet.

Då LIS etablerades 2015, innan dataskyddsförordningen trädde i kraft, och endast i vissa delar har reviderats och kompletterats saknas i ledningssystemet en styrning av dataskyddsarbetet utifrån dataskyddsförordningens anvisningar och krav. Däremot finns vissa beskrivningar av krav och åtgärder som har sin utgångspunkt i Personuppgiftslagen, den tidigare lagstiftningen för personuppgiftshantering som dataskyddsförordningen ersatt.

Dåvarande dataskyddsombud har upprättat en rapport som beskriver regionstyrelsens dataskyddsarbete under perioden mars 2020 – mars 2021[2]. Av rapporten framgår att det saknas en styr- och förvaltningsmodell för dataskyddsarbetet. Det är därtill, utifrån beskrivningen ovan, otydligt hur arbetssätt och metoder i dataskyddsarbetet förhåller sig till regionens LIS.

En ny Riktlinje för informationssäkerhet[3] har beslutats 2018 som är gällande parallellt med den tidigare riktlinjen, enligt verkställighetsbeslut av regiondirektören[4]. Den nya

[1] Riktlinjer för informationssäkerhet i Västra Götalandsregionen, Regionstyrelsen, 2015-09-01,

[2] Dataskyddsombudets granskning enligt artikel 39 GDPR, 2021-04-09, dnr saknas.

[3] Beslutad av regionstyrelsen, 2018-12-11 § 349, dnr RS 2018 - 00129

[4] Beslut av regiondirektören, 2019-03-07, dnr RS 2019-01501

riktlinjen anger att dataskyddsförordningen är en av de portallagstiftningar som regionens informationssäkerhetsarbete ska omfatta.

Regionstyrelsen har därtill beslutat om Riktlinje för behandling av personuppgifter[5] vilken presenteras nedan tillsammans med Rutin för rapportering av personuppgiftsincident[6].

4.1.2 Riktlinje Behandling av personuppgifter i Västra Götalandsregionen

Regionstyrelsen har beslutat om Riktlinje för behandling av personuppgifter. Riktlinjen beskriver hantering av personuppgifter utifrån dataskyddförordningens grundläggande principer och dess relation till offentlighetsprincipen och arkivlagen. Enligt dokumentet riktar den sig till alla medarbetare i VGR som på något sätt hanterar personuppgifter.

4.1.3 Rutin Rapportering vid personuppgiftsincident

Det finns en beslutad rutin för Rapportering vid personuppgiftsincident. I rutinen finns en beskriven incidenthanteringsprocess. Det finns även instruktion om när kontakt ska tas med de registrerade samt hantering när incidenter ska anmälas till tillsynsmyndighet. Vi noterar att rutinen anger att kontakt ska tas med Datainspektionen. Myndigheten har dock från 2021 bytt namn till Integritetsskyddsmyndigheten.

4.1.4 Personuppgiftsansvar

Varje nämnd och styrelse i VGR har personuppgiftsansvaret för sin behandling av personuppgifter. Enligt reglementet för regionstyrelsen (RS 2018-03535) är styrelsen personuppgiftsansvarig för de register och andra behandlingar av personuppgifter som sker i styrelsens verksamhet. Beslut med anledning av

[5] Beslutad av regionstyrelsen 2019-08-27, dnr RS 2019-00485

[6] Direktör på Koncernkontorets stab för utförarstyrning och samordning 2018-05-25, dnr RS-2018-02985

regionstyrelsens personuppgiftsansvar är delegerat till regiondirektören[7]. Denna granskning avser koncernkontorets hantering av personuppgifter vilket ingår i regionstyrelsens personuppgiftsansvar.

4.1.5 Bedömning

Vår bedömning är att regionstyrelsen till viss del har tillsett att det finns styrande dokument för regionens dataskyddsarbete. Vår bedömning är dock att nuvarande dokument är alltför övergripande för att säkerställa efterlevnad av dataskyddsförordningen.

Vår bedömning är därtill att det är en brist att inte krav enligt dataskyddsförordningen är inkluderade i regionens ledningssystem för informationssäkerhet mer än genom en laghänvisning i riktlinje för informationssäkerhet (2018). Detta då hantering av integritetskänslig information är en väsentlig del i det systematiska informationssäkerhetsarbetet tillsammans med efterlevnad av övriga portallagstiftningar som riktlinjen inkluderar.

