
Risikovurdering av informasjonssystem

med utgangspunkt i forskrift til personopplysningsloven



Datatilsynet

Innholdsfortegnelse

1 Innledning	4
1.1 Risiko og personvern	4
2 Akseptabelt risikonivå.....	6
3 Forberedelse av risikovurdering.....	7
3.1 Planlegging.....	7
3.2 Organisering.....	8
4 Kartlegging.....	9
4.1 Verdier og miljø	9
4.2 Verktøy.....	9
4.3 Kartlegging av personopplysninger	10
5 Identifisere uønskede hendelser	11
5.1 Årsak	12
5.2 Hendelser som berører personvernet.....	12
6 Konsekvens	13
6.1 Konsekvensvurdering.....	13
6.2 Personvernkonsekvens	14
7 Sannsynlighet	15
7.1 Sannsynlighetsvurdering.....	15
7.2 Vurdering ut fra letthetsbetraktning.....	15
7.3 Vurdering med utgangspunkt i motivering	16
7.4 Sannsynlighet og personvern	17
8 Risiko	17
8.1 Beskrivelse av risiko	17
8.2 Personvernrisiko.....	18
9 Anbefalte tiltak.....	19
9.1 Risikohåndtering	19
9.2 Sikkerhetstiltak.....	19
9.3 Sikring av personopplysninger.....	20

Sammendrag

De aller fleste behandlingsansvarlige vil måtte gjennomføre en risikovurdering i forhold til informasjonssikkerhet dersom de skal bli i stand til å bringe behandlingen av personopplysninger i samsvar med personopplysningsloven og forskriften til denne. Dette dokumentet er laget for å gi veiledning i den prosessen.

I forskriftens § 2-1 presiseres det at sikkerhetstiltakene skal stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd. Videre heter det i merknaden til § 2-4 om risikovurdering at arbeidet med å avdekke risiko ikke bør være mer omfattende eller formalisert enn strengt tatt nødvendig.

Uansett vil en risikovurdering inneholde noen grunnleggende elementer, som beskrives nærmere i dette dokumentet.

En forutsetning for å kunne ha en forsvarlig risikostyring er at det finnes noen kriterier å styre i forhold til. Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et på forhånd akseptert nivå. Beskrivelsen av dette nivå blir ofte betegnet som akseptkriterier eller akseptabelt risikonivå.

Risikovurdering er normalt en situasjonsbetinget aktivitet – det vil si at arbeidet igangsettes ved behov og ikke ved faste intervaller. Ideellt sett bør risikovurdering foretas allerede i planleggingsfasen for et informasjonssystem. Bakgrunn for senre igangsetting vil normalt være endringer av betydning for informasjonssikkerheten. Endringene kan være forårsaket av virksomheten selv, eller oppstå uavhengig i forhold til denne.

En forutsetning for å kunne si noe om behovet for sikkerhetstiltak er at det er foretatt en kartlegging av de personopplysninger som behandles. Krav om oversikt over personopplysninger følger ikke utelukkende av bestemmelsen om risikovurdering. Også andre plikter i personvernregelverket gjør det nødvendig med slik oversikt – som avdekking av formål for, og hjemmel til behandling av personopplysninger, plikt til å gi innsyn og informasjon, melde- og konsesjonsplikt. Det er derfor aktuelt å legge kartleggingsarbeidet opp slik at oversikten dekker alle slike formål.

En lang rekke hendelser kan påvirke sikkerheten, og dermed personvernet. Det er nødvendig å identifisere hendelser som faktisk medfører en risiko som krever vurdering av tiltak. Denne utvelgelsen må ta utgangspunkt i det taps- eller skadepotensial som kan anslås, og som er del av en konsekvensvurdering.

I risikobegrepet ligger også en hypotese om sannsynlighet for at en uønsket hendelse skal inntreffe. Dette vil ofte være den vanskeligste vurderingen å foreta. I dette dokumentet nevnes flere tilnæringsmåter som kan bidra til å vurdere sannsynlighet.

En risikovurdering skal være et styringsverktøy for den som har ansvaret for informasjonssikkerhet. Risikovurderingen må resultere i en beskrivelse av risiko som er avdekket og en sammenlikning av dette risikonivå med det som er definert som akseptabelt risikonivå. Restrisiko håndteres ved hjelp av sikkerhetstiltak, enten for å redusere konsekvensene av eller sannsynligheten for uønskede hendelser.

1 Innledning

§13 i Personopplysningsloven (POL) pålegger den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Dette pålegget gjelder alle, uavhengig av hva slags personopplysninger som behandles og uavhengig av hva slags hjelpemidler som benyttes. I forskrift til loven finnes bestemmelser om informasjonssikkerhet som gjelder for all behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, ”...der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet, er nødvendig med sikkerhetstiltak”.

Vurdering av risiko er utgangspunkt for ethvert sikkerhetsarbeid – sikkerhet er nettopp håndtering av risiko. Risikovurdering i denne sammenheng har som formål å identifisere hendelser som kan få betydning for sikring av personvernet, og uttrykke en hypotese om konsekvenser av hendelsene og sannsynligheten for at de inntreffer. En viktig del av oppgaven er kartlegging av de aktiva som må sikres, og å kartlegge det miljø verdiene befinner seg i. Risikovurderingen skal i tillegg identifisere behov for risikoreducerende tiltak – ved å sammenligne avdekket risiko med akseptabelt risikonivå. I forlengelsen av dette er det naturlig å gi anbefalinger om sikkerhetstiltak – for å understreke resultater av vurderingen, og til hjelp i videre arbeid.

Risikovurdering er altså et sentralt element i sikkerhetsarbeidet. Risikovurdering er også viktig ved lovregulering av sikkerhet. Kravet nå er ofte at sikkerhetstiltak skal implementeres forholdsmessig overfor aktuell risiko. Det er ikke bare i personopplysningsloven man finner bestemmelser om risikovurdering; andre eksempler er SIS-loven, sikkerhetsloven og helseregisterloven¹.

Det finnes en rekke verktøy til hjelp ved vurdering av risiko. Felles for mange er at de er svært omfattende, med fokus på detaljert og formell metodikk. Det er viktig at arbeidet med å vurdere risiko får et omfang som tjener formålet. Det er derfor nødvendig å ta hensyn til både verdienes art og sikkerhetsbehov, og virksomhetens størrelse og kompleksitet ved valg av arbeidsmåte.

