Årlig rapport till regionstyrelsen enligt ledningssystemet för informationssäkerhet och dataskydd 2022

Innehållsförteckning

1 Inledning

Betydelsen av ett välfungerande informationssäkerhets- och dataskyddsarbete blir allt större. Det rådande omvärldsläget parallellt med en digitaliseringsomställning i samhället ställer krav på såväl hög kunskap inom området som en välfungerande arbetsmetodik.

Specialistkompetensen inom informationssäkerhet och dataskydd är eftertraktad i hela Sverige vilket medför att det är relativt svårrekryterade profiler, så även för Region Skåne. Behovet av en stabil kompetensförsörjning inom organisationen är av betydelse för det kommande arbetet. Parallellt behöver säkerhetskulturen i hela Region Skåne öka. Dessa faktorer tillsammans kan ge både effektivare arbetssätt, arbetsmetoder och en hanterbar arbetsmiljö för medarbetarna.

Ett fortsatt fokus inom verksamheten är att implementera dataskydd i ledningssystemet för informationssäkerhet. Ledningssystemet för informationssäkerhet (LIS) ska gå till ett ledningssystem för informationssäkerhet och dataskydd (LISD). Målet är att nå ett systematiskt arbetssätt som ger en samlad kvalitetshöjning inom området.

I denna rapport belyses det arbete som har skett sedan föregående rapportering samt vissa av de utmaningar som organisationen står inför och som kommer prägla det fortsatta arbetet. En redogörelse ges även kring några av de omvärldsfaktorer som är viktiga att ta med i beaktning för att säkerställa att Region Skåne står väl rustad inför nuvarande och kommande krav som ställs inom informationssäkerhet och dataskydd.

2 Ledningssystem för informationssäkerhet och ledningens genomgång

Region Skånes ledningssystem för informationssäkerhet utgår ifrån SS-ISO/IEC 27000. I enlighet med fastställda riktlinjer för informationssäkerhet ska informationssäkerhetsarbetet vara en integrerad del av organisationens samtliga processer och övergripande ledningsstruktur. Detta genom att informationssäkerhet beaktas i utformningen av samtliga processer, informationssystem och säkerhetsåtgärder inom Region Skåne. Efterlevnaden av Region Skånes riktlinjer för informationssäkerhet samt uppföljning av beslutade kortsiktiga mål för informationssäkerheten i Region Skåne med förslag på eventuella justeringar ska årligen rapporteras.

Rapporten är framtagen av Region Skånes regionala funktioner för informationssäkerhet och dataskydd och avser perioden 2021-10-01 till 2022-09-31.

3 Status för åtgärder som beslutats vid tidigare genomgångar och måluppfyllnad

3.1 Måluppfyllnad – informationssäkerhet

För att uppnå de långsiktiga målen fastställs kortsiktiga mål som beslutas av Regionstyrelsen. De gällande kortsiktiga målen för informationssäkerhet beslutades av Regionstyrelsen 2021-04-29 och eventuella justeringar genomförs årligen.[1]

Arbeten pågår inom flera målområden.

- Införande av stödsystem för riskhantering kommer att genomföras. Stödsystemet kommer att medföra ett förändrat arbetssätt där man utgår från informationen istället för system som därmed också kräver en omställning i verksamheten med ett mer aktivt informationsägarskap. IT-stödet kommer också att möjliggöra ett

[1] Kortsiktiga mål för informationssäkerheten i Region Skåne

enhetligt systematiskt arbetssätt för informationsklassificeringar vilket på sikt medför bra beslutsunderlag för att arbetet inte behöver upprepas. Man återanvänder den data som tagits fram vid tidigare klassificeringar igen.

- Informationsägarebeslutet omarbetas och ska förtydliga vilka krav som ställs på beslutsunderlag för hur Region Skånes information ska hanteras.
- Arbete pågår för att öka säkerhetskulturen i Region Skåne. En grundutbildning är sedan tidigare framtagen och revideras vid behov, men ytterligare aktiviteter behöver genomföras.
- Ytterligare systematik i arbetet utvecklas genom att arbeta i ett gemensamt ledningssystem, LISD, och en gemensam årshjulsmetod. Uppföljning och förbättringsarbete kan bättre överskådas och ger möjlighet till specifika punktinsatser.