[7] Regionstyrelsens delegeringsordning antagen 2019-10-15 § 292

4.2 Dataskyddsorganisation

4.2.1 Resurser i dataskyddsarbetet

I dataskyddsförordningens artikel 38 som reglerar dataskyddsombudets ställning framgår krav på att den personuppgiftsansvariga ska stödja dataskyddsombudet i utförande av de uppgifter som åligger dataskyddsombudet, se avsnitt 4.2.2, genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter. Därtill framgår att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

Inom koncernkontoret finns Enheten för säkerhet och beredskap, ESB. Enheten har en funktion för informationssäkerhet och dataskydd som leds och samordnas av en funktionsledare. Enhetens och funktionernas uppdrag är främst samordning av regionens dataskyddsarbete. Funktionen ansvarar för framtagande av ledningssystem för informationssäkerhet och dataskydd. Medarbetare inom funktionen alternerar hantering av rapporterade incidenter enligt schema och samordnar utredning och analyser när incidenter rör flera personuppgiftsansvariga inom VGR. Därtill finns en regionutvecklare med ansvar inom informationssäkerhet och dataskydd. Regionutvecklaren har även en roll när det sker regionövergripande händelser inom dataskyddsområdet där samordning krävs i utredning eller analyser, exempelvis vid personuppgiftsincidenter.

ESB har tagit fram ett förslag till dataskyddsorganisation med definierade roller som det finns behov av i regionens dataskyddsarbete. Enligt förslaget ska varje förvaltning utse dataskyddssamordnare. Dessa ska vara kontaktpersoner i dataskyddsfrågor och ansvara för hanteringen av vissa uppgifter kopplat till dataskyddsförordningen som åligger myndigheten.

Enligt intervjuuppgifter finns i nuläget utsedda dataskyddssamordnare i flertalet förvaltningar inom VGR. Då det inom koncernkontoret under en tid har saknats en dataskyddssamordnare har vissa arbetsuppgifter fördelats på resurser från en annan

enhet inom koncernavdelning ärendesamordning och kansli. Även medarbetare inom funktion informationssäkerhet och dataskydd på ESB har utfört arbetsuppgifter som är avsedda för dataskyddssamordaren. En ny dataskyddssamordnare har utsetts under hösten 2022.

I styrande dokument avseende informationssäkerhet och dataskydd saknas beskrivning av dataskyddssamordnarnas ansvar och uppdrag.
I det interna beslutsunderlag som vi beskrivit tidigare i rapporten avseende samordning av dataskyddsombuden i regionen, framgår dock följande beskrivning av dataskyddssamordnarens uppgifter:

- ta fram handlingsplaner
- hantera begäran om registerutdrag från registrerade
- hantera personuppgiftsincidenter
- säkerställa att personuppgiftsbiträdesavtal finns
- utföra registervård
- informera och utbilda i dataskydd inom den egna förvaltningen,
- följa upp den egna förvaltningens dataskyddsarbete
- delta och stötta vid riskanalyser, konsekvensbedömningar och informationsklassningar inom den egna förvaltningen.

4.2.2 Dataskyddsombud

Utnämning av dataskyddsombud

Dataskyddsförordningen, artikel 37.1, fastställer krav på när ett dataskyddsombud, (DSO) ska utses. Enligt artikeln ska ett dataskyddsombud utses om personuppgiftsbehandlingen genomförs av en myndighet eller ett offentligt organ. Beslutet ska dokumenteras och vara protokollfört. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Vi har i granskningen tagit del av delegationsbeslut fattat av regiondirektören där nytt dataskyddsombud för regionstyrelsen har utsetts. Delegationsbeslutet är noterat i regionstyrelsens protokoll 2022-05-17[8]. Det framgår av beslutet att nytt dataskyddsombud anmälts till Integritetsskyddsmyndigheten. I regionstyrelsens delegeringsordning finns delegation till regiondirektören att besluta om dataskyddsombud för regionstyrelsens räkning. Det dataskyddsombud som utsågs i april 2022 har enligt protokollet även anmälts till Integritetsskyddsmyndigheten.

