Fördelning av ansvar för informationssäkerhet

Beslutad 2018-06-01, av: Regionstabschef

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning/bakgrund

Informationssäkerhetsarbetet har sin utgångspunkt i gällande lagstiftning. Regionens policy för informationssäkerhet och dataskydd (RS/937/2018) anger vad som ska uppnås med informationssäkerhetsarbetet. d.v.s. att uppnå nivå av sekretesskydd, riktighet, tillgänglighet och spårbarhet för information. Arbetet ska så långt som möjligt ske i enlighet med svensk standard för informationssäkerhet SS-ISO 27001:2014.

I begreppet informationssäkerhet avses i de här bestämmelserna även dataskydd samt personuppgiftsbehandling, således omfattar fördelningen av ansvar även dessa områden. Det finns ett separat dokument om organisation för personuppgiftsbehandling enligt Dataskyddsförordningen (RS/1511/2017) där roller och ansvar för personuppgiftsbehandling beskrivs.

Dokumentet beskriver fördelning av ansvar från Regionfullmäktige ner till den enskilde medarbetaren. Det innehåller också en beskrivning av specialist- samt stödjande funktioner för informationssäkerhetsarbetet. Rollerna dataskyddsombud (DSO), biträdande DSO samt registerkoordinatorer (RK), systemägare, registerägare (RÄ) samt informationsägare förtydligas.

Fördelning av ansvar för informationssäkerhet
2018-06-01, Dnr RS/664/2018

Handläggare
Anna-Lena Alfreds
Enheten för krisberedskap, säkerhet och miljö

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

INNEHÅLLSFÖRTECKNING

SAMMANFATTNING/BAKGRUND 1

1 INLEDNING 3

2 ANSVAR FÖR INFORMATIONSSÄKERHET 3

2.1 Regionfullmäktige 3

2.2 Regionstyrelsen och nämnderna 3

2.3 Regiondirektören 4

2.4 Hälso- och sjukvårdsdirektör, Regional utvecklingsdirektör och Regionstabschefens ansvar 4

2.5 Avdelningschefers och områdeschefers ansvar 4

2.6 Enhetschefers ansvar 5

2.7 Medarbetares ansvar 5

3 ÖVRIGA ANSVARSROLLER 6

3.1 Systemägare 6

3.1.1 Registerägare 6

3.2 Informationsägare 6

3.3 Kvalitetsstrateg 6

3.4 Dataskyddsombud (DSO) 6

3.4.1 Biträdande dataskyddsombud 7

3.5 Registerkoordinatorer (RK) 8

4 ÖVRIGA STÖDJANDE FUNKTIONER MED SPECIALISTKOMPETENS INOM INFORMATIONSSÄKERHET 8

4.1 Informationssäkerhetssamordnare 8

4.2 IT säkerhetsansvarig 9

4.3 Informationssäkerhetsråd 9

4.4 Arbetsgrupp informationssäkerhet 10

5 BEKRÄFTELSE AV MOTTAGANDE 11

1 Inledning

Informationssäkerhetsarbetet har sin utgångspunkt i gällande lagstiftning. Regionens policy för informationssäkerhet och dataskydd (RS/937/2018) anger vad som ska uppnås med informationssäkerhetsarbetet. d.v.s. att uppnå nivå av sekretesskydd, riktighet, tillgänglighet och spårbarhet för information. Arbetet ska så långt som möjligt ske i enlighet med svensk standard för informationssäkerhet SS-ISO 27001:2014.

I begreppet informationssäkerhet avses i de här bestämmelserna även dataskydd samt personuppgiftsbehandling, således omfattar fördelningen av ansvar även dessa områden. Det finns ett separat dokument om organisation för personuppgiftsbehandling enligt Dataskyddsförordningen (RS/1511/2017) där roller och ansvar för personuppgiftsbehandling beskrivs. Rollerna Dataskyddsombud (DSO), biträdande DSO samt Registerkoordinatorer (RK) förtydligas ytterligare i detta dokument.

2 Ansvar för informationssäkerhet

2.1 Regionfullmäktige

Fastställer informationssäkerhets- och dataskyddspolicy.

