# En veiledning om internkontroll og informasjonssikkerhet

Datatilsynet

**DATATILSYNET** Gateadresse: Tollbugata 3, Oslo | Postadresse: postboks 8177, dep 0034 Oslo
E-post: postkasse@datatilsynet.no | Telefon: 22 39 69 00 | Faks: 22 42 23 50

# Forord
# Informasjonssikkerhet og internkontroll - et ledelsesansvar

Håndtering av opplysninger er i økende grad en del av samfunnets verdiskaping. Opplysninger samles inn, bearbeides, analyseres og inngår som underlag for å stadfeste status, rettigheter og plikter. Ulike opplysninger kan omhandle enkeltpersoner, forretningsprosesser, produktutvikling, strategier og metoder. Felles for alle opplysninger, er at det stilles varierende krav til behandling og beskyttelse. Opplysninger som kan knyttes til individet, skal behandles i samsvar med personopplysningsloven.

Personvern kan ikke avgrenses til informasjonssikkerhet. Like viktig er det å ha en saklig grunn for å behandle personopplysninger. Grunnlag for behandling er normalt basert på lovhjemmel eller samtykke fra den registrerte. Uavhengig av grunnlaget har virksomheten plikt til å informere den registrerte om hvordan den har tenkt å behandle opplysningene. Det betyr at det må informeres om formål, rettigheter og lagringstid for opplysningene. På en måte, kan man si at dette inngår som en del av samfunnskontrakten. Ingen kan ta seg til rette og gjøre hva man vil med opplysningene man forvalter. Tvert imot skal de anvisninger og begrensninger som kontrakten har satt opp, følges.

Virksomheter i offentlig sektor behandler ofte opplysninger som trenger høy grad av beskyttelse. Det ligger i oppgaven som tjenesteleverandør for blant annet vital infrastruktur samt helse og omsorg. Selv om det offentlige er underlagt offentlighetsloven, må det vises utstrakt grad av edruelighet i praktiseringen. Det forvaltes enorme mengder opplysninger som ikke er egnet for offentlighet. Det understreker behovet for å ha klare rammer for hva som skal offentliggjøres og på hvilken måte det skal skje. I praksis er det dessuten stor forskjell på aktiv publisering av opplysninger og det å gi innsyn på begjæring.

Private virksomheter har ofte store utfordringer når det kommer til ansvarsfordeling og kompliserte organisasjonsstrukturer. Dette gjør ofte tilnærmingen til regelverket tilsvarende vanskelig. Personopplysninger kan ikke flyte fritt på tvers av virksomhetsgrensene, selv om eier er den samme.

Datatilsynet forventer ikke alltid at øverste leder har inngående kunnskap om informasjonssikkerhet. Derimot forventes det at personopplysninger er sikret på en forsvarlig måte, og at øverste leder ser etter at dette blir gjort. I praksis betyr det å sørge for at virksomheten har oversikt over hvilke plikter som gjelder, hvordan opplysninger behandles og sikres, at alle rutiner knyttet til dette er godkjent og blir fulgt opp av alle ansatte. Informasjonssikkerhet er ikke et mål i seg selv, men et middel for å oppnå tilfredsstillende kvalitet på virksomhetens tjenester. Tillit er en skjør egenskap som raskt kan bryte sammen. Bare hendelsen rammer noen kraftig nok skal det lite til for å svekke tilliten. Og problemet er at svekket tillit kan ramme hele sektoren og den kan være vanskelig å gjenopprette.

*Publisert november 2009*

# Innholdsfortegnelse

# 1. Innledning

## 1.1 Bakgrunn

De fleste virksomheter behandler personopplysninger i en eller annen form. Dette innebærer at de må følge personopplysningsloven og ha tilfredsstillende rutiner for både bruk og beskyttelse av disse opplysningene. Denne veilederen hjelper deg som er ansvarlig for virksomheten med å bygge opp internkontroll slik at personopplysninger blir behandlet lovlig, sikkert og forsvarlig. De tilhørende malene kan du fylle ut og endre slik at de til sammen utgjør virksomhetens internkontroll.

Behandling av personopplysninger medfører plikter for virksomheten og rettigheter for den registrerte. Ulike opplysninger og ulike formål medfører at ingen virksomhet er lik, og hver virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin situasjon. Det samme gjelder for vedlikehold av internkontrollen; hver virksomhet må tilpasse kontrollrutinene slik at rutiner og tiltak gjenspeiler behovene over tid.

Vær oppmerksom på at også andre regelverk kan stille krav om internkontroll for andre formål enn å sikre forsvarlig håndtering av personopplysninger. Mange virksomheter finner det hensiktsmessig å benytte et felles system for å tilfredsstille ulike internkontrollplikter. Andre regelverk kan også gi konkrete regler for hvordan personopplysninger skal behandles.

Virksomheten plikter etter personopplysningsloven å ha kontroll på sin håndtering av personopplysninger. Det er en samfunnsplikt å sørge for at opplysninger om enkeltpersoner håndteres med nødvendig respekt, noe som også bør være en spore til ryddighet. Å gi et godt inntrykk rundt håndteringen av personopplysninger kan gi virksomheten positiv merverdi, på samme måte som manglende ryddighet kan virke negativt på virksomhetens omdømme.

## 1.2 Hensikten med dokumentet

Dette dokumentet skal, på en enkel og oversiktlig måte, veilede virksomheter gjennom arbeidet med å innføre internkontroll og informasjonssikkerhet slik at en oppnår en forsvarlig og sikker behandling av personopplysninger.

## 1.3 Omfang og målgruppe for dokumentet

Dette dokumentet er utarbeidet for et bredt spekter av virksomheter. Det finnes en egen forkortet utgave av denne veilederen tilpasset mindre virksomheter som kun håndterer personopplysninger om egne ansatte og kunder, for eksempel opplysninger om kontaktpersoner ved salg og leveranse av varer. Denne er tilgjengelig på www.datatilsynet.no.

Virksomheter som håndterer opplysninger om kunder hvor opplysningene anses som sensitive, for eksempel helseopplysninger om klienter, kan ikke benytte den forkortede versjonen.

## 1.4 Forklaring til teksttyper

Referanser til maldokumenter er skrevet i uthevet skrifttype, eksempelvis **Styringsdokument Internkontroll.** I vedlegg 2 finner du en liste over alle malene, og alle er tilgjengelige fra Datatilsynets nettside, www.datatilsynet.no.

Sjekkpunktene oppsummerer de viktigste spørsmålene som må avklares for å ha tilfredsstillende internkontroll og informasjonssikkerhet.

Symbolene som brukes er:

- Definisjon
- Sjekkpunkt
- Lovtekst

# 2. Bakgrunnskunnskap



## 2.1 Krav til internkontroll

Personopplysningsloven [1] stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet. Dette kan oppsummeres som

- rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter
- rutiner og tekniske tiltak for informasjonssikkerhet

## 2.2 Hva er internkontroll?

En virksomhet vil omfattes av mange ulike regelverk. Disse kan for eksempel omhandle helse, miljø, sikkerhet, regnskap eller avgifter. Tilsvarende finnes det regelverk for hvordan personopplysninger skal behandles. De som fastsetter regelverk, forventer at virksomhetene har en systematisk tilnærming i etterlevelsen. Først og fremst må man sette seg inn i de ulike bestemmelsene for å avgjøre hvilke som er relevante i egen virksomhet. Noen bestemmelser har spesiell relevans for ledelsen i virksomhetene, mens andre er ment å påvirke hvordan de ansatte kan utføre sitt arbeide. Det kan også være bestemmelser som gir andre personer eller grupper rettigheter, som virksomheten har plikt til å oppfylle.

Regelverket vil normalt peke på en person som den ansvarlige for å etablere internkontroll. Dette vil likevel ofte være et «sørge for ansvar». I praksis vil den som har ansvaret involvere andre i arbeidet. Dette er viktig av flere grunner. Den ansvarlige kan mangle tilstrekkelig kompetanse eller tid, eller ønsker å gjøre arbeidet mer effektivt. Å involvere flere i utformingen av systemene sikrer både tilgang til riktig kompetanse og gir eierskap til et system som siden skal brukes i de ansattes daglige virke.

For å ivareta krav om en systematisk tilnærming oppretter virksomhetene en internkontroll. Denne består gjerne av tre hovedelementer:

- *Styrende elementer,* som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll.
- *Gjennomførende elementer,* som i hovedsak retter seg mot ansatte. Her finner man beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.
- *Kontrollerende elementer,* som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Internkontroll kan gjerne kalles et kvalitetssystem for etterlevelse av regelverk.

### 2.2.1 Ledelsen

Ledelsen har et spesielt ansvar for å få i stand en systematisk prosess. Hvilke regelverk som er relevante for virksomheten må kartlegges, og ledelsen må sette av tilstrekkelig ressurser til at disse håndteres på en god måte. En kategorisering av pliktene i forhold til de tre nevnte hovedelementene kan være en god start. Ledelsen må være sentral i forhold til utvikling av de styrende elementer i internkontrollen, samt overvåke prosessen rundt utarbeidelse av de gjennomførende og

### § 14 Internkontroll

Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

[1] Personopplysningslovenl § 14

kontrollerende elementene. Det må være samsvar mellom innholdet i de styrende elementene, som ledelsen har fastlagt, og de gjennomførende og kontrollerende elementene. Ledelsen må videre være bevisst på at internkontroll er deres redskap for å styre virksomheten på en forsvarlig og lovlig måte.

### 2.2.2 Ansatte

Internkontroll er utviklet for å bidra til at virksomheten driver sitt virke i samsvar med de lover som gjelder. Brudd på rutiner vil ofte føre til at virksomheten operer i grenseland og i noen tilfeller på feil side av loven. Rutiner må derfor følges. Om man likevel oppdager brudd på disse, bør dette varsles som avvik. En avviksmelding kan bidra til å korrigere uønskede hendelser i virksomheten, men kan også bidra til å utvikle systemet slik at det heller ikke er for stramt.

### 2.2.3 Informasjonssikkerhet

Personopplysningsloven krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, *når* de har behov for disse [2].

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Dersom risikovurderingen avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.

En slik fremgangsmåte som skissert ovenfor vil sammen med tilhørende rutiner kunne utgjøre virksomhetens styringssystem for informasjonssikkerhet. Dette systemet for informasjonssikkerhet vil være en sentral del av virksomhetens internkontroll. Det er utviklet ulike standarder som beskriver hvordan styringssystem for informasjonssikkerhet skal etableres. En måte å etablere dette på er nærmere omtalt i kapittel 5 nedenfor.

## 2.3 Hva er personopplysningsloven og -forskriften?

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven sier at personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene. Personopplysningsloven forkortes ofte *pol*.

Personopplysningsforskriften gir utfyllende og mer detaljerte krav til behandling av personopplysninger. Forskriftens kapittel 3 gir utfyllende bestemmelser om internkontroll, mens kapittel 2 gir utfyllende bestemmelser om informasjonssikkerhet. Personopplysningsforskriften forkortes ofte *pof.*

Eksempler på handlinger som normalt vil krenke personvernet:
- Personopplysninger behandles skjult.
- Flere og mer inngående personopplysninger enn nødvendig samles inn.
- Personopplysninger blir ikke slettet når det ikke lengre er behov for disse.
- Den registrerte får ikke innsyn i opplysninger om seg selv.
- Personopplysningene som behandles er feilaktige.
- Personopplysningene tilflyter uvedkommende.

**PERSONOPPLYSNINGER**

Opplysninger og vurderinger som kan knyttes til en enkeltperson.

[2] Personopplysningsloven § 13

## 2.4 Hva er personopplysninger og sensitive personopplysninger?

**SENSITIVE PERSONOPPLYSNINGER**

Personopplysninger om
- rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- helseforhold
- seksuelle forhold
- medlemskap i fagforeninger

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson, for eksempel navn, adresse, lønn, referanseuttalelser om en person hos et rekrutteringsfirma, oppgavebesvarelser fra skoleelever, klientopplysninger ved krisesentre, skyldneropplysninger i inkassoselskaper, kundeopplysninger hos nettbokhandlere og klientopplysninger i advokatselskaper.

Sensitive personopplysninger er for eksempel informasjon om hvilke sykdommer en person har hatt, medisiner vedkommende bruker, straffedommer, tidligere og pågående rusmisbruk og seksuell legning.

Det knytter seg et særlig behov for vern rundt sensitive personopplysninger. Å bruke denne typen personopplysninger ses normalt på som mer inngripende og regelverket stiller derfor strengere krav til behandling av denne typen opplysninger. Misbruk eller urettmessig spredning av sensitive opplysninger får normalt også større konsekvenser for den enkelte. Opplysninger om personers økonomiske forhold, samt fødselsnummer, er ikke ansett som sensitive personopplysninger. Slike opplysninger oppfattes imidlertid ofte som sensitive av de registrerte, og det er derfor grunn til å vise varsomhet også ved behandling av slike. For bruk av fødselsnummer er det gitt egne bestemmelser i personopplysningsloven § 12.

## 2.5 Dokumentasjon av internkontrollsystemet

Det er et lovpålagt krav at interkontrollsystemet skal være dokumentert [3]. Denne veilederen viser anbefalt fremgangsmåte for å iverksette internkontroll, herunder å sørge for tilfredsstillende informasjonssikkerhet. Veilederen viser til ett sett av maler som kan benyttes av virksomheten. Dokumentene må tilpasses den enkelte virksomhet. Dokumentasjonen bør deles i følgende hoveddeler:

1. Styrende dokumentasjon som ledelsen er ansvarlig for å utarbeide.
2. Gjennomførende dokumentasjon med rutiner og tiltak for daglig drift.
3. Kontrollerende dokumentasjon med rutiner for oppfølging, korrigering og forbedring av internkontroll og informasjonssikkerhet.