Vid tidpunkten för granskningen har utsett dataskyddsombud avslutat sin roll som dataskyddsombud för regionstyrelsen. Vi har inte i protokoll kunnat notera att regiondirektören meddelat avslut av dataskyddsombud till regionstyrelsen under punkt delegeringsärenden eller att detta anmälts till Integritetsskyddsmyndigheten. Det har inte heller utnämnts något nytt dataskyddsombud för regionstyrelsen och ingen anmälan har gjorts till Integritetsskyddsmyndigheten vid tiden för granskningens genomförande.

Tidigare dataskyddsombud för regionstyrelsen var anställd inom Enhet juridik på koncernkontoret, som tillhör koncernavdelning Ärendesamordning och kansli. Då tidigare ombud slutat var rollen vid tiden för granskningen vakant. Tidigare

[8] Diarienummer RS 2021-06383

dataskyddsombudet var förutom dataskyddsombud för regionstyrelsen även dataskyddsombud för 17 andra styrelser och nämnder i VGR.

Rekrytering hade genomförts vid tiden för intervjuer i granskningen och nytt dataskyddsombud planerades tillträda under december 2022. I avvaktan på att nytt ombud kommer på plats samordnas dataskyddsarbetet mellan jurister inom Enhet juridik.

Det finns ett upprättat förslag till beslut om central samordning av regionens dataskyddsombud. Förutom det tidigare dataskyddsombudet för regionstyrelsen finns ytterligare sex dataskyddsombud utsedda inom VGR för andra personuppgiftsansvariga styrelser och nämnder. Det framgår av ett internt beslutsunderlag som vi tagit del av.

Förslaget innebär att en central organisation skapas där samtliga dataskyddsombud i VGR tillhör samma enhet, Enhet juridik. Av förslaget framgår att syftet med den nya organisationen är att få en effektivare samordning och ett mer enhetligt utförande av dataskyddsombudens ansvar och arbetsuppgifter. Den nya organiseringen av dataskyddsombud ska enligt förslaget därtill stärka dataskyddsombudens fristående ställning från den personuppgiftsansvariga myndigheten. I förslaget uppskattas behovet uppgå till fem dataskyddsombud för att täcka det totala behovet inom hela VGR.

Det har inte fattats något formellt beslut om organisering vid tiden för granskningens genomförande.

Dataskyddsombudets uppgifter

Dataskyddsombudet ska enligt dataskyddsförordningens artikel 37 utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.

Intervjuade uppger att tidigare dataskyddsombud för regionstyrelsen varit kompetent och motsvarat de krav som ställs i dataskyddsförordningen på rollen dataskyddsombud.

Enligt dataskyddsförordningen, artikel 39 ska dataskyddsombudet ha minst följande uppgifter:

Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt dataskyddsförordningen.

- Att övervaka och kontrollera efterlevnaden av dataskyddsförordningen.
- Att övervaka och kontrollera efterlevnaden av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripen ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
- Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.
- Att samarbeta med tillsynsmyndigheten.
- Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, och vid behov samråda i alla andra frågor.

Europeiska dataskyddsstyrelsens riktlinjer fastställer att dataskyddsombudets främsta prioritering bör vara ett möjliggöra efterlevnad av dataskyddsförordningen.

I de styrande dokument som är upprättade för dataskyddsarbetet inom VGR saknas beskrivning av dataskyddsombudets ansvar och uppdrag. Genom vår dokumentgranskning och de uppgifter vi fått i intervjuer saknas beslut där regionstyrelsen fastställt en arbetsbeskrivning för dataskyddsombudet som är utsett för regionstyrelsen.

Av dataskyddsombudets rapport, publicerad i mars 2021, framgår att det saknas tydlig information om rollen, vilka forum som dataskyddsombud ska ingå i samt vid vilka typer av beslut som dataskyddsombud ska kontaktas. Därtill bedöms resurserna både i det strategiska och operativa arbetet vara bristfälliga vilket medför att väsentliga aktiviteter i dataskyddsarbetet inte har kunnat genomföras.

I regionens ledningssystem för informationssäkerhet som bland annat utgörs av Riktlinjer för informationssäkerhet (2015) finns en beskrivning av rollen Personuppgiftsombud (PuO) utifrån den tidigare gällande lagstiftningen Personuppgiftslagen (PUL). PuO har enligt dokumentet till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt genomföra revision.