I dette dokumentet beskrives en metode for risikovurdering. Dokumentet tar for seg de elementer som naturlig inngår i en slik vurdering, og presenterer disse i naturlig rekkefølge for gjennomføringen. Det knyttet videre noen kommentarer til oppfyllelse av kravet om risikovurdering i personopplysningsforskriften § 2-4. Metoden kan virke omfattende – spesielt for mindre virksomheter. Det er imidlertid lagt vekt på å beskrive hva som skal gjøres, mer enn på hvordan aktivitetene utføres. Metoden bør derfor være skalerbar i forhold til virksomhetenes størrelse og sikkerhetsbehov, og det antas at den kan benyttes med godt resultat også av små virksomheter.

1.1 Risiko og personvern

Risikovurdering som beskrevet i dette dokumentet kan benyttes for de fleste typer risiko, og i de fleste samfunnssektorer. Det er imidlertid fokusert på oppfyllelse av

¹ Lov om Schengen informasjonssystem, Lov om forebyggende sikkerhetstjeneste, Lov om helseregistre og behandling av helseopplysninger.

personopplysningsforskriftens bestemmelse om risikovurdering. Metoden er følgelig i første rekke tenkt anvendt for å oppfylle disse kravene.

Bestemmelsen om risikovurdering ved behandling av personopplysninger er gitt i personopplysningsforskriften § 2-4 hvor det fremgår at risikovurdering skal gjennomføres ” ... for å klarlegge sannsynlighet for og konsekvens av sikkerhetsbrudd ... ”. Bestemmelsen utdypet det generelle sikkerhetskravet i personopplysningsloven § 13 om å sørge for ” ... tilfredstillende informasjonssikkerhet ... ”, det vil si etablering av sikkerhetstiltak i forhold til faktisk risiko.

Risikobegrepet rommer to størrelser: sannsynlighet for at noe skal skje, og hvilke konsekvenser denne hendelsen kan få. Når vi snakker om sikkerhetsrisiko for informasjonssystemer, vil de hendelsene som på denne måten vurderes være knyttet til de tre aspektene man vanligvis forbinder med informasjonssikkerhet. Dette er konfidensialitet², integritet³ og tilgjengelighet⁴.

I merknadene til personopplysningsforskriften § 2-4 presiserer Justisdepartementet at risikovurderingen ikke bør være mer omfattende eller formalisert enn strengt tatt nødvendig. Dette er en grunn til valget av begrepet *risikovurdering* i stedet for den mer formelle betegnelsen *risikoanalyse*.

Formålet med vurderingen skal være avdekking av personvernrisiko. – det vil si forhold knyttet til liv/helse, økonomi eller anseelse/integritet, for enkeltmennesker. Vurdering av annen risiko som virksomheten står overfor – eksempelvis forretningsmessig risiko – er ikke tema i denne bestemmelsen.

Risikovurdering kan foretas både i forkant og i etterkant av et informasjonssystem bygges opp. Det er allment akseptert at det ideelle er å kunne foreta vurderingen i planleggingsfasen. På dette tidspunktet er det mulig å være føre var, og finne de mest optimale løsningene.

En risikovurdering er ikke bare en passiv målemetode for å undersøke risikonivået. Metoden er like viktig for å definere hvilket risikonivå man er villig til å akseptere for behandlingen av bestemte personopplysninger i et system. Ved å beskrive de to størrelsene sannsynlighet og konsekvens kan man sette opp akseptkriterier for risikonivået. Senere risikovurderinger vil da ha som hensikt å måle det aktuelle risikonivået mot disse akseptkriteriene.

Ytterligere to aktiviteter er nødvendige for å kunne foreta en risikovurdering. Det må gjøres en vurdering av de personopplysningene som det skal vurderes sikkerhetsrisiko for. Hvor store vil konsekvensene av brudd på konfidensialitet være? Tilsvarende vurdering må gjøres i forhold til integritet og tilgjengelighet. Det er altså en sammenheng mellom personopplysningenes karakter, det planlagte formålet med behandlingen, og konsekvensen av sikkerhetsbrudd, som er det ene elementet i risikobegrepet.

² Med sikring av konfidensialitet menes beskyttelse mot at uvedkommende får innsyn i opplysningene

³ Med integritet menes at opplysningene ikke blir endret som følge av utilsiktet eller uautorisert aktivitet

⁴ Med tilgjengelighet menes at tilstrekkelige og relevante opplysninger er tilstede når det er behov

Videre må det gjøres et anslag over trusler, hvor man forsøker å identifisere mulige hendelser som kan føre til sikkerhetsbrudd. Eksempelvis vil tilknytning til Internett fra nettverket med personopplysninger gi opphav til en lang rekke trusler som må vurderes. I forhold til risikobegrepet vil vurderingen omfatte hvor stor mulighet det er for at truslene skal resultere i uønskede hendelser, og altså fokusere på det andre elementet i risikobegrepet.

Sannsynlighet for at en hendelse skal inntreffe som resultat av menneskelig aktivitet kan også vurderes ved en betraktning av hvor mye som skal til av tilfældigheter, kvalifisert kunnskap og grad av besluttsomhet. Vil uaktsomhet, forsett eller overlegg være tilstrekkelig?

Man skal heller ikke glemme de trusler som kommer fra omgivelsene, uten at mennesker nødvendigvis er direkte involvert når hendelsen utløses. Vann og brann er stikkord for hendelser som kan utløse både større og mindre katastrofer, ofte med store konsekvenser for tilgjengeligheten til informasjon.

2 Akseptabelt risikonivå

En forutsetning for å kunne ha en forsvarlig risikostyring er at det finnes noen kriterier å styre i forhold til. Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et på forhånd akseptert nivå. Å fastlegge et nivå for hvilken risiko virksomheten skal kunne leve med er en ledelsesbeslutning.

Disse akseptkriteriene vil også påvirkes av ytre rammevilkår og lovpålagte krav. For eksempel sier forskriften til personopplysningsloven at *”Datatilsynet kan gi pålegg om sikring av personopplysninger, herunder fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger”*.

Virksomhetene kan altså ikke fritt velge hvor stor risiko personopplysninger kan utsettes for. Målet med sikkerhetsbestemmelsene er blant annet å oppnå et minimumsnivå for sikkerhet, for blant annet å sikre tilfredstillende informasjonssikkerhet også når opplysninger overføres fra en virksomhet til en annen. Derfor omfatter bestemmelsene krav om konkrete tiltak – i første rekke i §§ 2-10 til 2-14.