Vedlegg 2 har en oversikt over dokumentene som inngår i settet med maler. Bruk denne oversikten som referanse gjennom arbeidet med internkontroll og informasjonssikkerhet. Malene kan lastes ned fra www.datatilsynet.no.

## 2.6 Oppdatering av internkontrollen

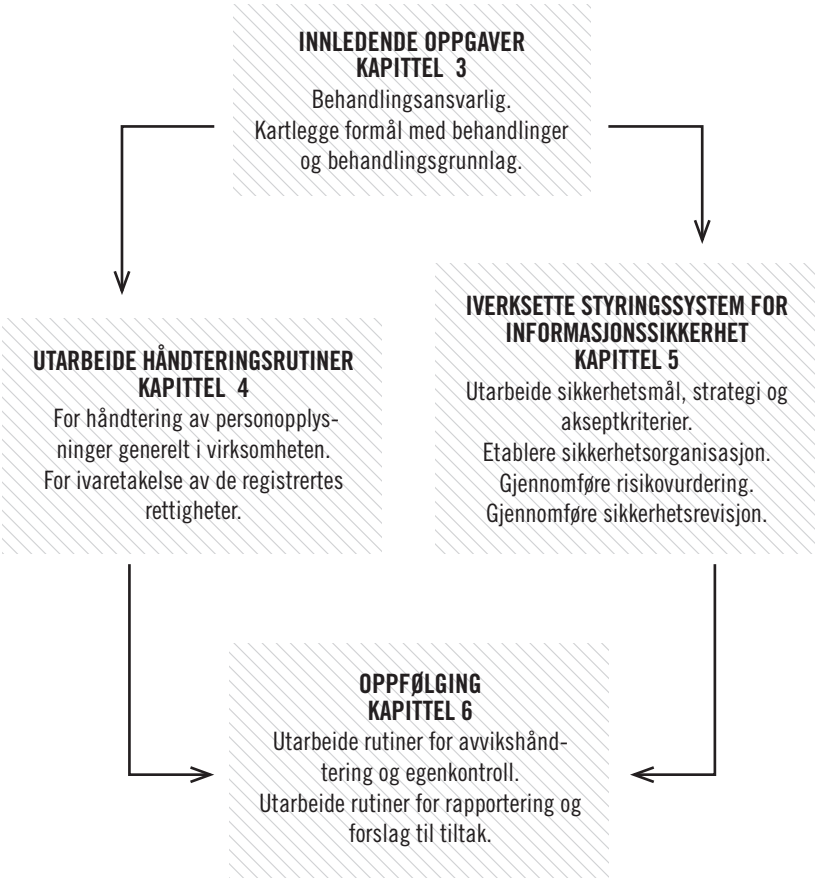
Etter at internkontrollen er etablert og forankret hos behandlingsansvarlig, må man sørge for at den gjøres kjent og etterleves blant de ansatte i virksomheten. Følgende faktorer kan inngå i årlig revisjon av interkontrollsystemet:

- Er virksomhetens mål og strategier de samme, og blir disse nådd?
- Er det endringer i regelverket eller andre rammefaktorer?
- Har risikobildet endret seg?
- Er det nye sikkerhetstrusler som må vurderes?
- Er rutinene kjent og funksjonelle for de ansatte?
- Blir rutinene fulgt?
- Har vi endret behandlingen av personopplysningene?

[3] Personopplysningsloven § 13

Se tabell neste side

## Oppgaver i prosessen




Figuren beskriver prosessen for å etablere internkontroll med henvisning til innholdet i denne veilederen.

Kapittel 3 beskriver aktiviteter som må gjennomføres før man utarbeider konkrete rutiner, prosedyrer og vurderer nødvendige sikkerhetstiltak. Oppgaver i kapittel 3 bør ferdigstilles før man fortsetter med kapittel 4 og 5.

Kapittel 4 beskriver krav til rutiner for håndtering av personopplysninger og gir eksempler på noen slike rutiner.

Aktivitetene i kapittel 4 kan gjennomføres parallelt med aktivitetene i kapittel 5.

Kapittel 5 beskriver etablering av styringssystem for informasjonssikkerhet og gir noen eksempler på dette.

Kapittel 6 beskriver etablering av rutiner for oppfølging og etterlevelse av internkontroll og sikkerhetstiltak, og gir eksempler på prosedyrer som kan tilpasses egen virksomhet.

# 3. Innledende oppgaver for internkontroll



## 3.1 Skaff kunnskap

Virksomheten må selv ha et minimum av kunnskap, og sørge for å ha tilgang til nødvendig kunnskap om personopplysningsloven og personopplysningsforskriften. Slik kunnskap er nødvendig for å kunne starte arbeidet med etablering av internkontroll og tilfredsstillende sikkerhetstiltak. Virksomheten må videre identifisere de lovpålagte pliktene den skal overholde.

**ANNEN RELEVANT INFORMASJON FRA DATATILSYNET:**
På Datatilsynets nettsider finner du oppdatert og relevant informasjon som kan benyttes i arbeidet med internkontroll og informasjonssikkerhet. Du finner blant annet informasjon om

- personvernombudsordningen
- bransjenormer i ulike sektorer
- internkontroll i mindre virksomheter (veileder)
- risikovurdering av informasjonssystem (veileder)
- databehandleravtale

**REGELVERK TILGJENGELIG HOS LOVDATA[4] :**

- personopplysningsloven
- personopplysningsforskriften
- helseregisterloven

**KUNNSKAP**

- ❑ Har virksomhetens leder selv et minimum av kunnskap om personopplysningsloven og personopplysningsforskriften?
- ❑ Har lederen eventuelt tilgang på nødvendig kunnskap og kompetanse?

## 3.2 Virksomhetens leder er behandlingsansvarlig

**BEHANDLINGSANSVARLIG**

Den som bestemmer formålet med behandlingen av personopplysninger og hvilke virkemidler som skal brukes.

Den behandlingsansvarlige er ansvarlig for at personopplysningsloven og personopplysningsforskriften følges. Normalt er den behandlingsansvarlige representert ved virksomhetens daglige leder eller administrerende direktør. Eksempelvis vil rådmannen være behandlingsansvarlig i kommunen. Behandlingsansvaret innebærer blant annet å sørge for at internkontroll etableres og etterleves. I personopplysningsloven[5] er dette beskrevet slik:

«Behandlingsansvarlig er ansvarlig for etablering og vedlikehold av planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet.»

Dette innebærer at den behandlingsansvarlige blant annet må

- bestemme formålet med behandlinger av personopplysninger
- bestemme hvilke virkemidler som skal benyttes
- påse at det er utarbeidet rutiner både for oppfyllelse av virksomhetens plikter og de registrertes rettigheter
- påse at det årlig avsettes tilstrekkelige ressurser, både personalmessige og økonomiske, slik at tilfredsstillende internkontroll opprettholdes

Behandlingsansvarlig skal videre sørge for at blant annet følgende er på plass

- sikkerhetsmål, sikkerhetsstrategi og akseptkriterier
- sikkerhetsorganisasjon
- dokumenterte rutiner og tekniske tiltak for oppfyllelse av sikkerhetsstrategi og akseptkriterier

[4] www.lovdata.no, [5] Personopplysningsloven § 14

Den behandlingsansvarlige kan delegere operativt ansvar for daglige arbeidsoppgaver i forbindelse med internkontroll, men kan ikke delegere ansvaret i forhold til loven.

**VIRKSOMHETENS LEDER**

- ❑ Er virksomhetens leder bevisst på rollen og medfølgende ansvar som behandlingsansvarlig?
- ❑ Har lederen informert resten av ledelsen og annet nøkkelpersonell om sin rolle og sitt ansvar?

## 3.3 Prosjekt for innføring av internkontroll

Mange ulike avdelinger og medarbeidere i virksomheten kan bli involvert i innføring av internkontroll. Virksomheten kan velge å organisere innføringen som et prosjekt. Prosjektleder må i så fall utarbeide en prosjektplan for planlegging og innføring, og være ansvarlig for å nå et definert resultat innen et planlagt tidspunkt. Leveransene til prosjektet er beskrevet i sjekkpunkter videre i denne veilederen. Forventet dokumentasjon ser man av oversikten i vedlegg 2.

**PROSJEKT FOR INNFØRING (VALGFRITT)**

- ❑ Er prosjektleder utnevnt?
- ❑ Er det utarbeidet en prosjektplan med leveranser, milepæler og ressurspersoner?
- ❑ Er alle berørte avdelinger informert?
- ❑ Har de ulike avdelingene akseptert planlagt ressursbruk?
- ❑ Er det besluttet hvem som skal godkjenne leveransene?

## 3.4 Støtteverktøy for gjennomføring av krav i personopplysningsforskriften

Uavhengig av om man velger å organisere innføringen av internkontroll som et prosjekt eller ikke, kan det være nyttig å bruke et verktøy for å følge opp ansvarlige personer og fremdrift for de ulike aktivitetene som skal utføres i virksomheten.

Datilsynet tilbyr et verktøy som letter gjennomføringen av aktivitetene i kapittel 2 og 3 i personopplysningsforskriften, henholdsvis krav til informasjonssikkerhet og til internkontroll. Verktøyet er et regneark som kan bidra til å effektivisere og forenkle koordineringen av innføringsarbeidet i virksomheten.

Verktøyet kan lastes ned fra Datatilsynets nettsted, under sidene for internkontroll.

## 3.5 Kartlegge virksomhetens behandlinger

**BEHANDLING AV PERSONOPPLYSNINGER**

Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Virksomheten skal ha en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse. Oversikten kan føres i **Styringsdokument internkontroll.**

Oversikten er nødvendig for at virksomheten skal kunne ivareta pliktene sine. Oversikten danner også grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi, og vil være underlag ved risikovurderinger.

Tabellen på motstående side er et eksempel på hvordan oversikten over hvilke personopplysninger som behandles, kan se ut. Informasjonen som er listet opp horisontalt må dokumenteres i en slik oversikt, og kan eventuelt suppleres. De vertikale kolonnene tilpasses hver enkelt virksomhet, ut i fra om det er en barnevernsinstitusjon, skole, salgsvirksomhet og så videre. De fleste virksomheter vil uansett behandle personopplysninger om egne ansatte, og føre oversikt over lønn og personal, samt hendelsesregister. Gjennom kapittel 3, 4 og 5 gis det en grundig gjennomgang og utfyllende informasjon om tabellens ulike felter.

# Eksempel på oversikt over personopplysninger som behandles

| Informasjon Formål | Behandlings-grunnlag | Melding/ Konsesjon | Sensitive person-opplysninger | Sikkerhets-tiltak | Lagring og kommunikasjon | Opplysningenes omfang | Avdeling | System-/ dataeier |
|---|---|---|---|---|---|---|---|---|
| Lønn og personal:<br>- lønnsopplys-ninger<br>- personal-opplysninger | Personopplys-ningsloven, § 8f | Unntatt i forskriftens § 7–16 | Nei | | | Ca. 130 ansatte | | |
| Barnevern:<br>- vurdering og tiltak | Barnevern-loven, § 3-1 | Meldt 14.01.2009 | Ja | | | Ca. 68 barn og foresatte | | |
| Helseopplys-ninger:<br>- pasient-journal | Helseper-sonelloven § 39 flg. | Meldt 14.01.2009 | Ja | | | Ca. 413 pasienter | | |
| Elevadminis-trasjon<br>- elever / foresatte<br>- lærere | Opplærings-loven § 13-5 | | Ja | | | Ca. 219 søkere | | |
| Hendelses-register:<br>- logg over brudd | Personopplys-ningsloven, § 13 | Unntatt i forskriftens § 7–11 | Nei | | | Arkivlogg, nettverks-logg og serverlogg, PC-logger | | |
| Kunde-opplysninger<br>- Salgskontakter<br>- Leveranse-kontakter | Personopplys-ningsloven, § 8 a | | Nei | | | Ca. 8000 | | |

### MER SPESIFIKT SKAL OVERSIKTEN GI KORTFATTET INFORMASJON OM

- hvilke opplysninger som behandles og formålet med behandlingen
- hjemmelsgrunnlag for å behandle opplysningene
- klassifikasjon av hvorvidt personopplysningene er sensitive eller ikke
- teknologiske sikkerhetstiltak med angivelse av sone eller nettverk
- hvor opplysningene lagres og om de overføres via eksterne media
- personopplysningenes omfang
- eventuell avdeling som behandler personopplysningene
- systemeier og/eller dataeier

### EKSEMPEL PÅ FREMGANGSMÅTE FOR KARTLEGGING AV BEHANDLINGER:

1. Dersom kartleggingen gjelder en større virksomhet, kan sikkerhetsansvarlig eller prosjektleder sende ut forespørsel om behandling av personopplysninger til hver avdelings-leder: Hva behandles, lagres eller overføres?
2. Vurder svarene. Er det behandlinger som mangler for at virksomheten skal fungere?
3. Skap en hensiktsmessig totaloversikt for virksomheten.

**UTARBEIDELSE AV SKRIFTLIG OVERSIKT OVER ALLE PERSONOPPLYSNINGER SOM BEHANDLES I VIRKSOMHETEN**

- ❑ Er behandling/formål identifisert?
- ❑ Er informasjonen kategorisert i personopplysninger og sensitive personopplysninger?
- ❑ Inkluderer oversikten en beskrivelse av hvilke dataelementer som omfattes?
- ❑ Er det tydelig hvilken avdeling som utfører behandlingene og hvilke ansvarlige som «eier» opplysningene?

## 3.6 Undersøke om behandlingene er lovlige

### 3.6.1 Identifisere formål

Det er ikke tillatt å behandle personopplysninger uten at det er definert et formål med behandlingen[6]. Formålet, eller formålene med de ulike behandlingene, skal være saklig i forhold til virksomheten og må identifiseres og godkjennes av virksomhetsleder.