4.2.3 Bedömning

Vår bedömning är att regionstyrelsen inte genom beslut fastställt en arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningens krav. Vi uppfattar att tidigare utnämnt dataskyddsombud för regionstyrelsen motsvarade de yrkesmässiga kvalifikationer som krävs enligt förordningen. Däremot har dataskyddsombudet inte haft tillräckliga förutsättningar att utföra de uppgifter som artikel 39 i dataskyddsförordningen reglerar. Det finns till viss del resurser för att stödja dataskyddsombudet i dataskyddsarbetet. Det saknas dock beskrivning av ansvar och uppdrag för centrala roller i dataskyddsarbetet, bland annat funktionsansvarig informationssäkerhet och dataskydd inom ESB samt för koncernkontorets dataskyddssamordnare.

4.3 Registerförteckning

I enlighet med dataskyddsförordningen, artikel 30, ska varje personuppgiftsansvarig föra ett register över personuppgiftsbehandling som utförts under dess ansvar. Registerförteckningarna ska på begäran redovisas för Integritetsskyddsmyndigheten, där registren ska utgöra en grund för övervakning av behandling av personuppgifter.

I dataskyddsförordningen regleras vilka uppgifter en behandling minst ska innehålla. Bland annat måste personuppgiftsansvarig beskriva ändamål med behandlingen, beskrivning av kategorier av registrerade samt om behandlingen innehåller känsliga personuppgifter. Varje behandling måste ha en laglig grund för behandlingen.

Av dataskyddsförordningens principer för behandling av personuppgifter, kap 2, femte artikeln framgår att behandling av personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas utan dröjsmål ska raderas eller rättas.

Inom koncernkontoret dokumenteras personuppgiftsbehandlingar i en digital SharePoint-lösning. Förteckningen består av en lista med personuppgiftsbehandlingar som är identifierade inom regionstyrelsen. Enligt intervjuade saknas ett antal personuppgiftsbehandlingar i förteckningen och de som finns registrerade är inte fullt ut uppdaterade och aktuella. Vi har tagit del av regionstyrelsens registerförteckning där vi kan konstatera att flertalet behandlingar inte aktivt har reviderats sedan lagens inträde och den ursprungliga behandlingen påbörjades.

En orsak som nämns till att revidering inte gjorts är att systemstödet är bristfälligt och försvårar uppföljningsarbetet. Intervjuade uppger därtill att det finns behov att kunna dela information om informationsklassningar och riskbedömningar utifrån personuppgiftshanteringen. Exempelvis finns behov av att delge information till koncernstab digitalisering då det ofta krävs tekniska åtgärder för att skydda personuppgifter efter att bedömningar gjorts för uppgifter som hanteras i digitala

systemstöd och applikationer. I nuläget finns inte etablerade former för att dela information.

4.3.1 Konsekvensbedömning

Dataskyddsförordningen artikel 35 reglerar att den personuppgiftsansvarige, för vissa typer av behandlingar, ska före behandlingen ska utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Kravet gäller behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Detta kallas konsekvensbedömning. Den personuppgiftsansvariga ska rådfråga dataskyddsombudet vid genomförande av konsekvensbedömningar. Konsekvensbedömningar är särskilt viktigt vid användning av ny teknik.

Intervjuade beskriver att det genomförts konsekvensbedömningar för vissa behandlingar inom koncernkontoret. De som genomförts avser behandlingar som identifierats som högriskbehandlingar eller vid nya systeminföranden. Det framgår inte av dokumentation hur många konsekvensbedömningar som gjorts men i dataskyddsombudets rapport från 2021 framgår att denne agerat rådgivande eller genomfört konsekvensbedömningar.

Regionen har en mall för konsekvensbedömning som är tänkt att vara självinstruerande. Intervjuade har uppgett att dataskyddsombudet har deltagit aktivt som metodledare i upprättande av konsekvensbedömningar. Intervjuade beskriver dock att det kan leda till en problematik om dataskyddsombudet i fråga har varit operativ i genomförandet eftersom ombudet i sin roll ska göra interna revisioner av det arbete som har gjorts. Det finns då risk att ombudet inte kunna göra revisionen på ett oberoende sätt.

