Informationssäkerhet och dataskydd

FÖRTROENDEMANNAUTBILDNING 2022

LARS CHRISTERSON
INFORMATIONSSÄKERHETSSAMORDNARE

REGION JÄMTLAND HÄRJEDALEN

Agenda

- **Dataskydd (GDPR):** Styrelsen/nämndernas ansvar som personuppgiftsansvarig enligt delegationsordning och regelverket för personuppgifter (PU)

- **Informationssäkerhet:** Varför är informationssäkerhet viktigt för regionen, ledningssystem för informationssäkerhet (LIS) och NIS-direktivet

REGION JÄMTLAND HÄRJEDALEN

Varför behöver vi skydda våra personuppgifter?

- EU-direktiv om medborgarnas fri- och rättigheter – GDPR (dataskyddsförordningen, med kompletterande svensk dataskyddslag)
- Vi lånar bara våra medborgares och medarbetares personuppgifter och behöver då vara försiktiga med hur de används – inte kränka integritet
- *Alla* verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter. Det gäller oavsett om det är en offentlig myndighet, ett privat företag, en förening eller någon annan typ av verksamhet.

Informationssäkerhet

Dataskydd

PU= Personuppgifter

Regionstyrelsen är personuppgiftsansvariga

- Regionstyrelsen är personuppgiftsansvarig - enligt delegationsordning och PU-regelverket med ansvar och roller.
- Ansvarar för att det finns ett PU-ombud och vad ombudet har för roll/ansvar/ mandat.
- Delegerar till Regiondirektör att följa upp och rapportera om dataskyddsarbetet.

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

Dataskydd - personuppgifter - Insidan (regionjh.se)

Fördelning av ansvar informationssäkerhet: https://diariet.regionjh.se/diariet/files/ef01d9eb-00b3-4858-802d-0abe5b47f30b.pdf

Ansvarsfördelning personuppgiftsbehandling: https://centuri/regno/54207

REGION JÄMTLAND HÄRJEDALEN

Krav på hantering av PU (personuppgifter)

- Vi behöver följa de grundläggande principerna i GDPR - se till att PU-behandlingen har en **rättslig grund**, att de registrerades **rättigheter kan tillgodoses** inklusive att **informera** dem om hur vi hanterar deras personuppgifter.
- Den som är personuppgiftsansvarig:

Laglighet, korrekthet och öppenhet	måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter ska kunna visa att man kan leva upp till dataskyddsförordningen och hur detta görs
Ändamålsbegränsning	får bara samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
Uppgiftsminimering	får inte behandla fler personuppgifter än vad som behövs för ändamålen
Riktighet	ska se till att personuppgifterna är riktiga
Lagringsminimering	ska radera personuppgifterna när de inte längre behövs
Integritet och konfidentialitet	ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
Ansvarsskyldighet	ska kunna visa att man uppfyller principerna i GDPR – ”omvänd bevisbörda” (innebär att varken den registrerade eller tillsynsmyndigheten behöver kunna visa att den personuppgiftsansvarige bryter mot principerna)

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Exempel: krav på konsekvensbedömning

- Om en personuppgiftsbehandling innebär en *särskild risk för integriteten hos den registrerade* måste den personuppgiftsansvarige göra en *konsekvensbedömning* innan denna behandling får påbörjas.
- Saknas en sådan dokumenterad bedömning kan viten dömas ut av tillsynsmyndigheten.

GDPR: höga viten vid överträdelser

Flera regioner har 2020-21 tilldömts höga viten (2-3 MSEK) för överträdelser av dataskyddsslagarna.

Exempel på överträdelser:

- E-postat känsliga personuppgifter via oskyddad e-post
- Ej gjort behovsbedömning innan tilldelning av behörigheter till patientuppgifter i journalsystem

Region Västerbotten dec 2020:

Tillsynsmyndighet är IMY (Integritetsskyddsmyndigheten)

Informationssäkerhet – varför behöver vi jobba med det?