3.2 Måluppfyllnad– dataskydd

Dataskyddsorganisationens mål för 2021 var att krav och risker kopplade till tredjelandsöverföring ska vara målgruppsanpassade och kommunicerade. Arbete med en handlingsplan för organisationens hantering av tredjelandsöverföring pågår. Aktiviteterna har beretts i Region Skånes informationsstyrningsråd. Vägledning och informationsinsatser avseende krav och risker relaterade till tredjelandsöverföring genomförs löpande i Region Skånes informationssäkerhets- och dataskyddsorganisation. Vägledning ges även inom ramarna för Region Skånes riskhanteringsprocess i respektive ärende.

Framtida mål för dataskyddsorganisationen kommer i takt med att Region Skånes LIS utvecklas till ett LISD och därmed bli en del av de lång- och kortsiktiga målen för informationssäkerhet.

4 Förändringar i externa och interna frågor som är relevanta för ledningssystemet för informationssäkerhet

4.1 Externa förändringar

4.1.1 Tredjelandsöverföringar av personuppgifter

Om en organisation planerar överföring av personuppgifter till tredjeland måste skyddet för personuppgifter vara väsentligen likvärdigt det skydd som garanteras inom EU/EES. Att skyddet är väsentligen likvärdig är till exempel fallet om mottagarlandet omfattas av ett adekvansbeslut från EU-kommissionen. Vad gäller tredjelandsöverföring till mottagare i USA har följande steg tagits på vägen till laglig överföring under 2022:

- Principöverenskommelse om nytt transatlantiskt ramverk: Trans-Atlantic Data Privacy Framework
- Europeiska dataskyddsstyrelsens (EDPB) uttalande 01/2022
- Amerikansk *executive order* om förstärkta skyddsåtgärder
- Utkast till nytt beslut om adekvat skyddsnivå för USA från EU-kommissionen

Ett adekvansbeslut för USA kommer troligtvis att fattas till sommaren 2023. Efter det kommer adekvansbeslutet och överenskommelsen med stor sannolikhet att prövas i EU-domstolen på samma sätt som Safe Harbour och Privacy Shield prövades. Det är därför ännu okänt om adekvansbeslutet kommer att vara tillfälligt eller bestående. Även om adekvansbeslutet inte fälls i EU-domstolen rekommenderar den Europeiska dataskyddsstyrelsen (EDPB) att EU-kommission utvärderar adekvansbeslutet efter 1 år, och därefter var 3:e år. Med anledning av detta bör Region Skåne även fortsatt iaktta försiktighet vid tredjelandsöverföring till USA.

4.1.2 Integritetsskyddsmyndigheten (IMY)

År 2022 inledde 22 nationella dataskyddsmyndigheter i Europa en undersökning om användningen av molnbaserade tjänster inom offentlig sektor. IMY publicerade de övergripande slutsatserna från Sverige i en rapport. Särskilda utmaningar som lyftes är vissa molntjänstleverantörers

bristande kunskaper om grundläggande dataskyddsregler samt avtalsvillkor som inte alltid är transparenta och ofta uppdateras ensidigt. Molntjänster överför dessutom ofta personuppgifter till länder utanför EU, vilket ger myndigheterna juridiska utmaningar.

IMY erbjuder nu fördjupad vägledning om dataskyddsfrågor i relation till innovation i syfte att bidra till att göra den snabba digitaliseringen i samhället hållbar. Med hållbar digitalisering avses offensiv datadriven innovation i kombination med ett starkt integritets- och dataskydd.

Rapporten *Digital integritet 2022* om den svenska befolkningen och personlig integritet i digital miljö publicerades i november 2022. Undersökningen visar att trots att många oroar sig för integritetsrisker, både för cyberangrepp och ny teknik, skyddar bara var femte svensk sina personuppgifter. IMY konstaterar att för att den offentliga sektorn ska kunna fortsätta att hantera svenskarnas persondata är det viktigt att undersöka befolkningens känsla av trygghet och otrygghet i förhållande till olika verksamheter. IMY lämnar i rapporten en rad rekommendationer för att främja det fortsatta arbetet med digital integritet.