Det finns dock ett pågående arbete med att ta fram rutiner för när dataskyddsombud ska involveras och enligt dessa ska ombudet främst ge ett utlåtande på genomförda konsekvensbedömningar, inte vara den som praktiskt genomför bedömningen. Det är enligt intervjuade inte möjligt med befintliga resurser att dataskyddsombuden är

delaktiga i det operativa arbetet utan behöver avsätta tid för mer komplexa ärenden och även få utrymme för uppföljning och revision.

4.3.2 Bedömning

Vår bedömning är att regionstyrelsen har en upprättad registerförteckning för vissa av de personuppgiftsbehandlingar där styrelsen är personuppgiftsansvarig. Vi konstaterar att förteckningen inte är komplett och det finns en risk för att behandling av personuppgifter sker utan att behandlingen finns förtecknad. Befintliga personuppgiftsbehandlingar i förteckningen har inte fullt ut aktualiserats så att det går att fastställa att behandlingarna är aktuella och korrekta vilket är ett krav i dataskyddsförordningen.

Vår bedömning är att konsekvensbedömningar till viss del har gjorts men att det bör tydliggöras inom regionen när det finns krav på att konsekvensbedömning ska göras. Vidare anser vi att det bör utvärderas om de bedömningar som gjorts är korrekta utifrån dataskyddsförordningens krav och att det bör säkerställas att dataskyddsombud involveras vid upprättande av konsekvensbedömningar.

4.4 Medvetenhet och kunskap om dataskydd

Dataskyddsförordningen innehåller särskilda skyldigheter för de som behandlar personuppgifter. Behandling av personuppgifter får exempelvis endast ske efter instruktion från den personuppgiftsansvarige och behandlingen måste ske i enlighet med dataskyddsförordningens krav. Dataskyddsförordningens bestämmelser om de registrerades rättigheter innebär skyldigheter för de som behandlar personuppgifter. Detta medför att det behöver finnas en grundläggande kunskap och förståelse för de krav som ställs för att kunna skydda personuppgifter och hantera dem i enlighet med förordningen. I offentliga verksamheter som Västra Götalandsregionen hanterar ett stort antal anställda personuppgifter i olika situationer och för olika ändamål.

Intervjuade uppger att utbildningsinsatser genomfördes inom koncernkontoret vid tiden när dataskyddsförordningen trädde i kraft 2018. Det var digitala, korta utbildningspass som riktade sig till samtliga anställda i VGR. Utbildningen uppges finnas kvar i regionens utbildningsplattform. Koncernstab HR har mandat att besluta vilka utbildningar som ska vara obligatoriska för medarbetare i regionen. Bland de obligatoriska utbildningarna som beslutats ingår inte GDPR-utbildningen. Intervjupersoner uppger att anledningen till det är att utbildningen i dess nuvarande form inte anses ändamålsenlig. Det pågår ett arbete med att ta fram en ny GDPR-utbildning och avsikten är att den nya ska vara obligatorisk.

Det har inte gjorts någon samlad uppföljning över hur många som genomfört utbildningen inom koncernkontoret. Intervjuade beskriver att det finns exempel på incidenter som lett till att flera rapporteringar till Integritetsskyddsmyndigheten har behövt göras, mot bakgrund av bristande kunskap hos de som hanterat den initiala incidenten.

Dataskyddssamordnaren i respektive förvaltning har enligt intervjuade ansvar för att fånga upp behov av utbildningsinsatser och förmedla till Enheten för säkerhet och beredskap som kan samordna genomförandet av utbildningar. Enligt intervjuade har

det inte inkommit några förfrågningar om utbildningsinsatser till ESB, vare sig för koncernkontorets medarbetare eller för andra verksamheter i regionen.

Dataskyddsombudet har enligt intervjuade genomfört riktade utbildningsinsatser för funktioner inom koncernkontoret som bedömts som särskilt viktiga. Exempelvis nämns inköpsorganisationen som behöver kunskap för att ställa rätt krav i upphandlingar av nya system och tjänster samt för att upprätta personuppgiftsbiträdesavtal med externa leverantörer.