I tillegg kan Datatilsynet gjennom pålegg fastlegge kriterier for akseptabelt risikonivå – for virksomheter som har besluttet et for lavt nivå, eller for virksomheter som slett ikke har fastlagt akseptabelt risikonivå. Datatilsynet kan også veilede virksomheter i arbeidet med sikring av personopplysninger, og bistå ved utarbeidelse av bransjevisse adferdsnormer. Det vil være naturlig å kombinere disse oppgavene i form av bransjenormer som angir akseptabelt risikonivå for en hel bransje eller samfunnssektor.

Akseptabelt risikonivå skal fastlegges for alle sikkerhetsbehov: Konfidensialitet, tilgjengelighet og integritet. I noen situasjoner kan disse tre behovene komme i konflikt. Særlig vil behov for konfidensialitet og tilgjengelighet kunne være vanskelig å forene. Det er viktig at kryssende hensyn identifiseres, og at prioritering mellom forskjellige behov fremgår av beskrivelsen av akseptabelt risikonivå.

Beslutning om akseptabelt risikonivå skal blant annet uttrykkes i virksomhetens sikkerhetsmål. Sikkerhetsmålet skal, på et overordnet nivå, beskrive formålet med bruken av informasjonsteknologi og angi sikkerhetsbehov med hensyn på

konfidensialitet, tilgjengelighet og integritet. Dette vil også kunne innebære en prioritering mellom forskjellige sikkerhetsbehov.

Eksempel på beskrivelse av overordnet prioritering mellom sikkerhetsbehov:

"... behov for tilgang skal ikke sikres på bekostning av behovet for konfidensialitet"

Det er også nødvendig med en detaljert beskrivelse av akseptabelt risikonivå. Denne beskrivelsen bør angi hvilke personopplysninger og behandlinger som berøres, hendelser med betydning for personvernet og akseptable nivåer for konsekvens og sannsynlighet. Beskrivelsen må angi prioritering mellom forskjellige sikkerhetsbehov, og – på overordnet nivå – beskrive risikoreducerende tiltak.

Detaljert beskrivelse av akseptabelt risikonivå skal inngå i underlag for gjennomføring av risikovurdering. Beskrivelsen kan også tas med i instruks for informasjonssikkerhet som del av informasjon om forventet sikkerhetsnivå.

Det følgende er enkle eksempler på beskrivelse av akseptabelt risikonivå ved behandling av personopplysninger:

"... Sikkerhetstiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne forårsake hendelser med katastrofale konsekvenser for enkeltmenneskers personvern. Egne medarbeidere uten gode resurser og god/fullstendig kjennskap til sikkerhetstiltak skal ikke kunne forårsake slike hendelser, og heller ikke ved uaktsomhet eller ved forsett"

"... Virksomheten registrerer sensitive personopplysninger om sine kunder. Utlevering av opplysningene kan medføre alvorlig tap av anseelse og integritet for dem det gjelder. Det er derfor nødvendig å sikre opplysningenes konfidensialitet. Dette hensynet har prioritet foran hensynet til tilgjengelighet og integritet. Det vil ikke være akseptabelt at medarbeidere kan forårsake konfidensialitetsbrudd uaktsomt eller ved forsett – eller at personer utenfor virksomheten med overlegg kan få tilgang til disse"

"... Virksomheten behandler personopplysninger av vital betydning for enkeltpersoner. Forsinkelser eller feil kan medføre uopprettelig økonomisk tap for disse. Det er derfor nødvendig å sikre opplysningenes tilgjengelighet og integritet. Selv om enkelte kunder kan oppfatte opplysningene som følsomme, vil hensynet til tilgjengelighet og integritet ha prioritet foran hensynet til konfidensialitet. Det må hindres at medarbeidere uaktsomt påvirker integriteten ved registreringer og uthenting av opplysninger. Videre er det avgjørende at personer utenfor virksomheten ikke forsettlig kan påvirke driftsstabiliteten..."

På bakgrunn av de beskrevne akseptkriteriene må det utarbeides en sikkerhetsstrategi som angir i hovedsak hvilke virkemidler som skal benyttes for å oppnå et tilfredsstillende sikkerhetsnivå.

3 Forberedelse av risikovurdering

3.1 Planlegging

Risikovurdering er normalt en situasjonsbetinget aktivitet – det vil si at arbeidet igangsettes ved behov og ikke ved faste intervaller. Bakgrunn for igangsetting er

endringer i verdier eller miljø av betydning for informasjonssikkerheten. Endringene kan være forårsaket av virksomheten selv, eller oppstå uavhengig – eksternt – i forhold til denne.

Forberedelse til risikovurdering omfatter i første rekke beskrivelse av mål – det vil si beskrivelse av den hypotese som skal undersøkes. Målet må angis sammen med eventuelle avgrensninger. Dette kan være avgrensninger i omfang, spesielle forutsetninger eller antagelser, samt resursbegrensninger – knyttet til tid, bemanning, utstyr, datagrunnlag, osv.. Målbeskrivelsen må også gi informasjon om hvem som berøres av arbeidet (virksomhet, avdeling, medarbeidere og evt. eksternt personell).

Risikovurdering må utføres slik at resultater er tilgjengelig i god tid før endring inntreffer, og kan inngå i beslutningsgrunnlaget for håndtering av endringen. Dette bør være mulig for endringer virksomheten selv forårsaker, men blir straks vanskeligere ved eksterne forhold. For å sikre at risikovurderinger gjennomføres til riktig tid, kan det være nødvendig å utarbeide kriterier for igangsetting. Disse kriteriene må gi informasjon om vilkår for igangsetting, og retningslinjer for overvåkning av interne og eksterne forhold som kan gjøre det nødvendig å gjennomføre risikovurdering.

3.2 Organisering

Risikovurdering kan organiseres som prosjekt, og gjennomføres i henhold til prosjektplan. Med utgangspunkt i målbeskrivelsen skal denne planen angi start- og sluttidspunkt, alle aktiviteter som skal utføres med ansvar for utførelse. Prosjektplanen må også gi informasjon om ansvaret for å lede/koordinere vurderingen.

Ved bemanning av prosjektet er det nødvendig å ta hensyn til kunnskaper og erfaring – innen risikovurdering, og i forhold til de aktiva og miljø som skal undersøkes. Kvaliteten på utført arbeide bør kontrolleres av en medarbeider som ikke er direkte involvert i selve vurderingen. Avhengig av omfanget kan slik kontroll gjennomføres fortløpende eller som sluttkontroll.