4.1.3 Civilt försvar – överenskommelse med SKR

Sveriges kommuner och regioner (SKR) och staten har ingått en överenskommelse om hälso- och sjukvårdens arbete med civilt försvar 2022[2]. Insatser som regionerna ska genomföra för att öka sin motståndskraft omfattar bland annat att bedriva ett systematiskt informationssäkerhetsarbete för att stärka förmågan att motstå cyberattacker i de digitala system som är kritiska för att bedriva hälso- och sjukvård, vilket stärker behovet av ett uppdaterat ledningssystem för informationssäkerhet och dataskydd i Region Skåne. Det finns starka beroenden till andra områden som säkerhet, beredskap och kontinuitet. Senast 31 mars 2023 ska Region Skåne lämna en redovisning till Socialstyrelsen där det framgår vilka insatser som genomförts, uppnådda resultat samt hur de medel som har tilldelats inom ramen för överenskommelsen använts.

[2] Civilt försvar, regioner | SKR

4.1.4 Strategier för informationssäkerhet och digitalisering

4.1.4.1 Struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

1 mars 2021 presenterade MSB ett metodstöd för mätning och uppföljning av offentliga aktörers systematiska informationssäkerhetsarbete.[3] Offentliga aktörer erbjöds att skicka in de resultat som metodstödet genererade, något som Region Skåne avstod från. Metodstödet utgör ett värdefullt verktyg som kommer att integreras i det systematiska informationssäkerhetsarbetet för att möjliggöra dels intern uppföljning och mognadsmätning, dels för att kunna jämföra Region Skånes mognadsgrad med andra offentliga aktörer gällande informationssäkerhet. De slutsatser som MSB drar från den data som samlades in av offentliga aktörer under 2021 är att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen i form av mer, och ett effektivare användande av befintliga, resurser.[4]

4.1.4.2 God och nära vård 2022 – överenskommelse med SKR

I enlighet med överenskommelsen mellan SKR och regeringen om God och nära vård[5] har det genomförts en uppföljning av regionernas arbete med informationssäkerhet. SKR har ansvarat för att etablera en gemensam struktur där varje region självständigt genomfört sin egen uppföljning. Regional informationssäkerhet svarade, tillsammans med förvaltningen Digitalisering IT och MT, på uppföljningen för Region Skånes räkning i januari 2022. Då slutredovisningen av denna uppföljning ännu inte är färdigställd av SKR kommer en redovisning och analys av resultatet och vad det innebär för Region Skåne ske under nästkommande verksamhetsår, 2022/2023.

4.1.4.3 Ett uppdaterat NIS-direktiv

NIS-direktivet är ett EU-direktiv i Sverige infört som lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Lagen omfattar leverantörer av samhällsviktiga och vissa digitala tjänster och innebär krav på systematiskt och riskbaserat arbete med informationssäkerhet och incidentrapportering.

EU-rådet antog 28 november 2022 ett nytt direktiv för att påskynda åtgärder och höja EU-medlemsstaternas skyddsnivå när det gäller samhällskritisk

[3] En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen
[4] Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen (msb.se)
[5] God och nära vård 2022

infrastruktur, vilket innebär att informationssäkerheten för samhällsviktiga tjänster ska förbättras. Det nya NIS-direktivet (NIS2) ska implementeras i svensk lag och ersätta det nuvarande lagstiftning. Det nya direktivet innebär att fler samhällssektorer omfattas, nya krav på riskhantering och en utökad rapportering. Det blir också striktare tillsynsåtgärder och efterlevnadskrav med ökade rättsmedel och sanktioner. NIS2 syftar också till ett mer effektivt samarbete mellan myndigheter, mekanismer för informationsdelning mellan myndigheter, medlemsstater och entiteter, samt inrättandet av EU-CyCLONe som ska hantera storskaliga cybersäkerhetsincidenter och ett europeiskt sårbarhetsregister.

EU-medlemsländer har 21 månader på sig att införliva NIS2t i nationell lagstiftning, vilket gör 17 oktober 2024 till det sista datumet.

Region Skåne behöver bedöma hur vi omfattas av de nya kraven i NIS2, var organisationen står säkerhets- och styrningsmässigt idag och vilka gap som finns. Sedan behöver organisationen implementera tekniska lösningar och de styrprocesser som krävs för att leva upp till den nya lagstiftningen.