4.4.1 Bedömning

Vår bedömning är att regionstyrelsen delvis vidtagit åtgärder för att säkerställa en tillräcklig kunskap hos medarbetarna inom koncernkontoret om de krav som ställs på personuppgiftshanteringen i enlighet med dataskyddsförordningen.

Utbildningsinsatser har genomförts för ett antal år sedan. Det finns dock inte krav på att genomföra utbildningar inom dataskydd viket vi anser borde införas, med tanke på den mängd integritetskänsliga uppgifter som regionens medarbetare hanterar. De utbildningar som erbjudits tidigare har inte följts upp så att det finns kännedom om vilka som genomgått dessa. Om bristande kunskap finns hos enskilda medarbetare är detta förknippat med risker i den dagliga hanteringen men även risk för att personuppgiftsincidenter inte upptäcks så att de kan hanteras i enlighet med dataskyddsförordningens krav. Det finns risk för att det i sin tur kan leda till personlig skada för de registrerade men även för ekonomisk skada eller förtroendeskada för regionen.

4.5 Personuppgiftsincidenter

En personuppgiftsincident kan innebära risker för registrerade personers fri- och rättigheter och kan få allvarliga konsekvenser till exempel:

- ekonomisk skada
- diskriminering
- identitetsstöld
- bedrägeri
- skadlig ryktesspridning.

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan påverka tilltron till den organisation som behandlar personuppgifter. Den kan också leda till att Integritetsskyddsmyndigheten genom tillsyn kan döma ut sanktionsavgifter

I dataskyddsförordningens artikel 33 om anmälan av personuppgiftsincident framgår att personuppgiftsincident ska anmälas av personuppgiftsansvarig utan dröjsmål, senast inom 72 timmar till tillsynsmyndighet. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

I samband med incidentrapportering till Integritetsskyddsmyndigheten ska en beskrivning av incidenten göras tillsammans med de kategorier av och ungefärligt antal registrerade som berörts. Därtill ska konsekvenser beskrivas och de åtgärder som personuppgiftsansvarig vidtagit eller föreslår för att mildra potentiella negativa effekter.

Som vi nämnt tidigare, i avsnitt 4.1, finns en beslutad rutin för Rapportering vid personuppgiftsincident[9]. I rutinen finns en process för att hantera incidenter beskriven. Incidenter anmäls i systemet MedControl. Till hanteringen finns en dokumenterad lathund för handläggning av incident. Vi noterar att regionstyrelsen eller andra personuppgiftsansvariga inte är inkluderade i rutin- eller processbeskrivning och det är därigenom inte tydliggjort om och i vilka fall information eller rapportering ska göras till personuppgiftsansvariga.

ESB har en övervakning av de incidenter som registreras i MedControl och eskalerar dessa vid behov. Om en verksamhet berörs hanteras analys och fortsatta steg i processen av den som är utsedd incidentansvarig i den berörda verksamheten.

I rutin Rapportering vid personuppgiftsincidenter framgår att varje personuppgiftsansvarig ska utse en incidentansvarig. Incidentansvarig ska säkerställa att varje personuppgiftsincident omhändertas på rätt sätt.

Det är funktionen för informationssäkerhet och dataskydd som är incidentansvarig för koncernkontoret.

I rutinen regleras även att incidentansvarig skyndsamt, inte senare än 72 timmar efter att denne ha fått vetskap om en personuppgiftsincident, ska göra anmälan till Datainspektionen (nuvarande Integritetsskyddsmyndigheten) vilket är i enlighet med gällande lagkrav.

Intervjupersoner bekräftar att hanteringen inom VGR sker i enlighet med beslutad rutin och process. Dataskyddsombudet har i sin rapport, där regionstyrelsens ansvar granskats, beskrivit att hen i sin roll varit rådgivande vid incidenthantering och rapportering till tillsynsmyndighet.

[9] Fastställd av direktör på Koncernkontorets stab för utförarstyrning och samordning 2018-05-25, dnr RS-2018-02985

Vidare beskrivs i intervjuer att det finns behov av ytterligare utbildning för medarbetare och utvalda funktioner så att kunskap om incidenter och hur de ska hanteras om de inträffar är etablerad. Koncernkontoret har enligt intervjuade haft få anmälda personuppgiftsincidenter. En anledning till det, som uppges av intervjuade, är troligen att det inom koncernkontoret inte finns samma kultur av att anmäla incidenter och avvikelser som inom vården.