Behandlingenes overordnede formål føres i dokumentet **Sikkerhetsmål, strategi og akseptkriterier.**

**EKSEMPLER PÅ FORMÅL MED BEHANDLINGER:**

- Akupunktør må ha behandlingshistorikk i klientregister for å yte effektiv behandling.
- Statlig etat må ha registrert ansatte med opplysninger for utbetaling av lønn.
- Advokat som jobber med erstatningssaker relatert til medisinsk behandling må ha klientregister for tilgang til saksfakta.
- Undervisningsinstitusjon må ha kopi av oppgaver eller karakterresultater fra oppgaver for å kunne sette standpunktkarakter og utstede vitnemål.

### 3.6.2 Fastsette behandlingsgrunnlaget

Det er ikke tillatt å behandle personopplysninger uten behandlingsgrunnlag. Personopplysningsloven § 8 gir vilkår for å behandle personopplysninger. Kort oppsummert kreves det at

- virksomheten innhenter samtykke[7] til behandlingen
- behandlingen følger av lov
- behandlingen oppfyller en av nødvendighetbestemmelsene definert i loven

### § 8 Vilkår for å behandle personopplysninger

Personopplysninger kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for
a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås
b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse
c) å vareta den registrertes vitale interesser
d) å utføre en oppgave av allmenn interesse
e) å utøve offentlig myndighet
f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen

For behandling av sensitive personopplysninger må i tillegg personopplysningsloven § 9 være oppfylt. På samme måte som for § 8 må behandlingen som hovedregel enten følge av samtykke, lov eller av en nærmere definert nødvendighetsgrunn. (I tillegg kan det behandles personopplysninger som den registrerte selv frivillig har gjort alminnelig kjent.)

### § 9 Behandling av sensitive personopplysninger

Sensitive personopplysninger kan bare behandles dersom behandlingen oppfyller et av vilkårene i § 8 og
a) den registrerte samtykker i behandlingen
b) det er fastsatt i lov at det er adgang til slik behandling
c) behandlingen er nødvendig for å beskytte en persons vitale interesser, og den registrerte ikke er i stand til å samtykke
d) det utelukkende behandles opplysninger som den registrerte selv frivillig har gjort alminnelig kjent
e) behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav
f) behandlingen er nødvendig for at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter
g) behandlingen er nødvendig for forebyggende sykdomsbehandling, medisinsk diagnose, sykepleie eller pasientbehandling eller for forvaltning av helsetjenester, og opplysningene behandles av helsepersonell med taushetsplikt
h) behandlingen er nødvendig for historiske, statistiske eller vitenskapelige formål, og samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for den enkelte

[6] Personopplysningsloven § 11, [7] Et samtykke er en frivillig, uttrykkelig og informert erklæring fra den registrerte, jf. personopplysningslovens § 2 nr 7

### 3.6.3 Vurdere om formål er i samsvar med hjemmel

De ulike behandlingene som er identifisert må vurderes mot aktuelle behandlingsgrunnlag, jf. punkt 3.6.2.

- Har virksomheten innhentet samtykke til den aktuelle behandlingen? Dette vil for eksempel være tilfelle der en person har takket ja til å delta i et forskningsprosjekt.
- Følger det av lov at behandlingen er tillatt? Dette kan for eksempel være tilfelle for arbeidsgivers mulighet for innsyn i ansattes e-post der den ansatte er langtidssykemeldt [8].
- Er et av de øvrige behandlingsgrunnlagene oppfylt? Dette kan for eksempel være tilfelle for gjennomføring av en kredittvurdering ved søknad om lån til ny bolig [9].

Hvis en av behandlingene ikke faller innenfor eksisterende behandlingsgrunnlag, må virksomheten avvikle behandlingen eller sørge for at det etableres et behandlingsgrunnlag, for eksempel ved innhenting av samtykke. Det samme er tilfelle der innsamlede opplysninger ønskes benyttet til noe nytt. Hvis en bokklubb for eksempel ønsker å selge sitt kunderegister, må de innhente kundenes samtykke til dette dersom dette ikke er gjort ved innmeldingen. Formål, behandlingsgrunnlag og tilhørende meldekrav i forhold til type personopplysninger føres i **Styringsdokument internkontroll.** Overordnede formål med behandlinger skal beskrives i **Sikkerhetsmål og -strategi.**

**BEHANDLINGER**

- ❑ Er formålet med de enkelte behandlingene klarlagt?
- ❑ Har virksomheten gjennomgått alle behandlinger og vurdert behandlingsgrunnlaget?
- ❑ Er de behandlinger som ikke har behandlingsgrunnlag avviklet?
- ❑ Er det alternativt sørget for et behandlingsgrunnlag for disse?
- ❑ Inneholder dokumentet **Sikkerhetsmål, strategi og akseptkriterier** en beskrivelse av overordnet formål med behandlingene?

## 3.7 Beskrive overordnede rammer

Dette kapitlet omfatter ledelsens begrunnelse for behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi i virksomheten. Begrunnelsene og de overordnede føringene skal beskrives i **Styringsdokument internkontroll.** Begrunnelsene omhandler virksomhetens behov for å behandle personopplysningene slik at den kan ivareta sine forpliktelser, herunder levere sine tjenester eller følge opp sine ansatte. De overordnede føringene er krav og plikter som virksomheten blir underlagt fordi den behandler personopplysninger. Slike krav og plikter kan blant annet følge av personvernlovgivningen, av konsesjon fra Datatilsynet eller av annen lovgivning. Andre føringer er sikkerhetsmål og sikkerhetsstrategier. Disse legger begrensninger på anvendelsen av IT for å sikre tilfredsstillende sikkerhet for personopplysningene. Sikkerhetsmål og sikkerhetsstrategier dokumenteres i **Sikkerhetsmål og -strategi.**

**EKSEMPLER – TEKSTLIG BESKRIVELSE AV BEGRUNNELSE FOR BEHANDLING AV PERSONOPPLYSNINGER:**

- Virksomheten leverer advokattjenester. Det er nødvendig for advokatene å lagre opplysninger om klientene og deres saker for å kunne yte klientene gode tjenester.
- Virksomheten er en høyskole og det er nødvendig å lagre informasjon om studentenes obligatoriske oppgaveinnleveringer og andre resultater for å styre undervisningen og gi karakterer. Det er også nødvendig å lagre informasjon om oppnådde karakterer gjennom studiet for å kunne gi studentene vitnemål.

**EKSEMPLER – KRAV OG PLIKTER SOM VIRKSOMHETEN MÅ OPPFYLLE**

- sikkerhetsloven
- forskrift om offentlege arkiv
- forskrift til voksenopplæringsloven, forskrift til lov om voksenopplæring vedrørende tilskudd, regnskap, revisjon og kontroll

**EKSEMPLER – SIKKERHETSMÅL OG -STRATEGIER SOM LEGGER FØRINGER PÅ HVA MAN KAN BRUKE IT TIL I VIRKSOMHETEN OG HVORDAN MAN KAN GJØRE DETTE:**

- Virksomhetens nett skal inndeles i soner der hver sone bare utveksler relevant trafikk med andre interne eller eksterne soner. Eksempler på slike soner er operasjonssentral-, driftsnett- og serversone.
- Brannmurer og tilsvarende sikkerhetsbarrierer skal benyttes for å oppnå et sikkert skille mellom virksomheten og eksterne nett.
- Det skal være elektronisk overvåking av ekstern nettverkstrafikk og mot virksomhetskritiske systemer og nettverk i virksomheten.

Andre føringer er krav til hendelseshåndtering, egenkontroll, avviksbehandling og ledelsens gjennomgang. Dette kan beskrives under strategier i dokumentet **Sikkerhetsmål og –strategi.** Disse områdene er beskrevet nærmere lenger bak i denne veilederen.

[8] Personopplysningsforskriften kapittel 9, [9] Personopplysningsloven § 8 bokstav a

## 3.8 Identifisere plikter

Behandling av personopplysninger medfører plikter for virksomheten. Ulike opplysninger og ulike formål medfører at ingen virksomheter er like. Hver virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin organisasjon.

Gjennom personopplysningsloven § 14 og -forskriftens kapittel 3 er virksomheten pålagt å identifisere alle plikter den er underlagt. Virksomheten må deretter utarbeide rutiner og tiltak som er tilpasset pliktene. Vær oppmerksom på at andre regelverk kan stille krav om internkontroll for andre formål enn å sikre forsvarlig håndtering av personopplysninger, for eksempel ivaretakelse av HMS-krav. Mange virksomheter ser det som hensiktsmessig å benytte et felles styringssystem for å tilfredsstille ulike internkontrollplikter. Andre regelverk kan også gi konkrete regler for hvordan personopplysninger skal behandles.

### IDENTIFISERING AV PLIKTER

- ❑ Har virksomheten identifisert alle plikter de er underlagt som følge av de kartlagte behandlingene av personopplysninger?
- ❑ Er rutiner, utover de som er beskrevet i kapittel 4, etter behov planlagt utarbeidet og iverksatt?

# 4. Rutiner for internkontroll



## 4.1 Generelt om rutiner for internkontroll

Personopplysningsloven stiller krav til internkontroll i form av planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet.

Dette kapitlet beskriver rutiner som er nødvendige for oppfyllelse av virksomhetens plikter og de registrertes rettigheter, samt hvordan rutinene bør utformes. Virksomheten kan ta utgangspunkt i listen nedenfor ved etablering av egne rutiner. Alle rutiner vil imidlertid ikke være relevante for alle virksomheter. En risikovurdering kan dessuten vise at virksomheten har behov for andre rutiner enn dem som er listet opp.

**RUTINER SOM KAN BESKRIVES I DOKUMENTET**

**Rutiner for håndtering av personopplysninger**

- iverksettelse og opphør av behandling
- overholdelse av melde- og eventuell konsesjonsplikt
- sletting av personopplysninger
- utlevering av personopplysninger til andre
- kvalitetssikring av personopplysninger
- innhenting og kontroll av samtykke
- oppfyllelse av plikt til informasjon
- innsyn, retting og supplering
- ivaretakelse av eventuell reservasjonsrett mot automatiserte avgjørelser
- publisering av personopplysninger på Internett
- innsyn i privat e-post og private filområder

Dette dokumentet tilhører kategorien gjennomførende dokumentasjon. Se vedlegg 2 for en oversikt over de ulike kategoriene av dokumentasjon samt hvilke dokumenter som inngår i kategoriene. Rutinene bør utformes i henhold til en felles mal. Rutinene blir da enklere å bruke, og det blir lettere å vurdere om de er fullstendige.

Følgende mal kan benyttes for utforming av rutiner:

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den?
2. Hvem er ansvarlig for å utføre de ulike aktivitetene?
3. Hva skal utføres av de ulike ansvarlige?
4 Hvordan skal aktivitetene utføres?
5. Når skal de ulike aktivitetene utføres, eller under hvilke betingelser?
6. Hva er forventet resultat ved utførelse av rutinen?

## 4.2 Håndtering av samlede personopplysninger

### 4.2.1 Rutine for iverksettelse eller opphør av behandling

Virksomheten skal ha rutiner for iverksettelse og opphør av behandling av personopplysninger. Den behandlingsansvarlige må sørge for at rutinene blir konkretisert.

Følgende elementer inngår i rutine for iverksettelse av behandling

- vurdere behov for ny behandling av personopplysninger
- vurdere formål opp mot behandlingsgrunnlag
- vurdere type opplysninger og gi melding til eller søke om konsesjon fra Datatilsynet, se kapittel 4.2.2
- gjennomføre risikovurdering
- gjennomføre nødvendige sikkerhetstiltak

Følgende elementer inngår i rutine for opphør av behandling

- kontrollere at oversikten over opplysninger stemmer
- vurdere om det er grunnlag for videre oppbevaring med et nytt behandlingsgrunnlag
- slette lagrede personopplysninger det ikke lenger er grunnlag for å behandle

### 4.2.2 Overholdelse av melde- og eventuell konsesjonsplikt

**MELDEPLIKT**

All behandling av personopplysninger er i utgangspunktet meldepliktig, jf. personopplysningsloven § 31. En del behandlinger er imidlertid unntatt i personopplysningsforskriften [10]. Dette gjelder blant annet kunderegistre, personalregistre og foreningers medlemsregistre. Krav til rutiner og sikkerhetstiltak gjelder selv om behandlingen er unntatt meldeplikt.

[10] Personopplysningsforskriften kapittel 7

**EKSEMPEL – RUTINE FOR MELDING OM BEHANDLING AV PERSONOPPLYSNINGER:**

- Den behandlingsansvarlige skal gi melding til Datatilsynet før behandling starter. Dette gjelder behandling av personopplysninger med elektroniske hjelpemidler, og før opprettelse av manuelt personregister som inneholder sensitive personopplysninger.
- Den behandlingsansvarlige skal gi melding til Datatilsynet før det iverksettes behandling av personopplysninger som går ut over rammen for behandling som tidligere er meldt.
- Meldingen skal gis senest 30 dager før behandlingen eller endret behandling tar til.
- Tre år etter at forrige melding ble gitt skal det gis ny melding, selv om det ikke har skjedd endring av behandlinger.

**KONSESJONSPLIKT**

Noen behandlinger er konsesjonspliktige, og skal dermed ikke meldes. Meldeplikten er her erstattet av konsesjonssøknad til Datatilsynet. Dette gjelder som hovedregel all behandling av sensitive personopplysninger som føres elektronisk. I tillegg er enkelte behandlinger som i utgangspunktet er meldepliktige, gjort konsesjonspliktige ved forskrift. Dette dreier seg om behandling av personopplysinger innen telesektoren, forsikringsbransjen og i banker og finansinstitusjoner. Noen behandlinger av sensitive opplysninger er likevel unntatt konsesjonsplikt. Behandlinger som er unntatt konsesjonsplikt, har meldeplikt dersom ikke annet er bestemt.

Detaljerte opplysninger om konsesjonsplikten finnes i §§ 33 – 35 i personopplysningsloven og i kapittel 7 i personopplysningsforskriften.