2.2 Regionstyrelsen och nämnderna

Regionstyrelsen har det övergripande ansvaret för informationssäkerheten inom Region Jämtland Härjedalen. Regionstyrelsens ansvar innefattar hantering av alla övergripande informationssäkerhetsfrågor

Regionstyrelsen och nämnderna i Region Jämtland Härjedalen ska var och en inom sitt område se till att det finns en organisation för informationssäkerhet och att arbetet med informationssäkerhet och personuppgiftsbehandling sker på ett ändamålsenligt sätt och i enlighet med fastställd informationssäkerhets- och dataskyddspolicy.

Regionstyrelsen och nämnderna är också personuppgiftsansvariga för alla personuppgiftsbehandlingar inom sina respektive verksamhetsområden. I det ansvaret ingår att säkerställa att det finns en organisation för personuppgiftsbehandling vilket innebär att det ska finnas ett dataskyddsombud (DSO).

Hälso- och sjukvårdsnämnden är ansvarig vårdgivare. Vårdgivaren ska utse en eller flera personer som ska leda och samordna informationssäkerhetsarbetet. Den, de som utses ska minst en gång om året sammanställa information om arbetet till vårdgivaren.

Ansvaret för arbetet med informationssäkerhet och dataskydd samt personuppgiftshantering följer sedan verksamhetsansvaret inom alla nivåer.

2.3 Regiondirektören

Regiondirektören ska arbeta för att Region Jämtland Härjedalens organisation för informationssäkerhet och personuppgiftsbehandling sker på ett ändamålsenligt sätt genom fastställda regler och riktlinjer.

I detta ingår ansvar för att:

- regionens ledningssystem uppfyller kraven för ISO 27001:2006
- informationssäkerhetsfrågor behandlas strategiskt, genom att tillsammans med ledningsgruppen årligen genomföra ledningens genomgång där uppnådda resultat följs upp, analyseras och utvärderas
- beslut tas vid ledningens genomgång för att säkerställa ständiga förbättringar
- resurser avsätts för samordningen av informationssäkerhetsarbetet
- fastställa regler och riktlinjer för informationssäkerheten
- årlig plan för informationssäkerhetsarbete upprättas
- årlig rapportering sker till styrelsen om informationssäkerhetsarbetet.

2.4 Hälso- och sjukvårdsdirektör, Regional utvecklingsdirektör och Regionstabschefens ansvar

Har på regiondirektörens uppdrag ansvar för att:

- informationssäkerhetsarbetet inom respektive förvaltningsområde genomförs i enlighet med ledningssystemets regler och rutiner
- gällande lagstiftning efterlevs
- förvaltningsområdets chefer och övriga medarbetare fortlöpande får information och instruktioner som är nödvändiga för informationssäkerhetsarbetet
- regler och rutiner görs kända
- ständiga förbättringar och uppföljningar görs
- utse ett biträdande dataskyddsombud (bitr. DSO) för sitt förvaltningsområde.

2.5 Avdelningschefers och områdeschefers ansvar

Områdeschef/Avdelningschef ansvarar för informationssäkerheten samt att organisera arbetet inom den egna verksamheten. Det omfattar också att vara informationsägare för den information som skapas och används inom verksamheten. Ansvaret innefattar att informationen har rätt kvalitét för sitt ändamål, finns tillgänglig när den behövs och att sekretesskänslig information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas på ett säkert sätt.

Områdeschef/avdelningschef ansvarar för att:

- informationsklassning/riskanalys genomförs för information som hanteras i gemensamma IT- system eller när nya IT system/tjänster ska införas
- i samverkan med andra områden vara kravställare mot berörda systemägare/registerägare så att systemen/registren uppfyller informationssäkerhets- och dataskyddskraven.
- kontinuitetsplaner för informationssäkerhet upprättas och kommuniceras

- underställda chefer och medarbetare får nödvändig information och utbildning i informationssäkerhet
- utse en registerkoordinator (RK) för sitt område/avdelning.

För verksamheter inom hälso- och sjukvården ska en utsedd verksamhetschef finnas enligt Hälso- och sjukvårdslagen. Gällande fördelning av ansvar för informationssäkerhet likställs områdeschefens ansvar med verksamhetschefens.

För verksamhetschef tillkommer också ansvar för att:

- utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella arbetsuppgifter,
- hälso- och sjukvårdspersonalen och andra befattningshavare är informerade om de bestämmelser som gäller för hantering av patientuppgifter, och
- uppföljning av informationssystemens användning sker genom regelbunden kontroll av åtkomst till uppgifter s.k. loggkontroll.