- För att regionens verksamheter ska kunna utföra sitt uppdrag i form av kvalitativa samhällsviktiga verksamheter krävs tillgång till rätt information i rätt tid.
- Därför är det viktigt att informationen kartläggs, värderas och kan skyddas. Kunskap om vilken information som är mest verksamhetskritisk, och som behöver prioriteras, bli viktig för att säkra att verksamhetsuppdraget kan utföras.

Detta görs inom det systematiska arbetet med informationssäkerhet.

Informationssäkerhet - Ledningssystem - Insidan (regionjh.se)

Informationssäkerhet – en förutsättning för att kunna digitalisera

- Om vi inte vet vilken information vi har och behöver kan vi inte heller digitalisera verksamheterna och uppnå full effekt av detta.

!

Vad händer om vi inte jobbar med informationssäkerhet?

- Risk för **höga viten** för att vi inte uppfyller lagkraven (NIS och GDPR)
- Vi **tappar förtroende** från våra medborgare – om deras information inte hanteras rätt
- Vi drabbas av **kvalitetsbristkostnader** – t ex genom informationsförluster och verksamheter som får stänga/avboka besök mm.
- Vi riskerar att utföra **onödigt dubbelarbete** då samma information registreras flera gånger på olika ställen – slöseri med arbetstid/pengar
- Vi riskerar att fatta **beslut på felaktiga grunder** eftersom vår information som används som underlag är felaktig
- **Dålig arbetsmiljö** orsakad av informationsstress, felaktig information, brister i arbetsflöden

Informationssäkerhetspoli

Beslutad av regionfullmäktige:

- Informationssäkerhetspolicy

(dnr:RS/937/2018, senast uppdaterad nov 2020)

Målområden - principer:

- Säker och riskbaserad informationshantering
- God informationssäkerhetskultur
- Effektiv incidenthantering
- Robust informationshantering
- Informationssäkerhetsberättelse
- Handlingsplan

”Information är en av regionens mest kritiska resurser. Hela verksamheter är beroende av information. Avbrott i tillgången och felaktig information kan orsaka allvarliga konsekvenser i verksamheten eller för enskilda individer.”

Regionstyrelsen ansvarar för att informations-säkerhetspolicy och regler för informationssäkerhet utarbetas och hålls aktuella.

Regionstyrelsen beslutar om regler för informations-säkerhet och följer upp handlingsplan med mätbara mål för informationssäkerhet.

Varje nämnd och styrelse är ansvarig för informations-säkerhet och personuppgiftshanteringen inom sitt verksamhetsområde och ska, inom ramen för regionens ledningssystem anta verksamhetsspecifika styrdokument för informationssäkerhet och personuppgiftshanteringen där så är nödvändigt.

REGION JÄMTLAND HÄRJEDALEN

De största riskerna kommer inifrån

- En väletablerad sanning kring risker i informationshanteringen är att de största och flesta riskerna i vår informationshantering kommer från våra egna medarbetare som agerar felaktigt – omedvetet eller medvetet.
- Detta behöver vi vara medvetna om när vi prioriterar vad som ska göras i säkerhetsarbetet.

Vi behöver hjälpa medarbetarna att kunna göra rätt.

REGION JÄMTLAND HÄRJEDALEN

Ledningen behöver hålla sig informerad – om riskerna

- Regionledningen behöver ha kunskap om vilka de största riskerna mot vår information är. Utifrån detta kan beslut fattas om hur arbetet med att säkra tillgången på vår information ska prioriteras - och vilka resurser som behövs för att uppnå rätt nivå på säkerhetsarbetet.

Efterfråga vilka de fem största riskerna är och hur vi ska kunna minska dem!