4.2 Interna förändringar

4.2.1 Omorganisation av regional informationssäkerhetsfunktion

Under 2022 gjordes en omorganisation av den regionala informationssäkerhetsfunktionen och en sammanslagning av de regionala funktionerna skedde. Organisatoriskt tillhör nu båda funktionerna tillsammans med Informationsoffentlighet, Informationsstyrning och Informationsförvaltning, Koncernstab kansli. Att samla de regionala resurserna inom informationshanteringens olika aspekteter ger en effektivare och samlad kraft för att framöver stärka Region Skåne. Enheten kommer att samordna de olika uppdragen under året.

Specialistkompetensen som krävs för arbetet med informationssäkerhet och dataskydd är eftertraktad på arbetsmarknaden vilket gör att Region Skåne behöver verka för att säkerställa kompetensförsörjningen.

4.2.2 Årshjul för informationssäkerhet och dataskydd

Inför den aktuella granskningsperioden togs ett årshjul för informationssäkerhet fram och implementerades, vilket kompletterade det

befintliga årshjulet för dataskydd. Årshjulen stödjer förvaltningarna i det systematiska arbetet med informationssäkerhet och dataskydd, underlättar mätningen av det arbete som genomförts i organisationen och mynnar ut i årsrapporter på förvaltningsnivå. Dessa sammanställs och analyseras sedan av regionala informationssäkerhets- och dataskyddsfunktioner och redovisas i denna rapport i avsnitt 5.2.

4.2.3 Förbättringsåtgärder kopplade till patientsäkerhet

Föregående årsrapport tog upp införandet av förbättrande åtgärder avseende patienter med skyddade personuppgifter. Arbetet med detta har fortgått under nuvarande verksamhetsår och de nya styrande dokument och processer som har arbetats fram testas för närvarande i en förvaltning för att kunna utvärderas och vid behov justeras och/eller kompletteras.

5 Ledningssystemets, informationssäkerhetens och dataskyddets prestanda

5.1 Avvikelser, incidenter och korrigerande åtgärder

Personuppgiftsincidenter hanteras systematiskt och strukturerat i Region Skåne. En ny metod för bedömning av personuppgiftsincidenter har tagits fram under verksamhetsåret, vilket har underlättat för verksamheterna vid bedömningen av hur allvarliga incidenterna är. Hanteringen av informationssäkerhetsincidenter som inte rör personuppgifter är i behov av utveckling, varför redovisningen nedan endast inbegriper personuppgiftsincidenter.

Under perioden 2021-10-01–2022-09-30 registrerades 563 personuppgiftsincidenter i Region Skånes ärendehanteringssystem för incidenter. Majoriteten av incidenterna avsåg konfidentialitetsbrott, exempelvis genom att en medarbetare begått dataintrång eller att information inte skyddats på rätt sätt vid överföring eller lagring. 112 av incidenterna bedömdes utgöra en risk för enskilda, varför de anmäldes till IMY. 53 av incidenterna bedömdes utgöra en hög risk för enskilda, varför de drabbade informerades om dem. Detta är en minskning i förhållande till

föregående mätperiod. Registrerade incidenter var då 730 och andelen som anmäldes till IMY var 67.

5.2 Resultat från uppföljning och analys

De förvaltningsspecifika årsrapporter som tas fram under arbetet med årshjulen är viktiga verktyg för uppföljning av Region Skånes systematiska informationssäkerhets- och dataskyddsarbete.

Vid analys av det som sammantaget framkommer från förvaltningarnas årsrapporter tydliggörs utmaningar inom organisationen kopplat till befintliga arbetsprocesser och resurssättning.
Flera förvaltningar uttrycker behov av stöd från centrala resurser för att kunna utveckla och utföra ett fullgott arbete inom de processer som informationssäkerhets- och dataskyddsarbetet kräver. För att nå en tillräcklig mognadsgrad behöver kompetensförsörjning säkerställas på såväl förvaltningarna som inom den centrala funktionen. Detta tillsammans med möjliggörande faktorer i form av exempelvis effektiva arbetsprocesser och adekvat resurssättning utifrån den tidsåtgång som krävs för att utföra uppdraget.

5.2.1.1 Utveckling av ledningssystem

Utvecklingen av regionens ledningssystem för informationssäkerhet och dataskydd är central för att öka mognadsgraden för regionens informationssäkerhets- och dataskyddsarbete. En utveckling av ledningssystemet syftar bland annat till att förtydliga styrningen och ledningen av arbetet med informationssäkerhet och dataskydd och att tydligare definiera processer samt roller och ansvar.