Omfang og detaljeringsgrad for planlegging og organisering av risikovurdering avhenger av sikkerhetsbehovet og virksomhetens størrelse/kompleksitet. Som nevnt foran er det resultatet av vurderingen som er viktig, og selv en enklere tilnæringsmetode vil kunne gi gode resultater. Generelt kan det sies at nytteverdien er større ved å forenkle metoden samtidig som analysen gjennomføres på en skikkelig måte, enn ved å forsøke seg på et komplisert opplegg man kanskje ikke behersker fullt ut.

Det kan imidlertid være nødvendig å utarbeide retningslinjer for planlegging og organisering av risikovurderinger – med informasjon knyttet til fremgangsmåte, bemanning og kompetansekrav, rapportering og lignende.

Personopplysningsforskriften § 2-4 pålegger gjennomføring av risikovurdering ” ... ved endringer som har betydning for informasjonssikkerheten ... ”. Risikovurderinger skal fortrinnsvis gjennomføres før behandlingen av personopplysninger settes i gang, og deretter ved endringer – enten disse følger av beslutninger virksomheten har tatt, eller er endringer virksomheten ikke har herredømme over.

Vurdering av personvernrisiko forutsetter kompetanse innen personvern og sikring av personopplysninger – i tillegg til kunnskaper om risikovurdering generelt og om det miljø som skal undersøkes.

Personvernregelverket omfatter krav om at arbeidet med å oppfylle bestemmelsene skal utføres ” ... *planlagt og systematisk* ... ” – det vil si i henhold til rutiner. Det er derfor aktuelt å utarbeide rutiner for risikovurdering.

4 Kartlegging

4.1 Verdier og miljø

Informasjon er et aktivum som, i likhet med andre viktige virksomhetsaktiva, har en verdi for en organisasjon og derfor må vernes på forsvarlig måte. Personopplysninger er i tillegg et aktivum av særlig stor verdi for dem informasjonen omhandler. Begrepet *verdi* benyttes for det aktivum virksomheten må sikre konfidensialitet, tilgjengelighet eller integritet for. Verdier kan være eiendeler som utstyr eller programvare, eller informasjon/opplysninger. Verdier identifiseres ved å anslå taps- eller skadepotensial – i form av kostnad for gjenanskaffelse, indirekte kostnader som tap av ”goodwill”, osv. I personvernsammenheng vil verdiene kunne representeres ved å anslå tap/skadepotensial for enkeltmenneskers liv, helse, økonomisk tap, tap av anseelse eller integritet. Kartlegging av verdier resulterer i oversikt hvor antatt sikkerhetsbehov knyttes til den enkelte verdi.

Anslått taps- eller skadepotensial gir grunnlag for å anta sikkerhetsbehovet. Det videre arbeid har som formål å avdekke risiko og dermed fastslå det faktiske sikkerhetsbehovet. Noen ganger vil dette behovet være annerledes enn antatt innledningsvis. I så fall må det vurderes om verdikartleggingen må gjøres på nytt.

Begrepet *miljø* beskriver de omgivelser eller situasjoner verdiene befinner seg i. Miljøet omfatter blant annet informasjonssystem, (fysisk-)installasjon og organisasjon. Også de prosesser og driftstilstander verdiene inngår i er en del av miljøbeskrivelsen. I tillegg er det nødvendig å avdekke eksisterende sikkerhetstiltak – organisatoriske eller tekniske.

Ved risikovurdering undersøkes verdier som befinner seg i et konkret miljø. Undersøkelsen må ta for seg grensene mellom dette miljøet og ”verden for øvrig”, samt grensene mellom forskjellige elementer internt i miljøet. Miljøkartleggingen må følgelig identifisere ulike grensesnitt, som koblinger mellom informasjonssystemet og eksterne datanett, fysiske yttergrenser, forholdet ”menneske/maskin” (kompetanse, rutiner), mv.

4.2 Verktøy

Forskjellige verktøy og metoder kan tas i bruk for kartlegging av verdier og miljø – også metodikk som ikke direkte er utarbeidet for kartlegging ved risikovurdering. Resultater fra *prosesskartlegging* forteller om hvor og hvordan verdier bearbeides, og vil samtidig gi informasjon om muligheter for tap eller skade. *Sikkerhetstester* vil avdekke om kjente sikkerhetsteknikker eller -tiltak er tatt i bruk og fungerer. Rapporten fra sikkerhetsrevisjoner gir informasjon om sikkerhetsarbeidet i virksomheten slik det

faktisk gjennomføres – i forhold til de beslutninger som er tatt. Rapportene forteller også om virksomheten oppnår planlagt sikkerhetsnivå.

4.3 Kartlegging av personopplysninger

Ved vurdering av personvernrisiko representerer personopplysningene de *verdiene* som behandles. Potensial for tap eller skade må knyttes til følgene for den enkeltes personvern. Av personopplysningsforskriften § 2-1 fremgår det at opplysninger skal sikres for å ”... hindre fare for tap av liv og helse, økonomisk tap, eller tap av anseelse og personlig integritet ...”. Verdiene – personopplysningene – kartlegges følgelig i forhold til potensialet for slike tap.

Til hjelp i arbeidet med å anslå taps- eller skadepotensial er det aktuelt å avdekke om personopplysningene er *sensitive*. Dette begrepet skal ikke oppfattes som en sikkerhetsgradering i seg selv. Personopplysningsloven benytter begrepet for vidt forskjellige opplysninger, også for slike som i seg selv ikke utløser særlige krav til sikkerhetstiltak (medlemskap i fagforeninger). Det sier imidlertid noe om forventet diskresjon, det vil si angir behov for konfidensialitet – men det må understrekes at begrepet ikke sier noe om andre behov (tilgjengelighet eller integritet). Tilsvarende gjelder for *taushetsplikt* som også angir forventet diskresjon.

Taps- eller skadepotensial kan ikke knyttes til opplysningstypen alene. Også formålet med behandlingen av personopplysninger påvirker sikkerhetsbehovet. Eksempelvis vil manglende konfidensialitet for pasientopplysninger benyttet for statistikk medføre tap av anseelse og personlig integritet. Manglende tilgjengelighet for de samme opplysningene benyttet for medisinsk behandling, vil få følger for liv og helse.

Omfanget av personopplysninger som behandles vil også være et viktig element å kartlegge. Et eksempel er behandling av personopplysninger i forbindelse med teleoperatørens virksomhet. Som grunnlag for debitering lagres meget store mengder opplysninger om enkeltpersoners bruk av telenettet. Slike informasjonsmengder kan si mye om disse personenes privatliv.