REGION JÄMTLAND HÄRJEDALEN

Var börjar säkerhetsarbet

- För att vi ska veta vilken information vi behöver och hur viktig den är i verksamhetens uppdrag behöver vi kartlägga den. Vi kallar detta för ”kartläggning av informationstillgångar”.
- **Vad behöver vi ha tillgång till för information för att arbetet ska kunna utföras på rätt sätt? Vilka konsekvenser uppstår om vi inte kan använda informationen eller om den läcker till obehöriga?** Dessa konsekvenser blir grunden till informationsklassning – en del av kartläggningen.
- Klassningen görs utifrån tre aspekter: hur viktigt det är…

Tillgänglighet	…att informationen är åtkomlig när den behövs, i överenskommen omfattning
Konfidentialitet	… att informationen endast är åtkomlig för berörda/behöriga
Riktighet	… att informationen är aktuell, fullständig, korrekt och begriplig

REGION JÄMTLAND HÄRJEDALEN

Ägarskap för informationen

- För att kunna hantera informationstillgångarna på ett strukturerat sätt kopplas en ägare till varje identifierad informationstillgång. Denna roll kallas **informationsägare**.

- Att vara informationsägare innebär att ansvara för informationstillgången genom att se till att rätt krav ställs på tillgången och att den hanteras på rätt sätt med rätt skydd. Till sin hjälp har ägaren stöd som anger vilka skyddsåtgärder som krävs för en viss klassningsnivå.

- Regionen ska upprätthålla ett centralt register över sina informationstillgångar. Detta krav ställs i standarden för informationssäkerhet ISO 27001.

MSB har det nationella ansvaret för att vägleda inom informationssäkerhet

- Metodstöd för informationssäkerhet finns på https://www.informationssakerhet.se/

NIS-direktivet

- NIS-lagstiftningen kom 2018 och syftar till att uppnå en **hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU**. Det europeiska NIS*-direktivet är svensk lag.

- Omfattar de som levererar samhällsviktiga tjänster, såsom hälso- och sjukvård, däribland regioner och kommuner.

- Tillsynsmyndighet för hälso- och sjukvårdsorganisationer är Inspektionen för vård och omsorg, IVO. **Höga vitesbelopp kan utdömas om systematiskt säkerhetsarbete inte kan redovisas.**

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

REGION JÄMTLAND HÄRJEDALEN

* NIS står för “The Directive on Security of Network and Information Systems”

NIS-direktivet forts

Kraven i NIS:

- Vi behöver vidta säkerhetsåtgärder för att skydda nätverk och informationssystem.
- Vi ska rapportera incidenter (till MSB) som gäller avbrott i de samhällsviktiga tjänsterna – *viktigt att vi vet vilka IT-tjänster som omfattas av NIS-kraven.*

Tillsynsmyndighet ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer lagens bestämmelser.

Det är verksamheten själv som ansvarar för att identifiera sig som en samhällsviktig tjänst under NIS.

Lagen/direktivet gäller från 2018. Gäller organisationer/leverantörer som har 50 eller fler anställda.

Ledningens genomgång

Informationssäkerhetsarbetet redovisas för regionledningen vår och höst. Följande punkter tas upp:

1. Omvärld – risker och trender
2. Resultat från måluppföljning verksamhetsplanering
3. Utvärderingar av interna regler, arbetssätt, åtgärder och stöd
4. Övergripande riskanalys
5. Interna och externa revisioner av informationssäkerheten
6. Allvarliga risker som inte har åtgärdats med förslag till beslut om förbättringsåtgärder
7. Brister avseende tilldelning av ansvar, resurser, mandat och befogenheter för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet

Kommande – från 2023: Uppföljning resultat från internkontrollplan informationssäkerhet

Informationssäkerhet

Dataskydd

Sammanfattning

- Regionstyrelsen har det övergripande ansvaret för dataskydd och informationssäkerhet.
- Styrelsen har ansvar att informera sig om de största riskerna samt i vilken utsträckning som skyddsåtgärder och styrande regelverk finns införda.
- Särskilt fokus bör läggas på att följa upp i vilken grad medarbetarna har genomgått grundutbildning i informationssäkerhet, hur de kan tillämpa regelverket och därmed kan arbeta på ett säkert sätt. Orsak – de största riskerna för informationen kommer inifrån – de egna medarbetarna.

En robust informationshantering bidrar till att skapa tillit, sparar pengar och ger en förbättrad arbetsmiljö. Sammantaget bidrar detta till att verksamhetens mål lättare kan uppnås.

REGION JÄMTLAND HÄRJEDALEN