Universitetet i Sørøst-Norge

Dato: 13.06.2018
Dok.nummer: 18/02520-13

NOTAT

Til: Johnny Thorsen/Avdeling for infrastruktur
Kopi til:

Fra: Ragni Serina Zlotos/ Avdeling for infrastruktur

Retningslinje for ROS informasjonssikkerhet og personvern - oppfølgingsnotat

Ledelsessystem for informasjonssikkerhet – USN

Retningslinje for risiko- og sårbarhetsvurderinger (ROS) av informasjonssikkerhet og personvernkonsekvenser

Type dokument	Retningslinje
Forvaltes av	Infrastrukturdirektør
Godkjent av	Rektor
Klassifisering	Åpen
Gjelder fra	01.06.18
Versjon	1.0
Unntatt offentlighet	-
Referanse interne dokumenter	Gjennomførende dokument etter Policy for informasjonssikkerhet

Innhold

1. Hva er en ROS-vurdering?

En ROS-vurdering blir bestilt fra en leder, risikoeieren[1].

Den blir foretatt av de som er eksperter på prosessen som kan ha eller gi risiko eller sårbarheter. Eksperter kan være mennesker med ulike bakgrunn og perspektiv. Det kan være brukere som administrative brukere, studenter, pasienter, undervisere eller forskere. Det kan være superbrukere, prosjektledere, utviklere, administratorer, med mer.

Produktet er et utfylt skjema som gjenspeiler gruppens vurdering av konsekvens og sannsynlighet av mulige uønskede hendelser og anbefalinger av eventuelle tiltak for å senke sannsynlighet og konsekvens.

Risikoen som er gjenspeilet i dokumentet skal bli vurdert av leder. Ansvaret for å godta, unngå, delegere eller senke konsekvens og sannsynlighet ligger hos lederen som eier risikoen.

2. Hva er informasjonssikkerhet/personvern?

Informasjonssikkerhet

Informasjon er all informasjon som blir bearbeidet i virksomheten. Sikkerheten av informasjonen beror på disse fire pilarer. Risiko og sårbarheter knyttet til informasjonssikkerhet defineres som brudd av disse elementer. Ved ulike informasjonsverdier, systemer og tjenester er det forskjellige behov som veier tyngre enn andre.

Konfidensialitet (K)

Informasjon som er konfidensiell skal kun være tilgjengelig til de som skal ha tilgang til den til enhver tid.

[1] USN Policy for informasjonssikkerhet kapittel 4.2.6 andre ledd jamfør 4.2.8

Integritet (I)
Informasjonen som finnes skal være riktig og forbli uforandret av uvedkommende eller tekniske feil.

Tilgjengelighet (T)
Informasjon skal være tilgjengelig til de som skal ha tilgang ved behov

Robusthet (R)

Informasjon skal være lagret/kommunisert i sikre systemer med sikre metoder, som er egnet til å gjenopprette normaltilstanden etter brud.

Personvern

Hva er en personopplysning?
En personopplysning er informasjon som kan knyttes til en person. Dette gjelder opplysninger som vi tenker på automatisk, slik som navn, adresse, bilskilt, osv. Men også opplysninger som er egnet for å skape atferdsmønstre, som GPS-data eller hva en person handler gjelder som personopplysninger. Datatilsynet har en definisjon av «personopplysning».[2]

Særskilt sensitiv karakter har personopplysninger som omhandler religion, legning, etnisk tilhørighet, tilhørighet til fagforening o.l., på lik linje med det som tidligere ble kalt «sensitive personopplysninger».

Hva er kriteriene for å bedømme personvernkonsekvens?
Hovedfokus er konsekvensene for rettighetene til de registrerte. Vurderingen må ifølge veilederen til Datatilsynet vise:[3]

a) En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.

b) En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.

c) En vurdering av risikoene for de registrertes rettigheter og friheter

d) De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

Det er mulig å bruke skjemaet i vedlegget til vurderingen, da mange av de mulige konsekvensene vil også kunne formuleres som uønskede hendelser og være et brudd på pilarene av informasjonssikkerheten. Likevel er personvernkonsekvensutredningen en særskilt vurdering av hvorvidt personvernforordningen overholdes i forhold til de registrertes rettigheter.

3. Roller og ansvar

Roller og ansvar er beskrevet i policy for informasjonssikkerhet.

I hver ROS bør risikoeieren sørge for at det er en fasilitator. En fasilitator forbereder og samler en gruppe til risikovurdering. Fasilitering av risikovurderingen innebærer å engasjere alle deltakerne til å snakke om uønskede hendelser og årsakene til disse. Fasilitatoren hjelper å komplettere vurderingen og skriver rapporten.

Deltakere i ROS-vurderingen bidrar med sin erfaring og fra sitt ståsted. Det er viktig å velge en viss bredde av roller, men samtidig ikke gjøre gruppen for stor.

En ekstern leverandør til et system kan delta i ROS vurderingen, men kun fra sitt ståsted. ROS vurderingen er ikke en salgsarena. Det er bedre å rette spesifikke spørsmål før og underveis til leverandøren og be om svar.

[2] https://www.datatilsynet.no/om-personvern/personopplysninger/

[3] https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/?id=8322

4. Hva utløser en ROS-vurdering eller revisjon?

En ROS-vurdering skal gi grunnlag for virksomhetsstyring og veivalg. ROS-vurderinger skal gjennomføres systematisk ved oppstart og underveis, se under. En personkonsekvensutredning (DPIA[4]) skal utføres som del av risikovurderingen når (før) behandling av personopplysninger som medfører høy risiko.[5] Risikoen vurderes i DPIA-delen fra de registrertes synspunkt, virksomhetens risiko er her sekundær.