2.6 Enhetschefers ansvar

Enhetschefen ansvarar för att:

- arbetet utförs utifrån områdets/avdelningens organisation för informationssäkerhet
- tillse att regionens regler och rutiner är kända och efterlevs
- tillse att kontinuitetsplaner finns och är kända
- ta emot, bedöma, utreda och rapportera negativa händelser, tillbud, risker
- medarbetarna får den information och utbildning som krävs avseende informationssäkerhet.

2.7 Medarbetares ansvar

Varje medarbetare har ett ansvar att i det dagliga arbetet följa aktuell lagstiftning och regionens informationssäkerhetsregler för anställda. Ansvaret omfattar t ex att

- ansvara för att personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för obehöriga,
- ansvara för att datorer eller andra informationsbärare som har använts inte lämnas utan att patientuppgifterna, sekretessklassade uppgifter eller annan känslig information är skyddade från obehörig åtkomst
- endast ta del av den patientinformation/övrig sekretessklassad och känslig information som behövs för att utföra sitt arbete.

Alla anställda har också skyldighet att i regionens avvikelsehanteringssystem rapportera avvikelser, incidenter och risker kopplade till informationssäkerhet.

3 Övriga ansvarsroller

3.1 Systemägare

I Region Jämtland Härjedalens systemförvaltningsmodell ska varje IT system ha en systemägare. Systemägaren har ansvar för respektive IT-systems säkerhet och ansvarar även för framtagande av kontinuitetsplaner för systemet. För system som hanterar personuppgifter är systemägaren tillika registerägare och därmed ansvarig för att personuppgiftsbehandlingar anmäls till DSO samt att behandlingen/systemet registreras i regionens registerförteckning. I regionens ”kvalitetshandbok för systemförvaltning” beskrivs systemägarens ansvar.

3.1.1 Registerägare

För personuppgiftshantering är registerägare den som äger system/utrustning/tjänst där personuppgifter behandlas. Registerägaren är ansvarig för att personuppgiftsbehandlingar anmäls till DSO samt att behandlingen/systemet registreras i regionens registerförteckning Registerägaren ansvarar också för att ta fram regelverk för hur uppgifter i systemet/utrustningen/tjänsten får hanteras (på uppdrag av informationsägarna) men har inget ansvar att följa upp efterlevnad av regelverket. Ansvaret att följa regelverket och följa upp att detta görs vilar på informationsägarna.

3.2 Informationsägare

Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvaret, som följer verksamhetsansvaret, innefattar att informationen har rätt kvalitét för sitt ändamål, finns tillgänglig när den behövs och att sekretesskänslig information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas på ett säkert sätt. I Region Jämtland Härjedalen är områdes/avdelningschefer utpekade informationsägare för sina områden.

För personuppgiftsbehandling är informationsägaren den som äger ändamålet med personuppgiftsbehandlingen. Informationsägaren ansvarar för att personuppgifterna hanteras enligt gällande regelverk för personuppgiftsbehandling/dataskydd (t ex att gallring görs)

3.3 Kvalitetsstrateg

Kvalitetsstrateg ansvarar för den övergripande handläggningen av regionens ledningssystem där regler och rutiner m.m. för informationssäkerhet ingår.

3.4 Dataskyddsombud (DSO)

Region Jämtland Härjedalens dataskyddsombud är en självständig och oberoende stöd- och kontrollfunktion. Dataskyddsombudet samt biträdande DSO har en operativ roll och för

uppdraget krävs relevanta resurser. Det är inte dataskyddsombudet som ansvarar för att reglerna följs, utan organisationen.

I arbetsuppgifterna ingår bland annat att:

- informera, ge råd och stöd till personuppgiftsansvarig, handläggare och övrig personal
- vara tillgänglig för frågor från registrerade personer
- rapportera till högsta förvaltningsnivå om organisationens brister och utvecklingsbehov gällande att uppnå en korrekt och laglig personuppgiftsbehandling
- fungera som kontaktpunkt för tillsynsmyndigheten för dataskydd och vid behov genomföra förhandssamråd
- göra anmälan till tillsynsmyndigheten om brister inte åtgärdas
- föra en sammanställning (registerförteckning) över behandlingar av personuppgifter utifrån inlämnade register från respektive personuppgiftsansvarig
- övervaka regionens efterlevnad av dataskyddsförordningen och bevaka att registrerades rättigheter efterlevs
- bistå i utredning av misstänkta överträdelser och personuppgiftsincidenter och bedöma om inträffade incidenter ska anmälas till tillsynsmyndigheten
- bedöma handläggning för inkomna ärenden avseende t ex registerutdrag, klagomålshantering
- bistå registerägare och informationsägare med att identifiera rätt skyddsåtgärder för personuppgifter baserat på informationsklassning
- tillsammans med sakkunniga inom regionen kravställa och arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen
- tillsammans med sakkunniga ge råd vid genomförande av konsekvensbedömning för dataskydd och övervaka genomförandet av åtgärder som baseras på denna bedömning
- samverka med biträdande DSO för varje förvaltningsområde i dataskyddsfrågor
- tillhandahålla och bevaka en funktionsbrevlåda (dataskydd@regionjh.se) dit frågeställningar kan skickas både av interna och externa intressenter.

Dataskyddsombudets organisatoriska tillhörighet ska vara inom Regionstaben, Samordningskansliet.

3.4.1 Biträdande dataskyddsombud

I Region Jämtland Härjedalen ska förutom DSO finnas ett biträdande DSO för varje förvaltningområde. Biträdande DSO ska samordna dataskyddsarbetet inom det egna förvaltningsområdet samt stödja DSO med följande uppgifter:

- informera, ge råd och stöd till personuppgiftsansvarig, handläggare och övrig personal

- vara tillgänglig för frågor från registrerade personer (inkluderar att bistå med bevakning av Regionens funktionsbrevlåda för dataskyddsfrågor)
- sammanställa behandlingar av personuppgifter i central registerförteckning utifrån inlämnade register inom sitt förvaltningsområde (i dialog med registerkoordinatorer)
- övervaka efterlevnad av dataskyddsförordningen
- bistå i utredning av misstänkta överträdelser och personuppgiftsincidenter
- bistå vid genomförande av konsekvensbedömning för dataskydd
- bistå vid handläggning för inkomna ärenden avseende t ex registerutdrag, klagomålshantering
- delta i forum som syftar till kunskapsutbyte för och styrning av regionens dataskydd tillsammans med biträdande DSO för övriga förvaltningsområden samt regionens centrala DSO
- kunna ersätta DSO vid dennes frånvaro.

3.5 Registerkoordinatorer (RK)

Inom varje område/avdelning ska finnas en utsedd Registerkoordinator (RK). RK:s ansvar är att:

- registrera områdets/avdelningens personuppgiftsbehandlingar i regionens registerförteckning i samverkan med områdets registerägare samt att vid ändringar av eller vid nytillkomna behandlingar hålla registerförteckningen aktuell
- bistå registerägare med att upprätta, bevaka och uppdatera GAP-analyser och åtgärdsplaner för aktuella personuppgiftsbehandlingar
- delta vid genomförande av konsekvensbedömningar för dataskydd
- bistå med handläggning vid begäran om registerutdrag
- bistå med grundläggande stöd och vägledning till sitt område/avdelning i frågor om dataskydd, registrering och behandling av personuppgifter (i samarbete med förvaltningsområdets biträdande DSO).

4 Övriga stödjande funktioner med specialistkompetens inom informationssäkerhet

4.1 Informationssäkerhetssamordnare

I regionen ska det finnas en utsedd informationssäkerhetssamordnare som på uppdrag av regiondirektören ansvarar för att:

- samordna regionens strategiska informationssäkerhetsarbete i enlighet med regionens policy för informationssäkerhet och dataskydd.
- utarbeta årlig plan för aktiviteter inom informationssäkerhetsarbetet.
- utarbeta årlig informationssäkerhetsrapport till vårdgivaren avseende riskanalyser, incidenter, uppföljningar samt förbättringsåtgärder.