Datatilsynet har opprettet en tjeneste på www.datatilsynet.no for nedlasting av søknadsskjema og innsending av elektronisk meldeskjema. Denne tjenesten gir tilgang til skjema samt et veiledningsdokument, og er rask og enkel å bruke.

**EKSEMPEL – RUTINE FOR SØKING OM KONSESJON FOR BEHANDLING AV PERSONOPPLYSNINGER:**

- Behandlingsansvarlig skal søke Datatilsynet om konsesjon før konsesjonspliktig behandling av personopplysninger starter.
- Behandling kan ikke starte før konsesjon er gitt.

## 4.2.3 Rutiner for sletting av personopplysninger

Krav til sletting av personopplysninger er beskrevet i § 28 i personopplysningsloven. Bestemmelsen forbyr lagring av unødvendige personopplysninger.

Bestemmelsen slår fast at:
«den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.»

Vær oppmerksom på at en særlov kan gi andre regler for sletting.

Virksomheten skal ha rutiner for sletting av personopplysninger som det ikke lenger er nødvendig å lagre. Krav til sletting kan for eksempel inntreffe på grunn av en organisatorisk endring, bortfall av formål eller at tidskrav for lagring utløper. Historiske, statistiske eller vitenskapelige formål kan åpne for lengre lagring under visse forutsetninger.

Følgende elementer inngår i rutine for sletting av personopplysninger og må konkretiseres av den behandlingsansvarlige:

- Vurdere krav til sletting av personopplysninger ved endringer i virksomhetens tjenester, organisering og informasjonssystemer.
- Jevnlig, for eksempel månedlig, vurdere krav til sletting av personopplysninger basert på oversikt over opplysninger og lagringstid.
- Godkjenne sletting av utvalgte opplysninger.
- Utføre sletting av utvalgte opplysninger i alle kopier.

**EKSEMPEL PÅ RUTINE FOR SLETTING:**

Det er viktig at virksomheten konkret vurderer frister for sletting, også i forhold til krav i andre lover om oppbevaring. Følgende rutine er kun et eksempel:

**1) SALGSSJEF ER ANSVARLIG FOR PERSONOPPLYSNINGER OM KUNDER. SALGSSJEF SKAL:**

- Sørge for at personopplysninger relatert til kundeforholdet slettes etter tre års inaktivitet i kundeforholdet, med mindre skriftlig samtykke til fortsatt lagring er innhentet fra kunden.
- Påse at det ikke lagres flere personopplysninger om kunder enn nødvendig for formålet.
- Holde en oversikt over når det sist var aktivitet i de ulike kundeforholdene.
- Gi IT-driftsansvarlig beskjed om hvilke opplysninger som skal slettes og når de skal slettes.
- Motta bekreftelse fra IT-driftsansvarlig på at opplysningene er slettet.

Rutinen gjelder ikke opplysninger i virksomhetens regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

**2) PERSONALSJEF ER ANSVARLIG FOR PERSONOPPLYSNINGER OM ANSATTE. PERSONALSJEF SKAL:**

- Fjerne unødvendige opplysninger etter gjennomføring av personalsamtale.
- Fjerne unødvendige opplysninger ved avslutning av arbeidsforholdet.
- Gjennomføre ny vurdering av behov for fortsatt lagring ett år etter avslutning av arbeidsforholdet.
- Påse at det ikke lagres personopplysninger om ansatte som ikke er relevante for administrasjon av arbeidsforholdet.
- Gi IT-driftsansvarlig beskjed om hvilke opplysninger som skal slettes og når de skal slettes.
- Motta bekreftelse fra IT-driftsansvarlig på at opplysningene er slettet.

Rutinen gjelder ikke opplysninger i virksomhetens regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

### 4.2.4 Rutiner for utlevering av personopplysninger til andre

Dette kapitlet omfatter rutiner for utlevering av personopplysninger til andre behandlingsansvarlige. Utleveringen er i seg selv en behandling som krever behandlingsgrunnlag etter personopplysningsloven. Dersom ikke annet behandlingsgrunnlag finnes, må den behandlingsansvarlige som ønsker å utlevere data ha samtykke fra de/den registrerte for å utlevere opplysningene.

Utlevering omfatter ikke bruk av eksisterende personopplysninger til ny behandling innenfor samme virksomhet, men også i slike tilfeller må man sørge for et behandlingsgrunnlag. Utlevering omfatter heller ikke oversendelse av personopplysninger til databehandlere. Innsyn i egne personopplysninger omfattes ikke av dette kapitlet. Slikt innsyn er omtalt i kapittel 4.3.3.

Følgende elementer inngår i rutine for utlevering av personopplysninger og må konkretiseres av den behandlingsansvarlige:

- Behandlingsansvarlig kan delegere myndighet til leder eller medarbeider i virksomheten som skal godkjenne utlevering av personopplysninger. Slik delegering av myndighet skal være dokumentert. Dersom dette ikke er gjort er det kun virksomhetens leder selv som kan godkjenne utlevering.
- Det skal bestemmes hvem som skal utføre oppgaven, eventuelt oppgavene, i forbindelse med utlevering.
- På forespørsel om utlevering skal det vurderes om forespurte personopplysninger kan utleveres. Som ved andre behandlinger, skal utleveringen være formålsbestemt og tilfredsstille krav til behandlingsgrunnlag i personopplysningsloven § 8 og eventuelt § 9.

### 4.2.5 Rutiner for kvalitetssikring av personopplysninger

Opplysningene skal være korrekte og oppdaterte i forhold til formålet med behandlingen [11].

**EKSEMPEL – FREMGANGSMÅTE FOR OPPDATERING AV PERSONOPPLYSNINGER FRA REGISTRERTE:**

- Teknisk funksjon i nettsted som krever at bruker bekrefter, eventuelt oppdaterer egne kontaktopplysninger ved pålogging, må oppdateres jevnlig f.eks. en gang per halvår.

**DOKUMENTERTE RUTINER**

- ❑ Har virksomheten dokumenterte rutiner for iverksettelse og opphør av behandling av personopplysninger?
- ❑ Finnes det dokumenterte rutiner for overholdelse av meldeplikt og eventuelt konsesjonsplikt?
- ❑ Eksisterer det dokumenterte rutiner for sletting av personopplysninger?
- ❑ Har virksomheten dokumenterte rutiner for jevnlig oppdatering av database med personopplysninger?

## 4.3 Rutiner relatert til person

### 4.3.1 Innhenting og kontroll av samtykke

Behandling av personopplysninger bør i størst mulig utstrekning basere seg på samtykke fra den registrerte. Dette gir godt personvern ved at den registrerte har bedre kontroll med egne opplysninger. Samtykket må være frivillig, uttrykkelig og informert. Loven stiller ingen formkrav til samtykket, men Datatilsynet anbefaler at det innhentes skriftlig. Samtykke i skriftlig form vil minske bevisproblemer i situasjoner hvor det er tvil om hva den registrerte har samtykket til. Et samtykke kan trekkes tilbake når som helst.

[11] Personopplysningsloven § 11

**EKSEMPEL – INNHENTING AV SAMTYKKE FØR REGISTRERING PÅ NETTHANDELSSTED**

- kunde går inn på netthandelssted for å lese produktnyheter
- nettstedet sender et vindu/skjermbilde med forespørsel til kunde om å registrere seg med e-postadresse for å motta produktnyheter
- nettsted kan ikke sende reklame per e-post til private mottakere uten at mottakeren har samtykket

## 4.3.2 Oppfyllelse av plikt til informasjon ved innsamling av personopplysninger

Den behandlingsansvarlige er pålagt å informere den registrerte om behandlingen som igangsettes [12)].

Der personopplysningene innhentes fra den registrerte selv skal informasjonen gis før behandlingen tar til. Informasjon skal gis uoppfordret, uten at den registrerte krever det, og uten kostnader for den registrerte [13)].

Plikt til å informere når det samles inn opplysninger fra den registrerte er beskrevet i personopplysningsloven § 19.

## 4.3.3 Rutiner for innsyn, retting og supplering

**INNSYN**

Rett til innsyn i personopplysninger er beskrevet i personopplysningsloven § 18. Virksomheten skal ha

---

### § 18 Rett til innsyn

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling
a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant
b) hvem som har det daglige ansvaret for å oppfylle den handlingsansvarliges plikter
c) formålet med behandlingen
d) beskrivelser av hvilke typer personopplysninger som behandles
e) hvor opplysningene er hentet fra
f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om
a) hvilke opplysninger om den registrerte som behandles
b) sikkerhetstiltakene ved behandlingen, så langt innsyn ikke svekker sikkerheten

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser. Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte.

### § 19 Informasjonsplikt når det samles inn opplysninger fra den registrerte

Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om
a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant
b) formålet med behandlingen
c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker
d) det er frivillig å gi fra seg opplysningene
e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28

Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd.

### § 20 Informasjonsplikt når det samles inn opplysninger fra andre enn den registrerte

En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 19 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.

Den registrerte har ikke krav på varsel etter første ledd dersom
a) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov
b) varsling er umulig eller uforholdsmessig vanskelig
c) det er på det rene at den registrerte allerede kjenner til informasjonen varselet skal inneholde

Når varsling unnlates med hjemmel i bokstav b, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene.

[12)] Personopplysningsloven §§ 19 og 20, [13)] Personopplysningsloven § 17

rutine for behandling av forespørsel om innsyn fra mulig registrerte.

Følgende elementer inngår i rutine for behandling av forespørsel om innsyn og må konkretiseres av den behandlingsansvarlige
- mottak av forespørsel om innsyn fra mulig registrert person
- eventuelt be om skriftlig bekreftelse på forespørsel
- formidling av forespørselen til aktuelle system- eller dataeiere
- gi melding til den som ba om innsyn dersom forespørselen ga negativt resultat

Dersom den som ba om innsyn er registrert:
- Skrive ut og eventuelt utarbeide informasjon fra aktuelle systemer som spesifisert i personopplysningsloven § 18, i henhold til intern rutine.
- Samle informasjon fra aktuelle systemer og oversende til den som forespør.

#### RETTING OG SUPPLERING

Personopplysninger skal være tilstrekkelige og relevante for formålet med behandlingen [14)]. Kravet til relevans trekker opp en ytre grense for hvilke personopplysninger som kan tas med i behandlingen, og kan ikke fravikes gjennom samtykke fra den registrerte. Kravet til tilstrekkelighet innebærer at man må ha nok opplysninger for å kunne ivareta formålet med behandlingen.

Virksomheten skal ha rutine for behandling av forespørsel om retting og supplering for en registrert. Det kan også være behov for retting i henhold til lovens § 27. Bestemmelsen slår blant annet fast:

«Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene.»

Virksomheten skal også ha rutiner for retting når det avdekkes feil internt i virksomheten. Dersom virksomheten har behandlet personopplysninger som den ikke har adgang til å behandle skal retting som hovedregel skje ved at opplysningene slettes.

Følgende elementer inngår i rutiner for behandling av forespørsel om retting og supplering, og må konkretiseres av den behandlingsansvarlige
- mottak av forespørsel om retting eller supplering for en registrert
- formidling av forespørsel til aktuelle system-/dataeiere
- verifisere korrekthet av forespurte endringer av opplysninger
- hvis verifisert, utstede arbeidsordre for oppdatering av systemer
- bekrefte skriftlig til den som forespurte om endringer som er gjort

## 4.3.4 Ivaretakelse av eventuell reservasjonsrett mot automatiserte avgjørelser

I den grad den behandlingsansvarlige utfører fullt automatiserte avgjørelser i forhold til den registrerte, kan den registrerte kreve manuell behandling av saken/avgjørelsen. Det er gjort unntak der den registrertes personverninteresser ivaretas på en tilstrekkelig måte og avgjørelsen er hjemlet i lov eller knytter seg til oppfyllelse av kontrakt [15)]. Den behandlingsansvarlige skal ha rutiner for manuell behandling dersom det er aktuelt.

## 4.3.5 Innsyn i privat e-post og private filområder

Arbeidsgivers adgang til å foreta innsyn i ansattes private e-post og filer er regulert i personopplysningsforskriften kapittel 9. I og med at ulike virksomheter har ulike behov anbefaler Datatilsynet at virksomheten utarbeider utfyllende rutiner for når innsyn kan bli aktuelt og hvordan innsyn skal gjennomføres. Slike bestemmelser kan ikke fravike bestemmelsene i forskriftens kapittel 9 til ugunst for arbeidstaker. Instruksen kan overprøves av Datatilsynet. Dersom virksomheten ikke har utarbeidet utfyllende bestemmelser, vil innsyn måtte avgjøres ut fra tolking av personopplysningsforskriftens bestemmelser.

#### DOKUMENTERTE RUTINER 2

- ❑ Finnes det dokumenterte rutiner for innhenting og kontroll av samtykke?
- ❑ Er dokumenterte rutiner for oppfyllelse av plikt til informasjon på plass?
- ❑ Har virksomheten utarbeidet dokumenterte rutiner for innsyn, retting og supplering?
- ❑ Er det utarbeidet dokumenterte rutiner for ivaretakelse av eventuell reservasjonsrett mot automatiserte avgjørelser?
- ❑ Finnes det dokumenterte rutiner for innsyn i privat e-post og private filområder? (ikke obligatorisk)

[14)] Personopplysningsloven § 11, [15)] Personopplysningsloven § 25

# 5. Informasjonssikkerhet



## 5.1 Hva er informasjonssikkerhet?

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Personopplysninger kan eksistere i mange former. De kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektroniske media eller formidles muntlig. Uansett hvilken form informasjonen har eller hvilket middel den formidles gjennom og lagres på, bør den alltid beskyttes på en tilfredsstillende måte.