Krav om oversikt over personopplysninger følger ikke utelukkende av bestemmelsen om risikovurdering. Også andre plikter i personvernregelverket gjør det nødvendig med slik oversikt – som avdekking av formål for, og hjemmel til behandling av personopplysninger, plikt til å gi innsyn og informasjon, melde- og konsesjonsplikt. Det er derfor aktuelt å legge kartleggingsarbeidet opp slik at oversikten dekker alle slike formål.

Kartlegging av miljø for behandling av personopplysninger skiller seg ikke vesentlig ut fra kartlegging av miljøer for annen informasjonsbehandling. Ved bruk av prosesskartlegging i dette arbeidet er det naturlig å identifisere den formålsavgrensede behandlingen som ”prosessen” – i stedet for å ta utgangspunkt i typiske forretningsprosesser.

Eksempel

Nedenfor er et eksempel på kartlegging av personopplysninger:

Informasjonstype Formål med behandlingen	Hjemmel for behandling	Meldeplikt Konsesjonsplikt (evnt. unntak)	Sensitive person-oppl.?	Tausehetsplikt?	Omfang	Sikkerhets- behov
Lønns- og personaloppl.: Personaladm.	samtykke	(pof § 7-16)	nei	nei	400	K/T/I
Barnevern: -vurdering og tiltak	Barnevernloven, Konsesjon**) 1.1.91	Konsesjonspliktig	ja	ja	1200	K/T/I
Helse opplysninger: - pasientjournal		Meldepliktig (pof § 7-24)	ja	ja	2000	K/T/I
Oppl. Om sosialklienter: Adm. av sosialomsorg	Sosialtjenste- loven,	(pol § 33)	ja	ja	700	K/T/I
Kundeopplysninger: Kundeoppfølging	Pol § 8 a)	(pof. § 7-7)	nei	nei	5000	K
Hendelsesregister: - aktivitetslogg	Pol § 8 f)	(pof. § 7-11)	nei	nei	varierende	K/I

Pol: Personopplysningsloven. Pof: Personopplysningsforskriften

5 Identifisere uønskede hendelser

En hendelse er en handling eller tilstand som kan utsette verdier for risiko – i form av manglende konfidensialitet, tilgjengelighet eller integritet. Disse verdiene kan – grovt sett – påvirkes av tre typer uønskede hendelser: Utlevering, utilgjengelighet og endring. Hendelsene kan ytterligere detaljeres ved å inkludere elementer som kompensering, varighet og deteksjon i beskrivelsen:

- Utlevering
 - kan tilbakeføres
 - permanent
- Utilgjengelighet
 - avgrenset tidsrom
 - permanent
- Endring
 - sporbar og kan rettes
 - sporbar og permanent
 - ikke sporbar

Inndelingen kan benyttes som utgangspunkt for beskrivelse av hendelser. Slike beskrivelser må i tillegg gi informasjon om hvilke verdier som berøres, og hvor i miljøet hendelsen kan inntreffe – eksempelvis:

” ... *uønsket, permanent utlevering av kundeopplysninger via e-post systemet ...* ”

En lang rekke hendelser kan påvirke verdiene i virksomheten. Risikovurderinger vil bli svært omfattende dersom alle sammen skal omfattes av arbeidet. Det er derfor nødvendig å velge ut hvilke hendelser som faktisk medfører en risiko som krever vurdering av tiltak. Denne utvelgelsen må ta utgangspunkt i det taps- eller skadepotensial som er anslått ved kartlegging av verdier og miljø.

5.1 Årsak

Mens undersøkelsen av uønskede hendelser skal gi svar på spørsmål av typen ”*hva kan skje ...*”, er identifisering av årsaker spørsmål om ”*hvordan ...?*” Årsaken er den aktivitet eller situasjon som får hendelsen til å inntreffe. Ofte er det i denne sammenheng også naturlig å spørre om ”*hvem ...?*”, det vil si å avdekke hvilken person som forårsaker hendelsen. En grovinndeling i så måte er hvorvidt det gjelder egne medarbeidere eller personer utenfor virksomheten. I forlengelsen av avdekking av ”*hvem...?*”, kan det være aktuelt å spørre ”*hvorfor ...?*”. Svaret er imidlertid ikke en del av årsaksbeskrivelsen, men berører motivasjon og omfattes av sannsynlighetsvurderingen.

Årsaker til at uønskede hendelser utløses behøver ikke være resultat av en direkte handling fra personer. Like aktuelle er påvirkning fra omkringliggende miljø. Stikkord for slike årsaker er varme (både brann og overtemperatur), vann (både oversvømmelse og fukt), smitte fra hendelser i nærliggende virksomheter osv.

Det er viktig at hendelser og årsaker beskrives hver for seg. Dette for å sikre at alle hendelser av betydning er avdekket og omfattes av videre arbeid. Separate beskrivelser vil også bidra til at viktige årsaker blir mer synlige og dermed være til bedre hjelp ved valg av sikkerhetstiltak. Manglende skille mellom beskrivelse av hendelser og årsaker vil kunne resultere i omfattende beskrivelser som tilsynelatende dekker en rekke hendelser, men som i virkeligheten kun beskriver én hendelse med en mengde mulige årsaker.

Eksempel: En alvorlig trussel kan være at sensitive personopplysninger blir eksponert for uvedkommende. Årsakene til dette kan være flere: For eksempel datainnbrudd pga. for svak sikkerhetsbarriere, autorisert bruker som pga. dårlig skille mellom autoriserte og uautoriserte brukere får tilgang til opplysninger, mangelfulle rutiner ved sletting av lagringsmedia som skal avhendes osv.

Målet for årsaksanalysen er å beskrive årsaker (og hendelser) detaljert nok til at konsekvens- og sannsynlighetsvurdering kan gjennomføres – og til hjelp i arbeidet med å velge sikkerhetstiltak. Det vil ikke være uvanlig at det ut fra årsaksbeskrivelsen kan angis nødvendige sikkerhetstiltak allerede på dette stadium i risikovurderingen.

5.2 Hendelser som berører personvernet

Uønsket hendelse i personvernsammenheng er en handling eller tilstand som innebærer utilfredsstillende sikring av personopplysninger. Grovinndelingen av hendelsestyper som er beskrevet foran kan benyttes som utgangspunkt også ved beskrivelse av slike hendelser. Beskrivelsene må i tillegg angi hvilke personopplysninger – og hvilke behandlinger – som berøres. Spesielt gjelder ved utlevering av opplysninger som er omfattet av taushetsplikt at beskrivelsen bør gi informasjon om taushetsplikten også

gjelder for mottakere. Slik informasjon er nødvendig for å vurdere mulighet for å kompensere hendelsen.