Oppstart

Har en tjeneste eller et system aldri blitt ROS-vurdert, så skal disse vurderes. Ved oppstart av et prosjekt som skal utvikle eller etablere en ny tjeneste, eller før anskaffelse av en ny tjeneste, bør man risikovurdere. Tjenesteutsetting bør alltid risikovurderes. Særskilte eller store uønskede hendelser innen informasjonssikkerhet bør ROS-vurderes som del av institusjonens overordnede ROS, og bør planlegges som del av dette eller innordnes under årsplanen for informasjonssikkerhet.

Alle prosjekter eller eksisterende tjenester skal foreta en vurdering av hvorvidt det er aktuelt å foreta en personvernkonsekvensutredning.

Underveis

IT-systemer og tjenester forandrer seg. Noen av disse spørsmål kan utløse en revisjon av ROS vurderingen, en ny vurdering – eller en vurdering av personvernkonsekvenser.

- Kobles systemer sammen som ikke har vært koblet før?
- Bruker man nye måter å bearbeide dataene på enn før?
- Kobler man sammen datakilder?
- Bytter man leverandør?
- Begynner systemet eller tjenesten å bli overmoden/foreldet?

5. Prosess

Oversikt over IT systemer og tjenester og prioritering av ROS

En oversikt over systemer og tjenester er viktig for å kunne planlegge arbeidet med risikovurderinger. USN har en slik oversikt og oppfordrer til å oppdatere den ved endringer, senest til ledelsens gjennomgang i høst.

Oversikten skal også føre opp tidspunktet til siste ROS vurdering.

Oversikten kan brukes til å prioritere ROS-vurderinger. Kriterier til vurdering til prioritet er:

- Anslått risiko for USNs funksjonsevne og omdømme
- Anslått potensielt økonomisk risiko
- Mengde og omfang av personopplysninger
- Alder og status i livssyklus
- Risikobilde i tidligere ROS og avstand til siste ROS

Selve oversikten eies av informasjonssikkerhetsrådgiver. Risikoeiere må sørge for at informasjonen er tilgjengelig.

Bestilling

Risikoeier bestiller ROS-vurdering. Risikoeier kan bestemme fasilitator, legge føringer for deltakerliste, tidspunkt og frist for rapporten. Risikoeier kan velge å delegere detaljene i bestillingen, men behandlingen av rapport og dokumentasjon kan ikke delegeres.

[4] Data Protection Impact Assessment - *DPIA*

[5] https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/?id=8306

Deltakervalg, inkalling og forberedelse

Det er viktig å velge deltakerne nøye. Vurderingen blir jo bedre jo flere kan delta som spesialister på sitt område.

Forberedelsen består i å ta kontakt med eventuelle leverandører, innhente informasjon om tjenesten eller systemet og lage et lite skriv som kan hjelpe deltakerne å forstå prosessen og rollen deres. En mal stilles til disposisjon. Viktige prinsipper skal forklares.

Innkalling bør skje minst en uke i forkant.

Arbeidsform og fasilitering

I ett eller flere møter mellom fasilitator og deltakerne blir omfanget av ROS vurderingen definert og avgrenset, og mulige uønskede hendelser definert fra erfaring og bekymringer. Mulige årsak blir definert, eksisterende tiltak beskrevet. Det samlede bilde munner i en analyse av konsekvens- og sannsynlighetsnivå. Tallene velges ut fra definisjonene i risikomatrisen. Deretter kan det foreslåes konsekvens- eller sannsynlighetsreduserende tiltak. Disse bør enten av gruppen eller leder fordeles som arbeidsoppgaver med bestemt dato der de skal gjennomføres. Dette skal dokumenteres og følges opp.

Rapportering

Rapporten kan bruke en mal, og fatter sammen diskusjonen om systemet. Anbefalinger utover foreslåtte tiltak kan også dokumenteres her. Rapporten og skjemaet lastes opp i p360 og sendes til risikoeier. Dersom malen ikke brukes bør man kort forklare hvilke tilpasninger man valgte av hvilke grunner.

Overlevering og oppfølging

Risikoeier vurderer risikoen slik den er presentert. Ved ufullstendighet eller usikkerhet kan det stilles spørsmål til gruppen eller leverandør. Deretter håndterer risikoeier risikoen ved å

- Unngå
- Delegere
- Minske ved hjelp av tiltak
- Akseptere

Der mulige avvik vil gå utover risikoeiers budsjett må risikoeier forankre risikohåndteringen med sin leder eller virksomhetsledelsen. En generell pekepinn er at hendelser som etter vurderingen får gule eller røde risikotall skal ikke aksepteres uten at sannsynlighet eller konsekvens senkes med tiltak.
Beslutningen skal veie tiltakene mot risiko etter kost-nytte-prinsipp.

6. Ledelsens gjennomgang

I forkant av ledelsens gjennomgang, som er en fast del av årshjulet ved informasjons-sikkerhetsarbeidet vil enhetene måtte svare for ROS vurderinger som er gjennomført, tiltakene som er iverksatt eller avslått. Der ROS vurderinger skal bidra til virksomhetens læring om informasjonssikkerhet, kulturbygging og internkontroll er det viktig å dokumentere lærdommen for at informasjonssikkerheten kan forbedres kontinuerlig.

7. Vedlegg

Sannsynlighet – og konsekvensmatrise

Skjema for gjennomføring av ROS-vurdering

Mal Forberedelse av ROS—vurdering

Mal rapport

Versjon 1, Mai 2018, Ragni Serina Zlotos

Informasjonssikkerhetsrådgiver