**INFORMASJONSSIKKERHET OMFATTER HER BESKYTTELSE AV**
- konfidensialitet – hindre uvedkommende i å få tilgang på opplysningene
- integritet – ingen uautorisert eller utilsiktet endring av opplysninger
- tilgjengelighet – opplysningene er tilgjengelige når tilgang er nødvendig

I stadig større grad står organisasjoner og deres informasjonssystemer overfor en rekke sikkerhetstrusler, for eksempel datasvindel, spionasje, sabotasje og hærverk. Skadelige aktiviteter, som spredning av datavirus, datakriminalitet og tjenesteblokkering, er blitt mer omfattende, ambisiøse og stadig mer sofistikerte.

Informasjonssikkerhet oppnås ved hjelp av planlagte og systematiske tiltak. De tiltak som etableres, skal være både organisatoriske og tekniske. Sikkerhetstiltakene og selve informasjonssystemet skal dokumenteres og inngå som en del av internkontrollen i virksomheten. Sikkerhetsdokumentasjonen kan følge strukturen som beskrevet i kapittel 2.5.

Ved innføring av internkontroll, må virksomheten først identifisere hvilke personopplysninger som behandles. Deretter må det utarbeides en risikoanalyse med vurderinger av risiko for at en uønsket hendelse skjer, og eventuelle konsekvenser av dette.

**RISIKOVURDERING SKAL GI FØLGENDE RESULTAT**
- oversikt over identifiserte trusler
- angivelse av sannsynlighet for at en uønsket hendelse kan inntreffe
- angivelse av konsekvenser av en uønsket hendelse
- resultat fra analyse av sikkerhetstiltakenes effekt i forhold til risiko

Risikovurderingen danner grunnlag for iverksettelse av nødvendige sikkerhetstiltak og inngår i underlag for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten. Sikkerhetstiltakene må stå i forhold til vurdert risiko og sørge for at disse er innenfor de akseptkriterier virksomheten har fastlagt. Dersom risikovurderingen viser behov for ytterlige tiltak, planlegges og gjennomføres disse for å skape et tilfredsstillende sikkerhetsnivå. Avslutningsvis lages rutiner og prosedyrer som jevnlig gjennomføres, for å kontrollere at tiltakene virker etter hensikten. Denne fremgangsmåten og tilhørende rutiner kan organiseres og dokumenteres i et styringssystem for informasjonssikkerhet som en del av internkontrollen.

## 5.2 Sikkerhetsmål og sikkerhetsstrategi

Fra innledende aktiviteter er følgende fylt inn i **Sikkerhetsmål og -strategi**
- begrunnelse for behandling av personopplysninger
- formål med de ulike behandlinger (overordnet)
- retningslinjer for bruk av IT til behandling av personopplysninger
- retningslinjer for organisering av sikkerhet

Internkontrollen skal fange opp alle krav til informasjonssikkerhet i § 2-1 i personopplysningsforskriften. Formålet er å oppfylle personopplysningslovens krav om tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. På bakgrunn av dette skal det utarbeides sikkerhetsmål, som inkluderer mål, sikkerhetsstrategi, og hva som skal gjøres for å nå målene. Grunnlaget er lagt i kapittel 3.7, overordnede rammer. **Sikkerhetsmål og -strategi** er en del av styrende dokumentasjon og ledelsens ansvar.

### 5.2.1 Sikkerhetsmål

Sikkerhetsmålene omfatter ledelsens beslutninger om hva informasjonsteknologien skal brukes til i virksomheten og hvordan den skal benyttes for å nå virksomhetens øvrige mål. Sikkerhetsmål vil således utgjøre en del av virksomhetens beskrivelse av sin totale målsetting. Dokumentet **Sikkerhetsmål og –strategi** oppdateres med konkrete sikkerhetsmål for virksomheten. Det er gitt

utfyllende eksempler i denne malen. Sikkerhetsmålene bør i størst mulig grad være målbare, men dette er ikke alltid enkelt. Uansett skal de være retningsgivende for strategier.

**EKSEMPLER:**
- Krav i relevante lover og forskrifter skal etterleves.
- Selskapets informasjonsbehandling skal beskyttes mot alle identifiserte trusler – både interne og eksterne, samt tilsiktede og utilsiktede.
- Det skal være etablert rutiner for å håndtere uønskede hendelser.
- Medarbeidere som bruker virksomhetens informasjonssystemer skal ha tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov.

### 5.2.2 Sikkerhetsstrategi

Sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette går på fordeling av arbeidsoppgaver mellom ledelse og driftspersonell, og beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Forholdet mellom ledelse, driftspersonell, sikkerhetspersonell og den enkelte bruker må avklares her. Sikkerhetsstrategien skal gjøre rede for organisatoriske og tekniske strategiske valg, og må være utformet på en måte som gjør at de ansatte forstår hva ledelsen har bestemt. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene. Det kan velges ulike strategier for å tilfredsstille samme mål.

**EKSEMPLER:**
- Egenkontroll skal utføres regelmessig i henhold til systematiserte rutiner.
- Alle som får tilgang til fortrolige opplysninger om bedriften eller bedriftens kunder, skal signere en taushetserklæring.
- Nettverkstrafikk mot virksomheten fra Internett skal kontrolleres.

## 5.3 Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering. Gjennomgangen utføres i henhold til rutine beskrevet i dokumentet **Ledelsens gjennomgang**.

Ved ledelsens gjennomgang deltar representanter fra virksomhetens øverste ledelse sammen med sikkerhetsansvarlig og IT-driftsleder. Praktisk organisering av gjennomgangen, utarbeidelse av rapport og iverksetting av eventuelle tiltak kan med fordel legges til sikkerhetsansvarlig.

I ledelsens gjennomgang av informasjonssystemet skal blant annet følgende vurderes
- resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet
- endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder
  - endringer i offentlige sikkerhetskrav
  - endringer i de personopplysninger virksomheten skal behandle
  - endringer i trusselbildet som blant annet beskrevet i rapport fra utførte risikovurderinger
- om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet
- overordnet behandling av alvorlige avvik og hendelser

**MALDOKUMENT SIKKERHETSMÅL OG –STRATEGI**

- ❑ Inneholder dokumentet begrunnelse og formål med behandling av personopplysninger?
- ❑ Inkluderer dokumentet ledelsens mål for bruk av informasjonsteknologi?
- ❑ Er sikkerhetsmålene inkludert i dokumentet?
- ❑ Går sikkerhetsstrategien frem av dokumentet?

## § 13 Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

## Eksempel på rapport fra ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten

| Rapport fra ledelsens gjennomgang år xxxx | **VIRKSOMHET:** XX | **SKREVET AV:** Sikkerhetsansvarlig | **DATO:** 1.12.xxxx | **ARKIVREF:** xx.yyyy |
|---|---|---|---|---|
| **DELTAGERE:**<br>Virksomhetsleder NN<br>Sikkerhetsansvarlig NN<br>IT-driftsleder NN | | | | |
| **DISTRIBUSJON:** Møtedeltakerne | | | | |

| **SAKNR.** | **SAK** | **AKSJON** | **ANSV./ FRIST** |
|---|---|---|---|
| **1/XX** | Rapporter fra utførte sikkerhetsrevisjoner.<br>Rapportene fra sikkerhetsrevisjoner ble lagt fram uten merknader. | | |
| **2/XX** | Behandling av registrerte sikkerhetsbrudd og logger.<br><br>Innbrudd på nettsted bør gi endret sikkerhetsstrategi. | Det innhentes bistand til endring. | IT-driftsleder 15.12.xxxx |
| **3/XX** | Behandling av foreslåtte nye løsninger.<br>Prosjektforslaget for bruk av hjemmekontor ble godkjent. | | |

Resultatene dokumenteres i rapport i henhold til mal i dokumentet **Ledelsens gjennomgang.**

### LEDELSENS GJENNOMGANG

- ❑ Inkluderer dokumentet **Ledelsens gjennomgang** en rutine for ledelsens årlige gjennomgang av informasjonssystemet og informasjonssikkerheten i virksomheten?
- ❑ Er ansvar for forberedelse og innkalling på plass?
- ❑ Er det etablert en mal til rapport for dokumentet **Ledelsens gjennomgang?**

## 5.4 Sikkerhetsorganisasjon

Personopplysningsforskriften § 2-7 stiller krav til klare ansvars- og myndighetsforhold for bruk av informasjonssystemer som behandler personopplysninger. Det betyr at det må nedsettes en sikkerhetsorganisasjon, og at denne skal dokumenteres. Bruk dokumentet **Sikkerhetsorganisasjon** for å beskrive sikkerhetsorganisasjonen. Klare ansvars- og myndighetsforhold etableres med utgangspunkt i beslutninger tatt av virksomhetens ledelse (sikkerhetsstrategien).

Ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeidet (sikkerhetsledelse) må klarlegges. I mindre organisasjoner kan det være samme person som ivaretar disse oppgavene. For større organisasjoner fremlegges organisasjonskart som viser de nevnte funksjonene og deres plassering i forhold til ledelsen og virksomheten for øvrig. Ansvar og myndighet skal fremgå tydelig.

**SIKKERHETSORGANISASJON**

Er sikkerhetsorganisajonen dokumentert med
- ❑ rollebeskrivelser
- ❑ myndighet
- ❑ ansvarsområder
- ❑ plikter for virksomhetsleder til driftsansvarlig, for alle de ulike systemene som behandler personopplysninger?

## 5.5 Akseptabelt risikonivå

Personopplysningsforskriften § 2–4 stiller krav til at det skal gjennomføres risikovurderinger, for å kartlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd. En forutsetning for å kunne ha en forsvarlig risikostyring er at det finnes noen kriterier å styre etter. Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et på forhånd akseptert nivå. Akseptkriteriene vil videre påvirkes av ytre rammevilkår og lovpålagte krav.

Akseptabelt risikonivå skal fastlegges for alle sikkerhetsbehov, herunder konfidensialitet, tilgjengelighet og integritet. I noen situasjoner kan disse tre behovene komme i konflikt med hverandre. 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 i beskrivelsen av akseptabelt risikonivå.

Beslutning om akseptabelt risikonivå skal blant annet uttrykkes i virksomhetens sikkerhetsmål, beskrevet i **Sikkerhetsmål og -strategi**. Sikkerhetsmålet skal, på et overordnet nivå, beskrive formålet med bruken av informasjonsteknologi og angi sikkerhetsbehov med hensyn til konfidensialitet, tilgjengelighet og integritet. 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 sannsynlighet og konsekvens. Beskrivelsen må angi prioritering mellom forskjellige sikkerhetsbehov, og – på overordnet nivå – beskrive risikoreduserende tiltak. Detaljert beskrivelse av akseptabelt risikonivå skal inngå i underlag for gjennomføring av risikovurdering.

**EKSEMPLER PÅ BESKRIVELSE AV AKSEPTABELT RISIKONIVÅ:**
«Sikkerhetstiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne forårsake uønskede hendelser som medfører konsekvenser for enkeltmenneskers personvern. Egne medarbeidere skal ha tilstrekkelig kjennskap til hvilke sikkerhetsbestemmelser som gjelder i virksomheten slik at uønskede hendelser reduseres til et minimum.»

«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.»

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

**FLERE EKSEMPLER**

**KONFIDENSIALITET:**
- Sikkerhetskopier som bringes ut av virksomheten skal være kryptert, slik at tap av disse ikke får konsekvenser for konfidensialiteten uten at både krypteringsnøkkel og sikkerhetskopi kommer på avveie.
- Sensitive personopplysninger fra fagsystem skal ikke kunne utleveres gjennom informasjonssystemet ved uaktsomhet.

**INTEGRITET:**
- Sensitive personopplysninger i fagsystemer skal ikke kunne endres uten at dette er sporbart.

**TILGJENGELIGHET:**
- Det tillates maksimalt ett driftsavbrudd med varighet over en arbeidsdag per år.
- Ved total skade på lokal infrastruktur aksepteres maksimalt tap av de siste syv dagers arbeid. Eldre data skal kunne gjenopprettes ved hjelp av sikkerhetskopi lagret eksternt. Slik gjenoppretting skal kunne gjøres uten data, dokumentasjon eller krypteringsnøkler lagret i virksomheten.

**AKSEPTABELT RISIKONIVÅ**

- ❑ Er overordnet akseptabelt risikonivå beskrevet i Sikkerhetsmål og -strategi?
- ❑ Er detaljert akseptabelt risikonivå beskrevet i form av akseptable og uakseptable hendelser i forbindelse med risikovurdering, i dokumentet Risikovurdering?

## 5.6 Gjennomføre risikovurdering

Virksomheten skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i informasjonssystemet eller endringer i trusselbildet. Risiko betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse.

Eksempler på endringer som krever ny risikovurdering og godkjenning fra virksomhetens ledelse
- endring i klassifisering av opplysninger
- endringer i trusselbildet
- organisasjonsendringer
- endret tilkopling til sikret sone
- endret tilkopling til eksterne datanett
- ekstern overføring av nye typer opplysninger eller til nye partnere

Ledergruppen i virksomheten, med tillegg av IT-driftsansvarlig og sikkerhetsansvarlig, skal minst en gang årlig gjennomføre risikovurdering bl.a. i forbindelse med vurdering av endringer i trusselbildet og/eller planlagte endringer i informasjonssystemet. Risikovurderingen baseres blant annet på personopplysningsforskriften § 2 – 1, forholdsmessige krav om sikring av personopplysninger. Opplysninger av ulike typer/kategorier skal beskyttes godt nok. Beskyttelsestiltak koster penger og innsats, og i tillegg reduseres ofte tilgjengeligheten. Derfor segmenteres nettverk og systemer slik at man ikke beskytter opplysninger mer omfattende enn nødvendig.

Formålet med risikovurdering er å sikre at den risiko som avdekkes ved behandling av personopplysninger er innenfor de akseptkriterier virksomheten har fastlagt. Risikovurderingen danner grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten. Virksomhetens ledelse har ansvar for iverksetting av risikovurdering. Resultat fra analysen rapporteres til virksomhetens ledelse. Rutine for risikovurdering beskrives i maldokumentet **Risikovurdering**.