5.2.1.2 Process och metodstöd

Många av de svårigheter som uppgetts kopplat till process och metodstöd kommer sannolikt kunna, åtminstone delvis, åtgärdas genom Region Skånes införande av ett stödsystem för informationsklassificering och riskhantering. Detta kommer möjliggöra och förenkla ett utvecklande av relevanta processer inom informationssäkerhet och dataskydd, samt möjliggöra en tydligare spårbarhet och utökade möjligheter till uppföljning.

Tekniska lösningar kopplade till kommunikationssäkerhet är under utveckling eller nyligen tagna i drift, till exempel säker lagring, vilka

sannolikt kan öka mognadsgraden för såväl informationssäkerhets- som dataskyddsarbetet.

6 Förbättringsåtgärder för ledningssystemet

6.1 Riskbedömning

De regionala funktionerna för informationssäkerhet och dataskydd har identifierat risker kopplade till följande av Region Skånes mål:

- Bättre liv och hälsa för fler
- Tillgänglighet och kvalitet
- Hållbar utveckling i hela Skåne
- Attraktiv arbetsgivare, professionell verksamhet
- En långsiktigt stark ekonomi

Det finns risker som är identifierade och därtill föreslagna åtgärder för att undvika eller minska risker. Åtgärderna presenteras också i följande delar av avsnitt 6 tillsammans med övriga rekommenderade åtgärder för att förbättra Region Skånes ledningssystem för informationssäkerhet och dataskydd.

6.2 Vidareutveckling av ledningssystemet

Region Skånes nuvarande ledningssystem för informationssäkerhet fungerar *inte tillfredsställande* utifrån rådande interna och externa behov samt identifierade risker. Region Skåne behöver vidta åtgärder för att säkerställa att organisationen har ett ändamålsenligt, verksamt och effektivt ledningssystem för informationssäkerhet och dataskydd (LISD) för att kunna digitalisera hållbart i önskad takt i enlighet med EU:s, Sveriges och Region Skånes strategier för digitalisering och datadelning.

6.3 Ledningssystemets beroenden till andra områden

Ledningssystemet för informationssäkerhet och dataskydd har ett starkt beroende till andra säkerhetsområden inom Region Skåne, till exempel säkerhet och beredskap, säkerhetsskydd och IT-säkerhet. En samlad

styrning av berörda säkerhetsområde behövs för att säkerställa samstämmiga metoder och rapportering.

6.4 Kompetens och resurser

För att informations- och dataskyddsarbetet ska nå en högre mognadsgrad behöver kunskapsnivån i organisationen höjas ytterligare.

Vidare behöver informationsägarnas roll och ansvar i ledningssystemet stärkas genom att dessa tar en mer aktiv roll som kravställare och ägare av sina viktiga informationstillgångar, som hälso- och sjukvårdsinformation. Ett mer aktivt informationsägarskap där informationen proaktivt kartläggs och kravställs skapar bättre förutsättningar för digitalisering och datadelning, eftersom kraven då utan dröjsmål kan omhändertas i nya initiativ.

6.5 Åtgärder kopplade till övriga riskområden

6.5.1 MT-produkter

Region Skåne planerar att storskaligt införa tjänster för så kallad ”nära vård”. Detta innebär möjligheter till nya digitala arbetssätt för att erbjuda god vård till medborgare i regionen. För att kunna genomföra omställning på ett säkert sätt, för såväl verksamhet som för den enskilde, krävs en parallell satsning på informationssäkerhet och dataskydd. Risken är annars att Region Skånes IT-miljö öppnar upp för hot genom inbyggda sårbarheter i uppkopplade enheter, i synnerhet medicintekniska produkter (MT).

6.5.2 Framtidens hälsosystem och vårdens omställning

Eftersom digitaliseringen ses som en viktig förutsättning och möjliggörare för att Region Skåne ska kunna ställa om till ett mer personcentrerat arbetssätt och proaktiva hälsofrämjande och förebyggande insatser så behöver informationssäkerhet och dataskydd vara naturliga delar av denna digitalisering. Digitaliseringen måste ske på ett hållbart sätt, vilket IMY definierar som en offensiv datadriven innovation tillsammans med starkt integritets- och dataskydd.