Identifisering av årsaker til hendelser som berører personvernet er som for identifisering av årsaker for øvrig. Årsaksbeskrivelser skal angi aktiviteter eller situasjoner knyttet til behandlingen av personopplysninger.

Eksempler: Det følgende er eksempler på hendelser som berører personvernet. Den enkelte hendelse berører én type personopplysning benyttet i én behandling – og det er identifisert én årsak til hendelsen:

”... Personalopplysninger benyttet for skaderegistrering, utleveres til eksternt personell. Hendelsen inntreffer når egne medarbeidere overfører slike opplysninger eksternt uten kryptering – og opplysningene overføres til feil adressat, eller overføringen ”avlyttes” av eksternt personell ... ”

”... kundeopplysninger (leveransedata) er utilgjengelige. Hendelsen inntreffer når egne medarbeidere registrerer feil opplysning og ikke oversender bestillingsbekreftelse til kunde for kontroll ... ”

6 Konsekvens

6.1 Konsekvensvurdering

På samme måte som når årsaker vurderes, skal konsekvensvurderingen ta utgangspunkt i de uønskede hendelsene som er identifiserte. Konsekvensvurdering er vurdering av hvilke følger en hendelse kan få – det vil si å gi svar på spørsmålet av typen ”*hva medfører ...*”? Konsekvens kan uttrykkes som økonomisk tap, men også forhold til virksomhetens anseelse og som evt. straffeansvar for virksomhet og ledelse.

Økonomisk tap, tap av anseelse og straff kan betegnes endelig konsekvens. Ofte vil risikovurdering ha som mål å avdekke konsekvenskjeder eller årsakssammenhenger bak denne konsekvensen. Det kan derfor være aktuelt å angi konsekvenser detaljert, eksempelvis utilsiktet offentliggjøring av opplysninger, driftsavbrudd – nedetid, feil i datagrunnlag. Detaljert beskrivelse av konsekvenser er et viktig hjelpemiddel ved valg av sikkerhetstiltak. Tiltak for å begrense konsekvensene kan være å bryte årsakssammenhenger og hindre at hendelsen fører til en endelig konsekvens som nevnt foran. Konsekvensvurdering med høy detaljeringsgrad kan imidlertid bli svært omfattende. Valg av riktig detaljeringsgrad er derfor et viktig element i arbeidet.

Konsekvens må angis kvalitativt som beskrivelse av de følger en hendelse kan få. Det vil også være nødvendig å angi konsekvens som en kvantitativ størrelse, for å synliggjøre og oppsummere resultater fra risikovurdering, og til hjelp i arbeidet med å avdekke restrisiko. Denne kvantitative angivelsen av konsekvens er kun et middel for å angi nivå for akseptert risiko, og for å sammenlikne vurderinger fra forskjellige hendelser som

behandles i forbindelse med risikovurderingen. Eksempelvis kan ulike grader av konsekvens rangeres som følger:

- K=4, katastrofal konsekvens
- K=3, stor konsekvens
- K=2, moderat konsekvens
- K=1, liten konsekvens

6.2 Personvernkonsekvens

Ved vurdering av personvernrisiko er målet med konsekvensvurderingen å avdekke de følger en hendelse kan få for enkeltmenneskers personvern. Formålet er altså forskjellig fra arbeid med å avdekke annen risiko for virksomheten – eksempelvis forretningsmessig risiko. Det må imidlertid understrekes at selve metoden for konsekvensvurdering – og for risikovurderingen for øvrig – er den samme.

Ved vurdering av personvernkonsekvens er det naturlig å ta utgangspunkt i målet med sikring av personopplysninger: Beskyttelse av liv/helse, økonomi og anseelse/personlig integritet for enkeltmennesker. Personvernkonsekvens skal derfor beskrives i forhold til disse begrepene - både kvalitativt og kvantitativt:

- K=4, hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.
- K=3, hendelsen kan føre til tap av helse, eller kan medføre uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse og integritet.
- K=2, hendelsen kan medføre betydelig økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatte som krenkende, eller som andre kan gjøre nytte av).
- K=1, hendelsen kan medføre økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som følsomme).

Konsekvens av en hendelse vil i første rekke være knyttet til verdienes – personopplysningenes – art. I tillegg vil konsekvens også avhenge av hvor mange personer som berøres. Personvernkonsekvens må rangeres høyere, eksempelvis ett nivå, dersom hendelsen får følger for mange mennesker. Dette selv om følgene for den enkeltes personvern vurderes som liten.

Eksempel: Konsekvens angis kvalitativt og kvantitativt. Det understrekes igjen at vurdering av personvernkonsekvens har som formål å avdekke følger for den enkeltes personvern – ikke eventuelle følger sikkerhetsbruddet kan få for virksomheten. Med utgangspunkt i eksempler på hendelser beskrevet foran, kan konsekvens angis som følger:

” ... Personalopplysninger benyttet for skaderegistrering omfatter sensitive personopplysninger om helseforhold.. Utlevering av slike opplysninger til eksternt

personell vil føre til alvorlig tap av anseelse og integritet for den opplysningene gjelder. Personvernkonsekvensen er stor (K=3) ...”

” ... Kundeopplysninger benyttes for leveranse av tidskritiske tjenester. Manglende tilgang til slike opplysninger vil medføre betydelig – om enn opprettelig – økonomisk tap for kunder. Personvernkonsekvensen er moderat (K=2) ... ”

7 Sannsynlighet

7.1 Sannsynlighetsvurdering

Vurdering av sannsynlighet for at en hendelse inntreffer har som mål å finne svar på spørsmålet ”*hvor ofte ...?*”. Dette svaret må angis kvalitativt som beskrivelse av hyppighet av, evt. forutsetning for at en hendelse inntreffer. Som for konsekvensvurdering er det nødvendig å kunne representere graden av sannsynligheten kvantitativt:

- S=4, svært høy sannsynlighet for at hendelsen inntreffer.
- S=3, høy sannsynlighet for at hendelsen inntreffer.
- S=2, moderat sannsynlighet for at hendelsen inntreffer.
- S=1, lav sannsynlighet for at hendelsen inntreffer.