**EKSEMPLER PÅ ELEMENTER SOM INNGÅR I RISIKOVURDERING**
- planlegging og oppstart
- avgrensing av analyseobjekt
- beskrivelse av trusler mot informasjonssikkerheten med hensyn til
  - konfidensialitet
  - integritet
  - tilgjengelighet
- årsaksanalyse – vurdering av hvordan en uønsket hendelse kan inntreffe
- konsekvensanalyse – vurdering av de følger en uønsket hendelse kan medføre
- frekvensanalyse – vurdering av sannsynlighet for at en uønsket hendelse kan inntreffe
- beskrivelse av risiko
- vurdering av hvorvidt den avdekkede risiko er innenfor akseptkriteriene
- vurdering av sikkerhetstiltak

### 5.6.1 Uønskede hendelser

En trussel er en mulig uønsket hendelse som kan inntreffe. En hendelse er en handling eller tilstandsendring som kan utsette verdier for risiko – i form av mangelfull konfidensialitet, integritet eller tilgjengelighet.

**EKSEMPLER PÅ KONSEKVENSBESKRIVELSER**

**UTLEVERING, TAP AV LAGRINGSMEDIER, UTSENDING VIA E-POST MED MER**
- kan tilbakeføres
- permanent

**ENDRING**
- sporbar og kan rettes
- sporbar og permanent
- ikke sporbar

## Eksempel – Elektronisk klientregister

| KONSEKVENS | KONFIDENSIALITET | INTEGRITET | TILGJENGELIGHET I ÅPNINGSTID |
|---|---|---|---|
| Katastrofal (K=4) | X | X | |
| Stor (K=3) | | | X |
| Moderat (K=2) | | | |
| Liten (K=1) | | | |

Klientregisteret inneholder sensitive personopplysninger.

## Eksempel – Regnskapssystem

| KONSEKVENS | KONFIDENSIALITET | INTEGRITET | TILGJENGELIGHET I ÅPNINGSTID |
|---|---|---|---|
| Katastrofal (K=4) | | | |
| Stor (K=3) | | X | |
| Moderat (K=2) | X | | X |
| Liten (K=1) | | | |

Personopplysninger kan ha moderat på konfidensialitet og stor på integritet. Det gir potensial for lavere kostnader til beskyttelse av opplysningene enn om det hadde vært stor på begge, eller alle tre.

Sensitive personopplysninger vil som regel komme i kategorien stor eller katastrofal på konfidensialitet og katastrofal på integritet med denne rangeringsmetoden.

Fyll inn tabell i maldokumentet **Risikovurdering** med kategori katastrofal, stor, moderat eller liten for de ulike personopplysningene.

**UTILGJENGELIGHET**
- avgrenset tidsrom
- permanent

**EKSEMPLER PÅ TRUSLER / UØNSKEDE HENDELSER:**
- Publisering av andres navn og personnummer på Internett ved menneskelig feil.
- ID-tyveri; endring av annen persons postadresse og bestilling av kredittkort i annens navn.
- Elektronisk klientregister utilgjengelig i arbeidstid, systemet er nede.

## 5.6.2 Konsekvenser av uønskede hendelser

Konsekvensanalysen skal ta utgangspunkt i identifiserte trusler, og analysere konsekvensene av at de ulike truslene/uønskede hendelsene inntreffer. Virksomhetenes infrastruktur gjør gjerne at flere systemer er brukt i behandlingen av personopplysninger. Det kan derfor være hensiktsmessig å kategorisere hvilket beskyttelsesbehov de ulike systemene og nettverkene har med hensyn til konfidensialitet, integritet og tilgjengelighet. En mye brukt kategorisering er følgende;

K = 4; Katastrofal konsekvens
K = 3; Stor konsekvens
K = 2; Moderat konsekvens
K = 1; Liten konsekvens

Konsekvensen 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. Vurdering av personvernkonsekvens har som formål å avdekke følger for den enkeltes personvern – ikke eventuelle følger sikkerhetsbruddet kan få for virksomheten.

**EKSEMPEL PÅ BESKRIVELSE AV KONSEKVENS**
Ved vurdering av personvernkonsekvens er det naturlig å ta utgangspunkt i målet om 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, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.
- K=3, hendelsen kan føre til tap av helse, 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 oppfatter 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.

## 5.6.3 Overordnet vurdering av beskyttelsesbehov

På bakgrunn av hvilket potensial de ulike systemene representerer i forhold til konsekvens, kan vi gjøre en overordnet vurdering av hvilket beskyttelsesbehov som er nødvendig. Systemer hvor katastrofale hendelser kan inntreffe vil normalt, uavhengig av sannsynlighet, ha behov for en bedre beskyttelse enn systemer hvor slike hendelser ikke kan inntreffe. Hva er det verste som kan skje? Systemer/grensesnitt rangeres i fire kategorier innenfor hvert sikkerhetsaspekt, som vist på foregående side.

## 5.6.4 Sannsynlighet for uønskede hendelser

Vurdering av sannsynlighet for at en uønsket hendelse skal inntreffe basert på statistikk er krevende. Det finnes lite statistikk som er registrert under kontrollerte og sammenlignbare forhold. I tillegg forandrer tekniske forutsetninger seg kontinuerlig.

Den enkleste tilnærmingen er å vurdere hver enkelt uønsket hendelse, og vurdere kostnaden ved ett eller flere tekniske og organisatoriske tiltak som, i størst mulig grad, kan redusere sannsynligheten for at denne hendelsen skal inntreffe. Dersom kostnaden av tiltaket er begrenset i forhold til virksomhetens omsetning og sikkerhetsbudsjett, er den enkleste tilnærmingen å gjennomføre tiltaket inneværende år etter intern prioritering.

**RISIKOVURDERING**

- ❑ Er resultater av risikovurderinger dokumentert?
- ❑ Er trusler/uønskede hendelser som kan inntreffe inkludert?
- ❑ Er konsekvensen og sannsynlighet av mulige hendelser vurdert?

## Eksempel på vurdering av kategoriserte hendelser

| HENDELSE | KATEGORI: KONFIDENSIALITET, INTEGRITET, TILGJENGELIGHET | KONSEKVENS | SANNSYNLIGHET | RISIKO | VURDERES SOM AKSEPTABEL |
|---|---|---|---|---|---|
| Styreinformasjon på avveier | Konfidensialitet | Kan medføre uopprettelig økonomisk tap | Tiltak kan omgås av ansatte med små til normale ressurser | Stort uopprettelig økonomisk tap må påregnes innenfor 10-års periode | Ikke akseptabel hendelse |
| Uautorisert endring av opplysninger om en ansatt | Integritet | Kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi | Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene | Tap av anseelse eller integritet for 1 ansatt i en 50-års periode | Akseptabel |
| Utilgjengelighet av personalsystem i 24 timer | Tilgjengelighet | Hendelsen kan medføre økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet | Tiltak kan omgås av ansatte med små til normale ressurser | Svært liten konsekvens | Akseptabel |

I tabellen vises hvordan hendelser kan kategoriseres og vurderes. Først angis hvilke sikkerhetsaspekter som er relevante for hendelsen (konfidensialitet, integritet og/eller tilgjengelighet – KIT). Så gis en vurdering av mulig konsekvens, sannsynlighet for at hendelsen skal inntreffe og risiko som følge av dette. Til slutt gis det en vurdering av om risikoen er akseptabel eller ikke.

## Eksempel på tabell over akseptabel risiko

(Forklaring: Hvite felt representerer akseptabel risiko, gråfelt uakseptabel.)

| KONSEKVENS: SANSYNLIGHET: | LITEN | MODERAT | STOR | KATASTROFAL |
|---|---|---|---|---|
| LAV | | | Sensitive opplysninger om en ansatt på avveier. Uautorisert endring av opplysninger om en ansatt. | Sensitive opplysninger om alle ansatte på avveier. |
| MODERAT | Utilgjengelighet av personalsystem i 24 timer. | Budsjettinformasjon på avveier. | Styreinformasjon på avveier. | Konkurransesensitiv informasjon på avveier. |
| HØY | Informasjon med lavt beskyttelsesbehov på avveier. | En dags bortfall av sikkerhetskopiering. Ukjente mennesker i kontorlokalene. | | |
| SVÆRT HØY | | | | |

## Forklaring til konsekvens og sannsynlighet:

Konsekvens graderes etter hvor alvorlig hendelsen er for virksomheten eller for den registrerte. Dette kan måles i økonomisk tap, tap av liv og helse, samt tap av anseelse både for virksomheten og den registrerte. Følgende er et eksempel på beskrivelse av katastrofal hendelse (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.

Sannsynlighet kan uttrykkes ved hvor lett hendelsen kan inntreffe, for eksempel for sannsynlighet lav (S = 1):

Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå eller bryte tiltakene.

Rutine for risikovurdering beskrives i maldokumentet **Risikovurdering.**

For mer informasjon om risikovurderinger, og utfyllende informasjon om konsekvens og sannsynlighet, se Datatilsynets veileder «Risikovurdering av informasjonssystem» på www.datatilsynet.no.

## 5.7 Akseptabel risiko

Dette underkapitlet beskriver oppgaver i forbindelse med vurdering av om kartlagte trusler og/eller uønskede hendelser, med tilhørende risiko, ligger innenfor dokumentert akseptabelt risikonivå. Gå gjennom hver uønsket hendelse og vurder om denne vil medføre uakseptable konsekvenser i forhold til akseptabelt risikonivå. Hvis trussel eller uønsket hendelse medfører risiko utover akseptabelt risikonivå, og eksisterende sikkerhetstiltak ikke er gode nok til å oppfylle beskyttelsesbehov, må det settes inn tekniske og/eller organisatoriske tiltak.

**EKSEMPLER PÅ BESKRIVELSER:**

1. Beskrivelse av akseptabelt risikonivå:
- Sikkerhetstiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne forårsake hendelser med katastrofale konsekvenser for enkeltmenneskers personvern.

2. Beskrivelse av trusler/uønskede hendelser:
- Autentiseringsmekanisme ved innlogging på nettsted er for enkel, og personer utenfra med gode kunnskaper kan få tilgang til systemer med personopplysninger innenfor brannmur.
- Ansatt åpner vedlegget til en e-postmelding som inneholder spam, planter ondsinnet programvare på PC-en til virksomheten. Deretter sendes det ut sensitive personopplysninger per e-post til uautorisert mottaker.

**AKSEPTABEL RISIKO**

- ❑ Er uønskede hendelser vurdert med hensyn til risiko og vurdert opp mot akseptabelt nivå?
- ❑ Er hendelser med uakseptabel risiko identifisert?

## 5.8 Rutiner for informasjonssikkerhet

### 5.8.1 Konfigurasjonsstyring

Med konfigurasjon menes informasjonssystemets utforming, det vil si utstyr og program samt sammenkoblinger mellom disse. Informasjonssystemet skal konfigureres med utgangspunkt i føringene i dokumentet **Sikkerhetsmål, - strategi og akseptkriterier.**

Ved valg av konfigurasjon skal virksomhetens behov for informasjonssikkerhet tillegges vekt, i tillegg til vurdering av økonomi og behov for funksjonalitet. Slik vurdering vil kunne omfatte etablering av sikkerhetsbarrierer, bruk av nettverkssegmentering for å skille forskjellige behandlinger av personopplysninger fra hverandre i informasjonssystemet og lignende.

Virksomheten skal konfigurere informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås i henhold til risikovurdering og beslutninger om sikkerhetstiltak. Informasjonssystemets konfigurasjon beskrives i dokumentet **Beskrivelse av informasjonssystemet.**

Konfigurasjonen skal dokumenteres i en oversikt, eksempelvis i form av konfigurasjonskart, som angir
- koblinger mellom utstyr og program
- inndeling av informasjonssystemet i soner
- kommunikasjonspunkt for tilkopling til ekstern dataoverføring
- navn eller modellbetegnelse, og serienummer eller versjonsnummer på sikkerhetsutstyr/-programmer
- sikkerhetsfunksjoner med opplysninger om oppsett/innstilling av utstyr/program
- når sikkerhetsutstyret ble tatt i bruk, eller når utstyret ble tatt ut av bruk
- opplysninger om vedlikehold, skade, funksjonsfeil og reparasjoner

### 5.8.2 Brukersikkerhet

Sikkerhetskrav til ulike typer roller er dekket i maldokumentene
- **Sikkerhetsinstruks bruker**
- **Sikkerhetsinstruks leder**
- **Sikkerhetsinstruks sikkerhetsansvarlig**

Informasjonssystemet skal brukes slik som det fremgår av de ulike sikkerhetsinstruksene.

### 5.8.3 Logging

Virksomheten er pålagt å logge autorisert bruk og forsøk på uautorisert bruk av informasjonssystemet i henhold til personopplysningsforskriften:

- Autorisert bruk av informasjonssystemet skal registreres.
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Aktivitetslogger fra informasjonssystemet er under visse forutsetninger unntatt fra meldeplikt. Det er også viktig å være klar over at personopplysninger som fremkommer som følge av logging for drifts- og sikkerhetsformål, ikke senere kan benyttes for å overvåke eller kontrollere enkeltpersoner.

Hensikten med logging av autorisert bruk er å i ettertid kunne spore hvem som gjorde hva med hvilke personopplysninger, og på hvilket tidspunkt. Det er altså ikke behov for å logge for eksempel alle kall på databasenivå ved oppslag av opplysninger om en person.

