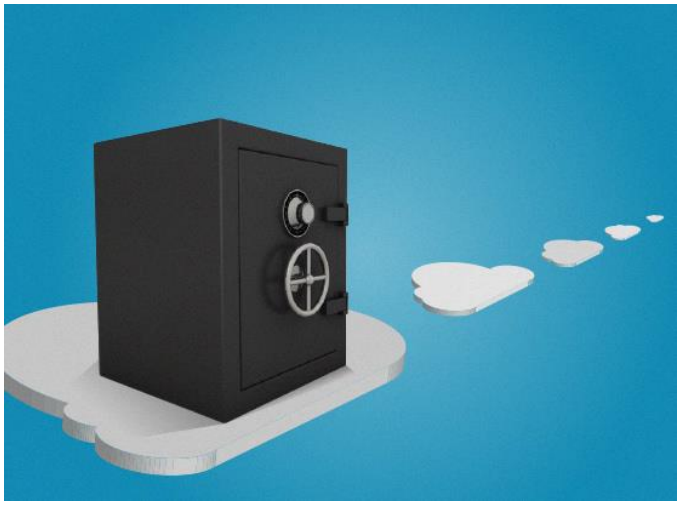
Om risikovurdering av kommunen si handsaming av personopplysningar

~ ei rettleiing ~

Fyrst ei grunngjeving :



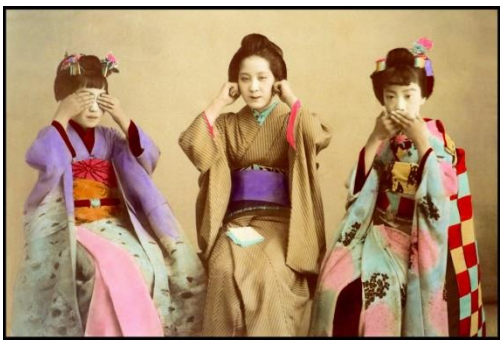
Lovverket slår fast at det er kommunen som er ansvarleg for all forvaltning av personopplysningar som kommunen nyttar. Ansvarstilhøvet gjeld også når andre forvaltar opplysningane på vegne av kommunen.

Kommunen må kunne dokumentere ei forsvarleg forvaltning. I dette ligg at kommunen må dokumentere eigen praksis, eiga vurdering av denne praksisen, samt gjennomføring av eventuelle korrigerande tiltak. Rutinemessig gjennomføring av risikovurderingar vil vere eit tenleg grunnlag for ei slik vurdering.

Når skal ein gjennomføre risikovurderingar ?

- **Ved innføring av ny personvernlovgjeving – les : GDPR.** Ei risikovurdering her skal ha som føremål å sjå til, og i neste omgang dokumentere – at eksisterande rutinar samsvarar med gjeldande lover og føresegner. Dette kan vere ei svært omfattande oppgåve, men er heilt naudsynt for at kommunane skal kunne dokumentere etterleving av gjeldande lovverk.
- **Som ein rutinemessig del av forvaltningsarbeidet.** Planmessig gjennomføring av risikovurderingar kan avdekke tilhøve som elles ville gått «under radaren» og sikre at korrigerande tiltak vert gjort der dette er naudsynt. Risikovurdringane vil også kunne fungere som nyttige repetisjonar av kva som er god praksis, og på den måten bidra til at arbeidet med å styrke personvernet vert halde i hevd.
- **Som ei oppfylgjing av avvik eller uynskte / uføresette hendingar.** Her vil risikovurdering som metode både kunne avdekke kva som var årsaka til at noko gjekk galt og påvise kva justerande tiltak som må setjast i verk. På same måte som i punktet over, vil dokumentasjon av at risikovurderingar og oppfylgjande tiltak er gjennomført, vere ein del av dokumentasjonen på at kommunen etterlever det lovpålagte datahandsamaransvaret.
- **Som ein rutinemessig del av ny bruk av personinformasjon,** til dømes når ein innfører nye tenester eller arbeidsrutinar basert på bruk av elektronisk personinformasjon. Dokumentasjonen av relevante tiltak vil då vere eit viktig grunnlag for planlegging av innføringa.

Tre sentrale aspekt i risikovurderingsarbeidet :



- **Ein skal trygge opplysningane sin konfidensialitet.** I dette ligg at opplysningane skal vernast mot innsyn frå uvedkomande.
- **Ein skal trygge opplysningane sin integritet.** I dette ligg at opplysningane ikkje skal endrast eller slettast grunna utilsikta eller uautorisert aktivitet.
- **Ein skal trygge opplysningane sitt tilgjenge.** I dette ligg at opplysningane til eikvar tid skal vere tilgjengelege for dei som har sakleg grunna behov for tilgjenge til dei.

Risikovurderinga skal altså kartlegge faktorar som kan føre med seg ei svekking av ***konfidensialiteten***, ***integriteten*** og ***tilgjenget*** til personopplysningane kommunen forvaltar. Identifiserte faktorar skal vurderast med omsyn til hyppigheit og konsekvens, og korrigerande tiltak skal setjast i verk og dokumenterast. I den grad omsyn til desse tre aspekta fører til ein interessekonflikt, skal omsyna vektast og prioriterast.

Utgangspunkt for risikovurderinga :

Ein kan tenkje seg at data har eit «livsløp» med fem «fasar». Desse er

- **data inn,** som handlar om korleis kommunen får tilgjenge til den aktuelle informasjonen,
- **data bruk,** som handlar om kva kommunen nyttar informasjonen til og korleis han vert nytta,
- **data eksport** om kommunen sine rutinar ved vidareformidling av informasjonen,
- **data lagring,** som handlar om korleis informasjonen vert lagra,
- **data sletting,** som handlar om korleis ein sikrar at informasjon kommunen ikkje har sakleg grunn til å ta vare på, vert sletta.