For å avdekke forventet hyppighet er det aktuelt å ta utgangspunkt i historiske data om identiske eller tilsvarende hendelser. Forutsatt at historiske data eksisterer vil sannsynlighetsvurderingen i så fall kunne baseres på statistiske metoder. I forhold til hyppighet – eller frekvens – kan sannsynligheten eksempelvis kvantifiseres som følger:

- S=4, hendelsen inntreffer flere ganger pr. år.
- S=3, hendelsen inntreffer årlig eller sjeldnere.
- S=2, hendelsen inntreffer 1 gang pr. 10 år eller sjeldnere.
- S=1, hendelsen inntreffer 1 gang pr. 50 år eller sjeldnere.

Svært ofte mangler historiske data. Dette fordi avvik korrigeres fortløpende, og at uønskede hendelser derfor ikke registreres flere ganger, eller fordi hendelsesregistreringen er mangelfull. Ofte skal risikovurdering gjennomføres for nye verdier og/eller nytt miljø, og historiske data er ikke tilgjengelige av den grunn.

7.2 Vurdering ut fra letthetsbetraktning

I mangel av historiske data kan avdekking av forutsetninger for at en hendelse kan inntreffe være et alternativ. En slik letthetsvurdering skal gi svar på spørsmålet ”*Hva skal til for at ...?*” Den må omfatte vurdering av behovet for resurser i form av utstyr og programvare, og i form av kompetanse og evner. Også mulighet til å forårsake hendelsen må vurderes. Denne delen av vurderingen henger tett sammen med informasjon om hvem som står bak – som angitt i årsaksbeskrivelsen.

Utgangspunkt for en slik ”letthetsvurdering” er, i tillegg til beskrivelser av hendelser og årsaker, utformingen av miljøet – herunder organisatoriske og tekniske sikkerhetstiltak. Gradert etter letthet kan sannsynlighet beskrives som følger:

- S=4, sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale resurser. Det er ikke nødvendig med kjennskap til tiltakene.
- S=3, sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten. Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene. Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale resurser.
- S=2, sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale resurser, som i tillegg har normal kjennskap til tiltakene. Eksternt personell trenger gode resurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse.
- S=1, sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode resurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene.

7.3 Vurdering med utgangspunkt i motivering

Ved sannsynlighetsvurdering er utgangspunktet i første rekke beskrivelse av miljøet. Også verdienes art påvirker vurderingen – i forhold til motivering for å forårsake hendelsen. Når målet er gevinst for den som forårsaker hendelsen, kan motivering avdekkes ved å svare på spørsmålet ”*Hvordan kan andre nyttegjøre seg ...?*” Det er altså nødvendig å knytte anslag over gevinst for andre til verdiene – i tillegg til taps- og skadepotensial for virksomheten selv.

Ofte vil motivet være vanskelig å avdekke. Bakgrunn for hendelsen kan være følelser som rettferdighet, prestisje, hevn, ødeleggelseslyst, mv. og det blir vanskelig å finne svar på spørsmålet ”*Hvorfor vil noen ...?*” Alternativet er å avdekke den innsats eller engasjement som må til for å forårsake hendelsen. Begrepene *uaktsomhet, forsett og overlegg* kan benyttes for å angi denne innsatsen. Sannsynlighet kan i så fall beskrives som følger:

- S=4, sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.
- S=3, sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettelig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.
- S=2, sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe

kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.

- S=1, sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.

7.4 Sannsynlighet og personvern

Som nevnt foran vil sannsynlighetsvurderingen i første rekke ta utgangspunkt i beskrivelsen av miljø. Sannsynlighet for hendelser som kan påvirke enkeltmenneskers personvern vil følgelig i mindre grad påvirkes av at det er personopplysninger som behandles. Unntaket er imidlertid også her knyttet til motivering.

Sannsynlighetsvurderingen må avdekke om noen kan ha nytte av å påvirke behandlingen av personopplysninger. Nytt i denne sammenheng kan eksempelvis være betaling for utlevering av opplysninger eller etter trusler om å påvirke behandlingen ved å hindre tilgang til, eller skade/endre opplysninger.

Eksempel: Sannsynlighet angis kvalitativt ved å beskrive hyppighet av, evt. forutsetning for hendelsen. Sannsynlighet beskrives også kvantitativt. Sannsynlighet kan angis som følger:

” ... Personalopplysninger som virksomheten behandler skal krypteres ved ekstern overføring. Den enkelte medarbeider må selv iverksette tiltak for kryptering. Opplysningene skal kun overføres til forhåndsbestemte adresser. Den enkelte medarbeider må selv velge riktig adresse. Egne medarbeidere kan omgå/bryte tiltakene med små til normale resurser – og uten kjennskap til tiltakene. Tiltakene kan omgås/brytes uaktsomt. Eksternt personell vil måtte trenge ytterligere ressurser, og god/fullstendig kjennskap til tiltakene, for å omgå/bryte disse. Eksternt personell må opptre med overlegg. Sannsynligheten for sikkerhetsbrudd anses være høy (S=3) ... ”

8 Risiko

8.1 Beskrivelse av risiko

Begrepet risiko uttrykker en hypotese om den fare en hendelse representerer overfor verdiene i virksomheten. Risiko er kombinasjon av konsekvens av en hendelse og sannsynlighet for at den inntreffer. Dersom konsekvens beskrives som økonomisk tap av en viss størrelse, og sannsynlighet angir forventet hyppighet, vil risiko uttrykke totalt tap over tid. Det er i denne sammenheng verd å merke seg at flere kombinasjoner av konsekvens og sannsynlighet kan gi likt eller tilsvarende risikonivå (liten konsekvens, høy sannsynlighet – stor konsekvens, lav sannsynlighet).

Som nevnt kan konsekvens og sannsynlighet angis som kvantitative størrelser, selv om disse snarere er tallverdier for beskrivelser av kvalitative begrep enn objektive verdier. Risiko kan da uttrykkes som produktet av de to faktorene. Dette gjør det enkelt å oppsummere resultatene fra risikovurderingen – i tabell, eller som grafisk presentasjon.

Risiko uttrykt som produkt av to størrelser gjør det også enklere å sammenligne avdekket risiko med det akseptable risikonivå som er besluttet.

Avdekket risiko skal også presenteres i detalj, som kvalitativ beskrivelse av kombinasjonen konsekvens/sannsynlighet. Presentasjonen bør fokusere på de hendelser som medfører størst risiko. Videre er det viktig at risiko over akseptabelt nivå kommer klart frem. Det samme gjelder i forbindelse med hendelser som representerer brudd på regelverk, enten dette er lovkrav, inngåtte avtaler eller virksomhetens egne retningslinjer.