**EKSEMPEL PÅ LOGGING AV AUTORISERT BRUK**

- logging av pålogging og avlogging til nettverk og applikasjoner

**EKSEMPEL PÅ LOGGING AV FORSØK PÅ UAUTORISERT BRUK**

- logging av mislykte forsøk på pålogging til nettverk og applikasjoner

Rutine for logging beskrives i dokumentet **Driftsrutiner.** Loggfiler og formater beskrives i dokumentet **Beskrivelse av informasjonssystemet.**

**RUTINER FOR INFORMASJONSSIKKERHET**

- ❑ Er informasjonssystemet konfigurert i henhold til dokumentet **Sikkerhetsmål og -strategi** og resultatet av risikovurderingen?
- ❑ Er konfigurasjonen beskrevet i dokumentet **Beskrivelse av informasjonssystemet**?
- ❑ Er de ulike sikkerhetsinstruksene gjort kjent i virksomheten og signert av alle relevante brukere og ledere, samt av sikkerhetsansvarlig?
- ❑ Er rutine for logging beskrevet i dokumentet **Driftsrutiner**, og tatt i bruk i drift av informasjonssystemet?

## 5.9 Valg av sikkerhetstiltak

Kapittel 2 i personopplysningsforskriften inneholder en del minimumskrav til konkrete sikkerhetstiltak alle virksomheter som behandler personopplysninger skal oppfylle. Dette gjelder for eksempel krav til tilgangskontroll, avvikshåndtering, logging, sletting og taushetsplikt.

Disse kravene oppfylles ved å fylle inn og tilpasse følgende maldokumenter – i henhold til virksomhetens behov og resultater av risikovurderinger

- **Informasjonshåndteringsrutine**
- **Sjekkliste nyansatt – slutter**
- **Taushetserklæring**

Følgende dokumenter vil i større grad påvirkes av resultatene av risikovurdering

- **Beskrivelse av informasjonssystemet**
- **Driftsrutiner**
- **Beredskapsplan**
- **Fysisk sikkerhet**

Under utarbeidelse av disse dokumentene velger man tiltak avhengig av beskyttelseskategori for personopplysninger og eventuell sannsynlighet.

**VALG AV SIKKERHETSTILTAK**

- ❑ Finnes det en beskrivelse av hvilke sikkerhetstiltak som er nødvendige for å motstå og avverge identifiserte trusler og uønskede hendelser?

# Strategi/tiltak for sikring av informasjon

Eksempler på aktuelle tekniske sikkerhetstiltak for personopplysninger og behandlende systemer med ulike beskyttelsesbehov. Listen er ikke uttømmende.

| KAT. | KONFIDENSIALITET | INTEGRITET | TILGJENGELIGHET |
|---|---|---|---|
| HØYT | • to-faktor autentisering<br>• kryptering av kommunikasjon over eksterne forbindelser inkludert forretningskritisk e-post<br>• felter med direkte økonomisk verdi krypteres ende-til-ende<br>• kryptering forretningskritisk informasjon ved lagring<br>• direkte økonomisk verdi<br>• passord<br>• informasjon på bærbare PC-er<br>• krypteringsnøkler<br>• sikkerhetsovervåking<br>• periodisk verifisering av sikkerhetsnivå og ved vesentlige oppgraderinger<br>• rutiner for sikkerhet i utvikling og testing<br>• bruk av proxy løsning /web front-end når tjenester skal nås fra Internett<br>• logging av all trafikk relatert til transaksjoner<br>• krypteringsnøkler skal være forskjellig mot leverandør fra krypteringsnøkler mot butikker/lagring<br>• dekryptering av informasjonsfelter med direkte økonomisk verdi skal bare skje etter betaling i butikk | • to-faktor autentisering<br>• autentisering av brukere ved personlige brukerkonti og passord samt smartkort iht. passordpolicy<br>• separat autentisering av eksterne brukere i tillegg til intern pålogging ved tilgang til internt nett<br>• autentisering av maskin-maskin kommunikasjon over eksterne forbindelser<br>• digitale signaturer på forretningskritisk e-post over Internett<br>• digitale signaturer på transaksjoner (skal vurderes for alle nye prosjekter)<br>• helhetlig logging<br>• transaksjoner initiert fra butikk skal kunne knyttes til operatøridentitet | **GENERELT**<br>• avbruddsfri strømforsyning<br>• driftsovervåking (24/7)<br>• maskinvaremonitorering (24/7)<br>• 24/7 måling og overvåking av oppetid på tilgjengelighet gjennom nettverk<br><br>**HØY 1 (ANBEFALTE TILTAK)**<br>• supportavtale (24/7) HW, SW og kommunikasjon med umiddelbar respons for både hoved- og reserveløsning (vurderes)<br>• redundans/ reserveløsning (full, dvs. HW, SW og kommunikasjon) skal ha umiddelbar aktivering av reserveløsning ved feil på hovedsystem<br>• fysisk separat reserveløsning<br><br>**HØY 2 (ANBEFALTE TILTAK)**<br>• supportavtale (24/7) HW, SW og kommunikasjon med responstid 2 timer for både hoved- og reserveløsning (vurderes)<br>• nødvendig redundans/ reserveløsning (delvis, dvs. maskinvare og kommunikasjon) slik at systemet reetableres etter maks 4 timer |
| MIDDELS | • kryptering av kommunikasjon over Internett eller andre eksterne IP-nett.<br><br>**Unntak:**<br>• leide linjer<br>• ISDN<br>• mobilkommunikasjon | • autentisering av brukere ved personlige brukekonti og passord iht. passordpolicy<br>• separat autentisering av eksterne brukere i tillegg til intern pålogging ved tilgang til internt nett<br>• autentisering av ISDN, analog eller mobil forbindelser ved bruk av A-nummer verifikasjon<br>• helhetlig logging | • supportavtale (24/7) HW, SW og kommunikasjon med responstid 8 timer<br>• redundans/ reserveløsning (delvis, reservedeler tilgjengelig ila 8 timer)<br>• avbruddfri strømforsyning |
| LAVT | • ingen utover generell strategi | • eksterne brukere uten passord skal bare ha tilgang på systemer plassert i DMZ (Demilitarisert sone) | • supportavtale (8-16) HW, SW og kommunikasjon med responstid 24/48 timer<br>• avbruddfri strømforsyning for servere<br>• driftsovervåking (periodisk) |

Mer detaljert informasjon om hvordan man gjennomfører sikkerhetstiltak finnes i Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2005) og Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet [16].

[16] www.standard.no

## 5.10 Gjennomføre sikkerhetstiltak

I mange tilfeller vil ulike trusler påvirkes av forskjellige sikkerhetstiltak, og ulike sikkerhetstiltak kan overlappe hverandre. Det er derfor viktig å analysere totalbehovet for tiltak, ut fra summen av de ulike tiltakene, slik at man kommer frem til en tilpasset og effektiv teknisk og organisatorisk totalløsning for informasjonssikkerheten i virksomheten. Samtidig må tiltak prioriteres ut fra hvor det er identifisert størst risiko.

Det er viktig å være bevisst på at det skal utarbeides dokumenterte rutiner og prosedyrer i standardform, som beskriver styringssystemet for informasjonssikkerhet i virksomheten. Standardiserte rammeverk øker brukervennligheten, letter arbeidet med oppdateringer og gjør det enklere å finne igjen informasjon.

Gjennomføring av nødvendige tiltak bør organiseres i en prosjektplan. Gjennomføring av tiltakene kan eksempelvis vare over flere år, i og med at budsjettmessige begrensninger kan forhindre at alle nødvendige tiltak utføres umiddelbart. Prosjektplanen vil også være et hjelpemiddel i budsjettarbeidet og ved ressursplanlegging. Hvis ledelsen har godkjent prosjektplanen for utbedring av informasjonssikkerheten, bør ledelsen også sikre nødvendige budsjetter, slik at utbedringene kan gjennomføres i samsvar med planen.

### GJENNOMFØRE SIKKERHETSTILTAK

- ❑ Er den dokumenterte aktivitetsplanen for å ivareta informasjonssikkerhet for behandling av personopplysninger, i overensstemmelse med resultater av risikovurdering?
- ❑ Finnes det en dokumentert budsjettplan som inkluderer en tids- og aktivitetsplan?

# 6. Oppfølging



## 6.1 Avvikshåndtering og egenkontroll

### 6.1.1 Behandling av avvik

Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerhet, skal virksomheten iverksette avviksbehandling [17].

Formålet med avviksbehandling er å lukke avviket så raskt som mulig, gjenopprette normaltilstand og hindre gjentagelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan personopplysninger håndteres eller informasjonssystemet benyttes, skal resultatet fra avviksbehandlingen brukes som grunnlag ved gjennomgang og endring av aktuelle rutiner.

**AVVIKSBEHANDLING BESTÅR AV:**

- Å oppdage avviket.
- Rapportering utføres normalt av den medarbeideren som oppdager avviket. Avviket rapporteres til virksomhetens sikkerhetsansvarlige eller i henhold til annen intern organisering.
- Iverksettelse av strakstiltak, blant annet med det formål å avgrense eventuelle følgeskader. Strakstiltakene kan utføres av den medarbeideren som oppdager avviket, eventuelt av den medarbeideren som har ansvar for håndteringsrutiner eller den berørte delen av informasjonssystemet.
- Iverksettelse av korrigerende tiltak for permanent å gjenopprette normaltilstand. Dette utføres normalt av virksomhetens sikkerhetsansvarlige (delegert myndighet fra behandlingsansvarlig) eller, i forbindelse med avvik for informasjonssikkerhet, av IT-driftssjef.
- Vurdering av hvorvidt korrigerende tiltak fungerer etter sin hensikt. Vurderingen utføres etter noe tid av henholdsvis sikkerhetsansvarlig eller IT-driftssjef.

**EKSEMPLER PÅ SITUASJONER SOM GJØR DET NØDVENDIG Å IVERKSETTE AVVIKSBEHANDLING:**

- Utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Lagring av personopplysninger uten samtykke eller annet behandlingsgrunnlag.
- Når medarbeidere benytter informasjonssystemet uten autorisasjon.
- Feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet.
- Henvendelse om innsyn har blitt avvist grunnet medarbeiderens manglende kjennskap til rutinene.

Avviksbehandling skal dokumenteres i en rapport som inneholder opplysninger om selve avviket, gjennomførte strakstiltak, iverksatte korrigerende tiltak, resultater fra evaluering av det korrigerende tiltakets effekt over tid, samt opplysninger om hvilke medarbeidere som har vært involvert i behandling av avviket.

Rapportering av avvik utføres normalt av de medarbeiderne som oppdaget avviket. Strakstiltakene kan utføres av den som oppdager avviket, eventuelt av den medarbeider som har ansvar for håndteringsrutiner eller den berørte delen av informasjonssystemet. Mal for avviksskjema til utfylling finnes i maldokumentet **Avviksskjema**.

Se også eksempel på neste side.

Dersom avviket har medført en uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

[17] Personopplysningsforskriften § 2-6

# Eksempel på avviksskjema

| | | | |
|---|---|---|---|
| **AVVIKSSKJEMA** | **VIRKSOMHET:**<br>XX | **SENDES TIL:**<br>Sikkerhetsansvarlig | **SAKSIDENT:**<br>xxxx |
| Formål: Skjemaet skal sikre at alle brudd og antatte brudd på håndteringsrutiner eller sikkerhetsrutiner blir registret og behandlet på en forsvarlig måte. | | | |
| **BESKRIVELSE AV AVVIKET:**<br>xxxxxxx<br>xxxxxxx<br>vedlegg: | | | |
| **BESKRIVELSE AV MIDLERTIDIG TILTAK:**<br>xxxxxxx<br>xxxxxxx<br>vedlegg: | | | |
| **MELDERS REGISTRERING** | Navn:<br>Xxxxxxxxx | Utstyr/ident:<br>xxxxxxxx | Dato/ kl:<br>xxxxxxxxx |
| **ANALYSE AV ÅRSAK**<br>xxxxxxx<br>xxxxxxx<br>vedlegg: | | | |
| **BESKRIVELSE AV IVERKSATTE TILTAK:**<br>xxxxxxx<br>xxxxxxx<br>Henv: | | | |
| **SIKKERHETS-ANSVARLIGES TILTAK** | **KLASSIFIKASJON:**<br>xxxxx | **RAPPORT SENDES DATATILSYNET:**<br>JA / NEI | **DATO / UNDERSKRIFT:**<br>NN |
| **EVALUERT DATO:** | | | |

Rutiner for avvikshåndtering beskrives i maldokumentet,
**Rutiner for avvikshåndtering og egenkontroll.**

### 6.1.2 Egenkontroll av rutiner og tekniske tiltak

Virksomheten skal kontrollere at rutinene for håndtering av personopplysninger og informasjonssikkerhetstiltak brukes og fungerer etter hensikten. Sikkerhetsansvarlig skal sørge for at egenkontrollskjema blir oppdatert etter ledelsens gjennomgang, og forøvrig ved behov som følge av avviks- og endringshåndtering.

Mal for egenkontrollskjema til utfylling finnes i maldokumentet **Egenkontrollskjema**.

Se også eksempel på neste side.

## 6.2 Rutiner for rapportering og forslag til tiltak

### 6.2.1 Læring og prosessforbedring

Det er viktig å innføre faste rutiner for å forbedre internkontrollen. Det skal derfor innføres rutiner for å lære av uønskede hendelser, dokumentere erfaring og forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår i fremtiden.

**EKSEMPEL – RUTINE FOR LÆRING OG PROSESSFORBEDRING**

- Det gjennomføres faste møter hvor styringssystemet for informasjonssikkerhet er tema, inklusiv gjennomgang av avvik og forslag til forbedring.
- Det gjennomføres halvårlige møter mellom sikkerhetsansvarlig og IT-drift hvor resultater av egenkontroller gjennomgås. Lærdom dokumenteres i kompetansedatabase og/eller endringslogg. Forslag til forbedring av håndteringsrutiner og sikkerhetstiltak gjennomføres. Alternativt legges disse frem for ledelsen for godkjenning.

### 6.2.2 Avvikshåndtering, egenkontroll og forslag til forbedring

Virksomheten skal ha rutine for rapportering og mal for rapport til ledere og ansvarlige fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporten skal også omfatte erfaringer som er gjort og forslag til forbedringer, både tekniske tiltak og prosessforbedringer.