Enligt intervjuade sker i nuläget ingen regelbunden rapportering av inträffade incidenter till regionstyrelsen. En sammanställning av inträffade incidenter kan tas fram ur avvikelsehanteringssystemet, dock uppges inte systemet vara anpassat efter incidenter utan mer verksamhetsmässiga avvikelser. Det försvårar i vissa delar analys och uppföljning. Funktion informationssäkerhet och dataskydd har som rutin att gå igenom inträffade incidenter som en del i det systematiska förbättringsarbetet.

4.5.1 Bedömning

Vår bedömning är att regionstyrelsen tillsett att det finns etablerade rutiner och en ändamålsenlig organisation inom koncernkontoret för incidenthantering utifrån dataskyddsförordningens krav. Det finns systemstöd för att anmäla incidenter, mottagare för bedömning och tydliggjorda eskaleringsvägar till personuppgiftsansvarig verksamhet. Därtill rådfrågas dataskyddsombud vid behov i incidenthanteringen och rapportering. Vi ser dock behov av att det tydliggörs i rutiner på vilket sätt och vid vilka tillfällen regionstyrelsen, som personuppgiftsansvarig, ska delges information om inträffade incidenter.

Vi ser behov av att stärka kunskapen om vad som är incidenter genom utbildning och informationsinsatser. De utbildningstillfällen som erbjudits anser vi inte vara tillräckliga för att etablera en kunskap och medvetenhet. Om så inte sker finns en risk för att incidenter inträffar som inte uppmärksammas och anmäls, vilket dels utgör en risk för de registrerades integritet, dels en risk att incidenter inte är dokumenterade och kan beaktas i förbättringsarbetet.

4.6 Uppföljning och kontroll

I 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnder inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Av Policy för styrning i Västra Götalandsregionen[10] framgår att intern kontroll är en del av styrningen i regionen och ett redskap för ständiga förbättringar. Den interna kontrollen ska även säkerställa att regler och riktlinjer följs samt att rapportering och information i och om organisationen är tillförlitlig.

Som vi beskrivit i avsnitt 4.2.2, dataskyddsombudet uppgifter enligt förordningen, ingår att övervaka efterlevnaden av dataskyddsförordningen och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter. I detta ingår ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av sina uppgifter. Hen får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

Som beskrivits tidigare i granskningen har vi tagit del av dataskyddsombudets rapport avseende regionstyrelsens dataskyddsarbete från mars 2020 till mars 2021. Av rapportens avgränsning framgår att granskningen genomförts med vissa begränsningar. Bland annat uppges att dataskyddsombudet ska avsluta sin anställning

[10] Beslutad av: Regionfullmäktige 2019-05-28 §104, dnr RS 2019-02491

i anslutning till rapportens framtagande vilket medfört att färre intervjuer har genomförts än planerat och att antal styrande dokument som ingått i granskningen varit begränsat.

Granskningens resultat består av ett större antal rekommendationer. En handlingsplan presenteras med fyra åtgärder i följande prioriteringsordning enligt förslag från dataskyddsombud:

1. Roller och ansvar
2. Upprätta strategidokument
3. Ständiga förbättringar
4. Gemensamma forum

Rapporten har enligt dokumentet överlämnats till avdelning Ärendesamordning och kansli för vidare hantering och kommunicering. Enligt vad som framgår av dokumentet fanns en plan att delge regionstyrelsen en förkortad version av innehållet i rapporten. Vi uppfattar av intervjuade att så inte har skett. Det finns enligt intervjuade ingen etablerad rapporteringsväg från regionstyrelsens dataskyddsombud till regionstyrelsen.

I regionstyrelsens riskanalys med riskvärdering för upprättande av plan för intern kontroll 2022 saknas identifierade risker avseende dataskydd. Regionstyrelsens plan för intern kontroll 2022 saknar därmed kontrollåtgärder avseende dataskydd.