I alle desse fasane må ein sjå til at data vert handsama med tanke på å trygge deira konfidensialitet, integritet og tilgjenge.

Det kan også vere greitt å ta utgangspunkt i at det er tre ulike område som ein må vere særskilt merksam på :

- **Teknisk tryggleik** omhandlar alt som gjeld den tekniske løysinga for dei systema som handsamar data. Delar av dette området tek dataleverandør seg av, men det er kommunen og den einskilde tilsette sitt ansvar å sjå til at utstyret som vert nytta til eikvar tid har korrekt versjon av programvare, og at ustyret vert nytta i tråd med oppsette rutinar.
- **Fysisk tryggleik** omhandlar alt som gjeld det fysiske miljøet som data vert handsama i. Aktuelle problemstillingar er fysisk tilgjenge til lokalitetar, planløysingar som hindrar utilsikta innsyn, låserutinar mm.
- **Organisatorisk tryggleik** omhandlar alt som handlar om å syte for at berre den/dei som har sakleg fundert krav på tilgjenge til data, får dette. Dataleverandør set opp reglar for kontroll med innsyn, men det er kommunane som må levere og oppdatere informasjonen som er naudsynt for å få dette til.

Nokre problemstillingar når risikovurdering vert gjennomført :

Dette er ei ufullstendig liste over aktuelle problemstillingar, tenkt som ein oppstart på arbeidet med risikovurdering.

	Konfidensialitet :	Integritet :	Tilgjenge :
Data inn :	• *Er det lagt opp til rutinar som sikrar at uvedkomande ikkje får tilgjenge til informasjonen når kommunen mottek denne ?*	• *I kva grad og korleis sikrar ein at informasjonen er korrekt når han vert motteken ?*	• *Er det lagt opp til rutinar som sikrar at informasjonen ved innlegging vert tilgjengeleg for dei som har sakleg grunn for tilgjenge til han – sakshandsamar, til dømes ?*
Data bruk :	• *Er det lagt opp til rutinar som sikrar at uvedkomande ikkje utan vidare kan få tilgjenge til informasjonen når denne vert nytta i samband med forvaltning og tenesteyting ?* • *I kva grad er informasjonen verna av tekniske / fysiske / organisatoriske tiltak?*	• *I kva grad kan data verte endra eller supplert undervegs i ei sakshandsaming?* • *I kva grad kan ein kontrollere at endringar skjer i tråd med gjeldande reglar?* • *I kva grad kan rett forvaltning dokumenterast ?*	• *I kva grad er det lagt opp til at dei som har sakleg grunn for tilgjenge til data, får høve til innsyn i desse som ein del av ordinær saksgang?*
Data lagring :	• *Er det utarbeidd retningsliner for korleis data skal lagrast ?* • *Er desse retningslinene tilfredsstillande ?* • *Korleis samsvarar eigne rutinar med gjeldande retningsliner ?*	• *I kva grad er data verna mot utilsikta eller ulovleg endring ved lagring ?*	• *Er det utarbeidd retningsliner for korleis ein sikrar tilgjenge til lagra data?*
Data sletting :	• *Kva rutinar har ein, og korleis verifisere at desse vert fylgde ?*	• *Kva rutinar har ein, og korleis verifisere at desse vert fylgde ?*	• *Kva rutinar har ein, og korleis verifisere at desse vert fylgde ?*

Eit verktøy for risikovurdering

Det er utarbeidd eit verktøy for risikovurdering i form av ei Excel-arbeidsbok som kommunane kan velje å nytte i arbeidet med risikovurdering. Det tek utgangspunkt i kva data som det er oppgitt at kvar avdeling / teneste forvaltar.

Verktøyet er bygd opp som ei arbeidsbok med seks ark. Dei fem fyrste arka tek for seg dei ulike fasane for data som kommunen forvaltar, slik dette er skildra på side 2 i denne rettleiinga. Det sjette arket er eit oppsummeringsark, der ulike justerande tiltak som vert lagt inn i på dei fem fyrste arka, vert attgitt. På dette arket kan ein kvittere ut for tiltak som er blitt gjennomførte.

På den måten kan dette verktøyet både nyttast som ein dokumentasjon av sjølve risikovurderinga, og som ei sjekkliste for gjennomføring av justerande tiltak.

Verktøyet er laga som ein passordbeskytta mal. Den/dei som har ynskje om å ta det i bruk, kan laste det ned og vende seg til DPO for å få tilsendt passord som opnar dokumentet.

Før ein startar med å bruke verktøyet, må det gjerast eit lite forarbeide :

For å kunne få eit bilete av kor alvorleg ein registrert risiko er, må det seiast noko om kor ofte ein risikabel situasjon oppstår – kva som er frekvensen for denne situasjonen - og kor alvorleg konsekvens denne kan ha. Dette har nær samanheng med korleis informasjonen vert nytta og kva han vert nytta til, og dette vil kunne variere frå avdeling. Difor må kvar avdeling sjølv formulere i forkant kva som vert lagt i dei omgrepa som vert nytta for frekvens og konsekvens. Dette må dokumenterast.

Omgrep knytt til frekvens er

- Sjeldan
- Av og til
- Ofte
- Hyppig

Omgrep knytt til konsekvens er

- Ikkje alvorleg
- Potensielt alvorleg
- Svært alvorleg
- Kritisk