Som hjelpemiddel til å uttrykke risikonivå og akseptkriterier kan det være nyttig å benytte matriser. En matrise kan for eksempel illustrere akseptabelt risikonivå i forhold til frekvens/konsekvens:

Konsevens ➤	Liten	Moderat	Stor	Katastrofal
▼ Sannsynlighet				
Lav				
Moderat	(Hendelse A)		(Hendelse B)	
Høy				
Svært høy				

Trusler/uønskede hendelser plasseres i matrisen. Området som er skravert representerer trusler som ut fra sin potensielle hyppighet og/eller konsekvens ikke kan aksepteres.

Risiko uttrykker en hypotese og må følgelig angis med en viss usikkerhet. Denne usikkerheten må angis – eller i det minste diskuteres – når resultatene fra risikovurderingen presenteres. I tillegg er det aktuelt å gi informasjon om hvordan resultatene kan etterprøves eller kontrolleres.

8.2 Personvernisiko

Personvernisiko er kombinasjonen av en hendelses konsekvens for den enkeltes personvern, og sannsynlighet for at hendelsen inntreffer. Også personvernkonsekvens angis kvalitativt og kvantitativt. Ved presentasjon av resultater fra risikovurderingen er det viktig å trekke frem hendelser med størst betydning for personvernet. I tillegg må hendelser som representere brudd på personvernregelverket beskrives.

Eksempel

Eksempel på oppsummering av resultater fra risikovurdering. Faktorene for sannsynlighet, konsekvens er beskrevet tidligere i dokumentet.

Type opplysning/ behandling	Hendelse	Sikkerhets- behov	Faktor Konsekvens	Faktor Sannsynlighet	Risikofaktor	Akseptabel risiko
Personalopplysninger - personaladministrasjon - effektivitetsmåling - adgangskontroll - IT-logger - fjernsynsovervåking - skaderegistrering	Utlevering – kan tilbakeføres	K	3	3	9	6
	Utlevering – permanent	K	3	3	9	6
	Utilgjengelighet – tidsavbrudd	T	1	3	3	8
	Utilgjengelighet – permanent	T	2	2	4	8
	Endring – sporbar og kan rettes	I	1	2	2	6
	Endring – sporbar og permanent	I	2	2	4	6
	Endring – ikke sporbar	I	2	1	2	6

Sikkerhetsbehov: K: Konfidensialitet, T: Tilgjengelighet, I: Integritet

9 Anbefalte tiltak

9.1 Risikohåndtering

Risikohåndtering må iverksettes når avdekket risiko er høyere enn akseptabelt risikonivå. Restrisiko håndteres ved hjelp av sikkerhetstiltak, enten for å redusere konsekvensene av eller sannsynligheten for uønskede hendelser. Disse kan være organisatoriske (fordeling av ansvar og myndighet mv.), eller tekniske (kryptering, brannmur mv.).

Valg av sikkerhetstiltak er ikke en del av risikovurderingen. Resultatene fra vurderingen bør imidlertid presenteres sammen med anbefalinger om tiltak som følger naturlig av det arbeid som er utført. Slike anbefalinger vil tjene både som presisering av resultatene, og som verdifullt grunnlag når nye tiltak skal besluttes.

Anbefalinger om sikkerhetstiltak kan angis med utgangspunkt i årsaksbeskrivelsen. I tillegg er resultater fra sannsynlighetsvurderingen et viktig underlag. Det bør i tillegg vurderes om risiko skal beskrives med og uten iverksetting av anbefalte tiltak.

9.2 Sikkerhetstiltak

Som nevnt foran kan både organisatoriske og tekniske tiltak benyttes for risikohåndtering. Tiltak kan videre deles inn i hvorvidt de er ment å virke forebyggende eller skadebegrensende. Ytterligere vurderingsgrunnlag for valg av tiltak er virkemåte – det vil si om tiltaket er ment å sørge for at hendelsen:

- unngås
- avskrekkes

- hindres
- isoleres
- oppdages

eller om tiltaket har som formål å gjenopprette tilstanden før hendelsen inntraff.

Det er også nødvendig å ta hensyn til kriterier for kvalitet. Det er aktuelt å sette krav til – og vurdere – funksjon, styrke og konsistens, og om tiltakene er fullstendige og dekkende. Ut over dette må det vurderes om tiltakene er kostoptimale og praktiske, og om det er mulig å verifisere at de gir tilsiktet effekt.

9.3 Sikring av personopplysninger

Personopplysningsforskriften omfatter bestemmelser om personellsikkerhet og fysisk sikring – samt om tiltak for å sikre konfidensialitet, tilgjengelighet og integritet:

- Bestemmelsene om *personellsikkerhet* (§§ 2-8 og 2-9) omfatter krav til at informasjonssystemet i utgangspunktet kun benyttes for å utføre oppgaver medarbeideren er pålagt. Privat bruk kan tillates kun så lenge slik bruk ikke utsetter personopplysningene for ytterligere risiko. Medarbeider skal ha nødvendig kunnskap for å benytte informasjonssystemet, og skal pålegges taushetsplikt.
- Bestemmelsen om *fysisk sikring* (§ 2-10) pålegger etablering av tiltak for å hindre adgang til utstyr som benyttes for å behandle personopplysninger – og til annet utstyr med betydning for informasjonssikkerheten.
- Bestemmelsen om sikring av *konfidensialitet* (§ 2-11) gjelder (kun) opplysninger der risikovurderingen har avdekket behov for slik sikring, samt for informasjon om sikkerhetstiltak når dette har betydning for informasjonssikkerheten. Aktuelle tiltak er kryptering ved ekstern overføring – samt merking, og rutiner for sletting av lagringsmedia.
- Bestemmelsen om sikring av *tilgjengelighet* (§ 2-12) gjelder (kun) for opplysninger der risikovurderingen har avdekket behov for slik sikring, samt for informasjon om sikkerhetstiltak når dette har betydning for informasjonssikkerheten. Aktuelle tiltak er beredskapsplanlegging og rutiner for sikkerhetskopiering.
- Bestemmelsen om sikring av *integritet* (§ 2-13) gjelder (kun) for opplysninger der risikovurderingen har avdekket behov for slik sikring, samt for informasjon om sikkerhetstiltak når dette har betydning for informasjonssikkerheten. Aktuelt tiltak er viruskontroll.

I tillegg til krav om sikring, omfatter personopplysningsforskriften generelle bestemmelser om hvordan sikkerhetstiltak skal utformes. Disse kravene er gitt i § 2-14.