- ta initiativ till arbete med att arbeta fram policy, regler och rutiner inom området
- ta initiativ till att utbildning tas fram och genomförs inom organisationen
- ta initiativ till och genomföra säkerhetsrevisioner
- bevaka och sammanställa informationssäkerhetsincidenter
- följa upp att föreskrifter för informationssäkerhet efterlevs
- omvärldsbevaka informationssäkerhetsområdet
- bistå informationsägare med stöd att genomföra informationsklassningar och riskanalyser inom informationssäkerhetsområdet
- i samverkan med IT säkerhetsansvarig samordna informationssäkerhetsarbetet gentemot regionens systemägare för att få enhetlig utformning och nivå på de olika verksamhetssystemens säkerhetsåtgärder/-funktioner
- bistå DSO samt verksamhet med kompetens inom dataskydd t ex att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen, bistå registerägare och informationsägare med att identifiera rätt skyddsåtgärder för personuppgifter baserat på informationsklassning samt ge råd vid genomförande av konsekvensbedömning för dataskydd.
- vara sammankallande i informationssäkerhetsrådet.

4.2 IT säkerhetsansvarig

IT- säkerhetsansvarig har till uppgift att införa förebyggande skyddsåtgärder för att undvika IT-säkerhetsincidenter som hotar verksamhetens informationshantering.
I uppgifterna ingår att:

- löpande initiera och genomföra säkerhetshöjande förbättringsåtgärder för IT-infrastrukturen, baserat på kraven för regionens verksamhetssystem
- handlägga auktorisationer av nya och uppgraderade IT-system för godkännande innan de anskaffas och införs i IT-miljön
- genomföra risk- och sårbarhetsanalyser av specifika delar i IT-miljön utifrån bl. a. ställda verksamhetskrav på informationssäkerhet
- löpande analysera och följa upp rapporterade IT-säkerhetsincidenter och utifrån dessa initiera säkerhetshöjande åtgärder
- vara konsultativ resurs för verksamheter som har behov av att utforma säkerhetshöjande åtgärder i IT-system
- agera kravställare säkerhet och säkerhetsrevisor på extern IT-driftleverantör som innehar avtal för regionens IT-drift
- samordna IT-säkerhetsarbetet gentemot regionens systemägare för att få enhetlig utformning och nivå på de olika verksamhetssystemens säkerhetsåtgärder/-funktioner
- bistå DSO med kompetens inom dataskydd t ex att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen

4.3 Informationssäkerhetsråd

I Regionstaben ska finnas ett informationssäkerhetsråd för regionens informationssäkerhetsarbete. Informationssäkerhetsrådet ska bidra till ett processorienterat

arbetssätt avseende säkerhetsfrågor inom området informations- och IT säkerhet. Rådet ska ha företrädare med kompetens och funktionsansvar inom:

- juridik
- personuppgiftsbehandling och dataskydd
- riskhantering
- patientsäkerhet
- IT-säkerhet
- informationssäkerhet
- vårdadministrativt system, COSMIC
- nationella ehälsotjänster/Journal via nätet

Andra företrädare för t ex arkiv, diarium, dokumenthantering, systemansvariga, kvalitetsutveckling kan adjungeras efter behov.

Informationssäkerhetsrådet är sakkunnigstöd och rådgivande inom området. Rådet ska bistå med att identifiera behov av och initiera arbete för säkerhetshöjande åtgärder. Beredskapschef är ordförande och informationssäkerhetssamordnaren är sammankallande samt sekreterare. Rådet träffas ca 4 gånger/år och genomförda möten ska dokumenteras i form av minnesanteckningar i Centuri.

4.4 Arbetsgrupp informationssäkerhet

Utöver informationssäkerhetsrådet finns en arbetsgrupp som leds av informationssäkerhetssamordnaren. Gruppens uppdrag är att:

- hålla övergripande regler för informationssäkerhet aktuella samt ta fram förslag till nya
- utifrån fastställda regler, utarbeta övergripande rutiner som ska finnas tillgängliga i ledningssystemet
- systematiskt arbeta för ständiga förbättringar bl.a. genom riskanalyser och granskningar inom området
- initiera och bistå informationssäkerhetssamordnaren med säkerhetsrevisioner
- initiera och föreslå säkerhetshöjande åtgärder utifrån genomförda riskbedömningar och kontroller
- fungera konsultativt som stöd och remissinstans för regionens verksamheter i informationssäkerhetsfrågor
- vara stödjande och rådgivande till DSO samt verksamheten gällande dataskyddsfrågor t ex avseende att kravställa, identifiera och ge förslag till säkerhetsåtgärder.

5 Bekräftelse av mottagande

Undertecknad bekräftar härmed mottagandet av denna fördelning av ansvar för informationssäkerhet

Ort och datum: _____

Namnunderskrift

Befattning

Namnförtydligande