4.6.1 Bedömning

Vår bedömning är att regionstyrelsen inte har en ändamålsenlig kontroll och uppföljning av dataskyddsarbetet för att säkerställa efterlevnad av dataskyddsförordningen. Detta då det dels saknas kontrollmoment i regionstyrelsens interna kontroll, dels i övrigt inte har etablerats uppföljning av regionstyrelsens efterlevnad av dataskyddsförordningen.

Det finns inte någon etablerad och regelbunden rapportering av dataskyddsarbetet som genomförs så att regionstyrelsen är medveten om och har kännedom om eventuella risker och brister. Den granskningsrapport som dataskyddsombud har upprättat har inte delgetts regionstyrelsen i sin helhet. Interna granskningar, utförda av dataskyddsombud, är en av de uppgifter som åligger dataskyddsombud enligt dataskyddsförordningens reglering. Det är därtill ett viktigt underlag för personuppgiftsansvarigas kontroll av efterlevnad av dataskyddsförordningen och en väsentlig handling för att fatta beslut om åtgärder utifrån de rekommendationer som dataskyddsombud lämnar. Vi uppfattar att ett stort antal av de rekommendationer som gavs i granskningsrapporten 2021 inte har åtgärdats.

Mot denna bakgrund är vår bedömning att regionstyrelsen inte fullt ut följer bestämmelser om uppföljning och intern kontroll i reglemente, kommunallagens bestämmelser och Policy för styrning.

5 Slutsats och rekommendationer

5.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen inte säkerställt att den inom sitt personuppgiftsansvar bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Det finns till viss del styrande dokument för regionens dataskyddsarbete, nuvarande dokument är dock alltför övergripande för att säkerställa efterlevnad av dataskyddsförordningen. Bland annat saknas i stora delar beskrivning av ansvar för centrala roller i dataskyddsarbetet både inom koncernkontoret och i andra verksamheter. Då detta saknas och styrande dokument inte är tillräckligt konkreta ser vi en risk för att arbetet inte är ändamålsenligt och för brister i efterlevnaden som en konsekvens av detta.

Vi konstaterar i granskningen att registerförteckning över regionstyrelsens personuppgiftsbehandlingar inte är komplett och inte heller uppdaterad vilket medför en risk att förteckningen inte är korrekt i enlighet med de krav som förordningen ställer.

Det saknas i nuläget en regelbunden rapportering av dataskyddsarbetet från dataskyddsombud till regionstyrelsen. Det sker inte heller någon rapportering av inträffade incidenter så att regionstyrelsen som personuppgiftsansvarig är medveten om eventuella risker och brister i sin hantering av personuppgifter. Regionstyrelsen har genom detta brustit i sin kontroll och uppföljning av arbetet.

Granskningens resultat visar att regionstyrelsen har en bristande efterlevnad av dataskyddsförordningen. Detta medför bland annat risk för skada för de registrerade men även risk för regionen i form av förtroendeskada eller ekonomisk skada om en bristande efterlevnad av dataskyddsförordningen medför sanktionsavgifter eller skadestånd.

5.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen att:

- Etablera en dataskyddsorganisation med tillräckliga resurser att stödja dataskyddsombud i utförande av de uppgifter som dataskyddsförordningen ställer krav på.
- Komplettera nuvarande riktlinje och rutiner med ansvarsbeskrivningar för nyckelroller.
- Integrera dataskyddsarbetet i ledningssystemet för informationssäkerhet genom att komplettera styrdokument med krav avseende personuppgiftshanteringen.
- Upprätta registerförteckning för samtliga personuppgiftsbehandlingar inom regionstyrelsens personuppgiftsansvar.
- Erbjuda regelbunden utbildning till samtliga medarbetare som hanterar personuppgifter, samt avväga vilka kompletterande utbildningar som bör erbjudas nyckelfunktioner och ansvariga i dataskyddsarbetet.
- Tydliggöra incidenthanteringsrutiner med instruktioner om när personuppgiftsansvariga ska informeras.
- Tillse att dataskyddsombud genomför årlig granskning av dataskyddsarbetet med bedömning av efterlevnad av dataskyddsförordningen och att uppföljning rapporteras till regionstyrelsen.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor
Projektledare

Ida Larsson
Kommunal revisor

Veronica Hedlund Lundgren
Certifierad kommunal revisor
Kvalitetssäkrare