**EKSEMPEL – RUTINE FOR RAPPORTERING**

- månedlig rapportering til sikkerhetsansvarlig om sikkerhetshendelser, avvik og resultater fra egenkontrollaktiviteter samt erfaringer og forslag til forbedringer
- årlig rapportering til ledelsens gjennomgang

**DOKUMENTERTE RUTINER 3**

- ❑ Er rutiner for læring og prosessforbedring, samt for rapportering beskrevet i maldokumentet **Rutiner for læring, prosessforbedring og rapportering?**

## Eksempel egenkontroll

| EGENKONTROLLTILTAK | EIER AV AKTIVITET | FREKVENS | RESULTAT TILTAK |
|---|---|---|---|
| Oppfølging/revisjon av risikovurdering og valgt sikkerhetsnivå. | Sikkerhets-leder | Årlig | |
| Sikkerhetsmål og strategier etterleves. | | | |
| Ansvars – og myndighetsforhold er som beskrevet. | | | |
| Rutiner etterleves (stikkprøver). Vekt på de deler av rutinene som i vesentlig grad bidrar til å opprettholde sikkerhetsnivået, inkludert rutiner for å verifisere nettverkssikkerhet, endringshåndtering, hendelseshåndtering, avvikshåndtering, installasjon/herding, sikkerhetskopier og annen beredskap og loggrevisjon. | | | |
| Oppdaterte rutiner, driftsdokumentasjon og konfigurasjonsoversikter foreligger (stikkprøver). | | | |
| Vurdere om risikobildet tilsier endrede tiltak og/eller revisjon av mål/strategi. | | | |
| Vurdere om rutiner og definisjon av ansvar fungerer etter hensikt. | | | |
| Periodiske sikkerhetsmøter mellom IT-sikkerhetsansvarlig og samband, system og drift. Oppfølging av egenkontroll og prosjekter. Sikkerhetsmøter ved behov ved alvorlige hendelser. | IT-sikkerhets-ansvarlig | Månedlig + ved behov | |
| Gjennomgang av privilegerte brukeres tilgangsrettigheter – administratorrettigheter. | IT-drift, samband og telefoni | Halvårlig | |

# 7. Brukeropplæring

Målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot informasjonssikkerheten, og at de er gitt mulighet til å etterleve organisasjonens sikkerhetspolitikk i sitt daglige arbeid. Brukerne bør få opplæring i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer.

## 7.1 Opplæring i internkontroll og informasjonssikkerhet

Før ansatte i organisasjonen og eventuelle tredjepartsbrukere får tilgang til informasjon eller tjenester, bør de få hensiktsmessig opplæring. Dette omfatter krav til internkontroll og informasjonssikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer. Dette inkluderer for eksempel innloggingsprosedyrer, bruk av programvare, og rapportering av avvik. I tillegg bør de få regelmessig oppdatering i organisasjonens politikk og prosedyrer.

## 7.2 Taushetserklæring

Taushetserklæringer brukes for å gjøre oppmerksom på at det forekommer konfidensiell informasjon i virksomheten. De ansatte skal undertegne en slik erklæring samtidig med ansettelseskontrakten. Taushetserklæringen oppbevares i den ansattes personalmappe under hele ansettelsesforholdet. Midlertidig ansatte og tredjepartsbrukere som ikke allerede er dekket av eksisterende kontrakt med taushetserklæring, bør undertegne en tilsvarende erklæring før de får tilgang til informasjonssystemer. Betingelsene og ansettelsesvilkårene bør opplyse om den ansattes ansvar for informasjonssikkerhet. Der det er relevant, bør dette ansvaret også gjelde i en nærmere spesifisert periode etter at ansettelsesforholdet er avsluttet.

Taushetserklæringer bør gjennomgås på nytt når ansettelsesforholdet endres, særlig når ansatte skal forlate organisasjonen, eller kontrakter løper ut.

## 7.3 Personvernombud

For virksomheten kan det være en stor fordel å ha en bestemt person å henvende seg til med spørsmål rundt behandling av personopplysninger knyttet til sin virksomhet. Sentrale oppgaver for ombudet vil være å bistå i opplæring internt i virksomheten og i behandling av klager fra både virksomhetens egne ansatte og eksterne aktører relatert til bruk av personopplysninger. Virksomheter med personvernombud er fritatt fra den lovpålagte meldeplikten til Datatilsynet[18], siden ombudet selv skal føre denne oversikten. Virksomhetens leder kan ikke være personvernombud.

Mer informasjon om dette finner du på www.datatilsynet.no/personvernombud.

[18] Personopplysningslovens § 31

# 8. Overføring av personopplysninger til utlandet

Formålet med å etablere rutiner og prosedyrer ved overføring av personopplysninger til utlandet er å sikre at personopplysningene bare blir overført til stater som sikrer forsvarlig behandling av personopplysninger. Den som er tillagt eller har fått delegert daglig behandlingsansvar i henhold til bestemmelsene i personopplysningsloven, skal tilrettelegge for og følge opp at bestemmelsene om overføring av personopplysninger til utlandet etterleves.

Såfremt personopplysningslovens generelle krav til behandling av personopplysninger er oppfylt, kan personopplysninger overføres til land innen EU og EØS-området. Videre kan opplysninger overføres til land som Europakommisjonen har godkjent, samt enkeltbedrifter i USA som har sluttet seg til Safe Harbor-avtalen. Slik overføring utløser ingen selvstendig melde- og konsesjonsplikt, men overføringen til utlandet må beskrives i konsesjonssøknad eller melding knyttet til hovedformålet med behandlingen. Eksempler på dette er forskningsprosjekter, varslingstjenester eller kontroll og overvåkning av ansatte.

Ved overføring til tredjeland som ikke er godkjent av Europakommisjonen eller til virksomheter i USA som ikke er en del av Safe Harbor, kan overføring skje på gitte vilkår [19]. For eksempel kan det være tilstrekkelig at den registrerte samtykker til overføringen.

Et gyldig samtykke må være avgitt frivillig og kan på ethvert tidspunkt trekkes tilbake [20]. Samtykke vil derfor ofte være lite egnet som grunnlag for overføring til utlandet.

Den enkleste måten å overføre personopplysninger til andre land på, er å bruke EUs standardkontrakter. Ved signering av en av kontraktene forplikter dataimportøren seg til å behandle dem i samsvar med de krav som gjelder innenfor EU og EØS-området. Mer informasjon om overføring av personopplysninger til utlandet og EUs standardkontrakter finnes på www.datatilsynet.no.

### OVERFØRING TIL UTLANDET

- ❑ Bor mottaker i et land innen EU eller EØS-området eller land som EU-kommisjonen har godkjent?
- ❑ Er mottaker en enkeltbedrift i USA? Har den i så fall sluttet seg til Safe Harbor-avtalen?
- ❑ Er en av EUs standardkontrakter egnet som grunnlag for overføringen?
- ❑ Er overføring av personopplysninger nødvendig i henhold til et av alternativene i pol § 30?
- ❑ Har den registrerte samtykket i overføringen?

[19] Personopplysningsloven § 30, [20] Personopplysningsloven § 2 nr. 7

# 9. Kontroll med sikkerhet hos partner/leverandør

Kontraktsregulering av forholdet til partnere og leverandører har som formål å avklare ansvarsdelingen når det gjelder informasjonssikkerhet. I tillegg utstyrer det virksomheten med et styringsverktøy overfor partner eller leverandør. Virksomheten skal ha rutiner og prosedyrer overfor alle partnere eller leverandører som virksomheten benytter ved behandling av personopplysninger, eller som har tilgang til utstyr eller program hvor personopplysninger behandles (databehandlere).

### EKSEMPLER PÅ PARTNERE ELLER LEVERANDØRER HVOR DET ER AKTUELT Å INNGÅ KONTRAKT MED SIKKERHETSVILKÅR

- databehandlere/leverandører
- firma med konsulentoppdrag i tilknytning til informasjonssystemet
- firma som utfører vedlikehold av utstyr eller program, eller som utfører arbeid i områder hvor utstyr eller program befinner seg
- renholdsfirma
- vikarbyrå

Det skal spesielt legges vekt på om partneren eller leverandørens personell er informert om taushetsplikten som gjelder og at personellet undertegner taushetserklæring. Det skal lages oversikt over hvilke av partnerens eller leverandørens personell som gis tilgang til informasjonssystemet eller adgang til områder eller utstyr, samt hvordan virksomhetens kontroll av sikkerhet hos partner og leverandør skal utføres.

Følgende vilkår bør inngå som grunnlag mellom virksomhet og partner/leverandør og skal kunne kontrolleres av virksomhet:

### ANSVAR

Leverandøren er ansvarlig for sikkerhetsbrudd for eget personale og brudd som har oppstått gjennom tilkopling av leverandørens utstyr. Leverandøren kan ikke engasjere en tredjepart/underleverandør til å utføre arbeidsoppgaver som følger av denne avtalen, uten at virksomheten har godkjent dette og leverandøren har inngått kontrakt med tredjepart med tilsvarende sikkerhetsbestemmelser.

### TAUSHETSPLIKT

Leverandørens personale skal undertegne taushetserklæring. De som undertegner taushetserklæring skal gjøres kjent med hva dette innebærer. Leverandøren kan kun benytte de personer til oppdraget som oppdragsgiver på forhånd har godkjent og er informert om. Taushetsplikten gjelder også etter at avtalen er opphørt, og etter at leverandørens personale har sluttet hos leverandøren.

### SIKKERHETSLØSNING

Leverandøren skal til enhver tid ha en organisatorisk og teknisk sikkerhetsløsning som tilfredsstiller Datatilsynets retningslinjer. Dette skal kunne dokumenteres overfor oppdragsgiver og Datatilsynet.

### SAMARBEID

Leverandøren skal ved behov samarbeide med virksomheten om de sikkerhetsbrudd som kan tilskrives leverandøren. Som ledd i virksomhetens årlige egenkontroll, bør det være et møte for å gjennomgå leverandørens organisatoriske og tekniske sikkerhetstiltak.

Datatilsynet har utarbeidet en kort veiledning og forslag til utforming av en databehandleravtale etter henholdsvis personopplysningsloven og helseregisterloven. Databehandleravtalen er tilgjengelig på www.datatilsynet.no.

# Vedlegg 1
## Definisjoner

**BEHANDLINGSANSVARLIG**
Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, pol § 2 nr 4.

**BEHANDLING AV PERSONOPPLYSNINGER**
Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder, pol § 2 nr 2.

**DATABEHANDLER**
Den som behandler personopplysninger på vegne av den behandlingsansvarlige, pol § 2 nr 5.

**INFORMASJONSSIKKERHET**
Personopplysningsloven, §13, stiller krav om at virksomheten *«skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger»*.

**INTEGRITET**
I forbindelse med informasjonssikkerhet:
At det verken tilsiktet eller utilsiktet skal skje uautoriserte endringer av personopplysninger.

**INTERNKONTROLL**
Internkontroll er ledelsens verktøy for å styre aktiviteten i virksomheten slik at driften skjer i overensstemmelse med lover og regler. Samtidig er styringssystemet medarbeiderens verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

**KONFIDENSIALITET**
At uvedkommende ikke får tilgang på opplysninger.

**KONFIGURASJONSENDRING**
Med konfigurasjon menes informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

**PERSONOPPLYSNING**
Opplysninger og vurderinger som kan knyttes til enkeltperson.

**POF**
Personopplysningsforskriften

**POL**
Personopplysningsloven

**REGISTRERT**
Den som en personopplysning kan knyttes til.

**SAMTYKKE**
En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv, pol § 2 nr 7.

**SENSITIV PERSONOPPLYSNING**
Personopplysning innenfor en av kategoriene, pol § 2 nr 8
- rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- helseforhold
- seksuelle forhold
- medlemskap i fagforeninger

**SIKKER SONE**
Med sikker sone menes den delen eller de delene av virksomhetens informasjonssystem som behandler personopplysinger, hvor kun autoriserte brukere med tjenstlig behov gis tilgang.

**TILFREDSSTILLENDE INFORMASJONSSIKKERHET**
At man etablerer sikkerhetstiltak i henhold til besluttet akseptabelt risikonivå og resultatene av en risikoanalyse. Risikoanalysen tar utgangspunkt i de personopplysningene som virksomheten behandler og behandlingene som utføres, ref pol § 13.

**TILGJENGELIGHET**
At opplysningene er tilgjengelige når vi trenger dem.

# Vedlegg 2
## Oversikt over maler

Disse malene kan lastes ned fra www.datatilsynet.no. Malene kan videre tilpasses din virksomhet.

**1. STYRENDE**

1-01 Styringsdokument internkontroll
1-02 Ledelsens gjennomgang

1-11 Sikkerhetsmål og -strategi
1-12 Sikkerhetsorganisasjon

**2. GJENNOMFØRENDE**

2-01 Rutiner for håndtering av personopplysninger

2-11- Risikovurdering

2-12 Sikkerhetsinstruks bruker
2-14 Informasjonshåndteringsrutine

2-15 Sjekkliste nyansatt slutter
2-16 Taushetserklæring

2-17 Sikkerhetsinstruks leder
2-19 Sikkerhetsinstruks sikkerhetsansvarlig

2-21 Beskrivelse av informasjonssystemet
2-22 Driftsrutiner
2-23 Overordnet IT beredskapsplan

2-24 Fysisk sikkerhet

**3. KONTROLLERENDE**

3-01 Rutiner for avvikshåndtering og egenkontroll
3-02 Avviksskjema
3-03 Egenkontrollskjema
3-04 Rapport fra avvikshåndtering og egenkontroll, og forslag til tiltak

# Vedlegg 3
## Sjekkliste for internkontroll

Datatilsynets kontroller har vist at mange virksomheter bare har internkontroll i forbindelse med informasjonssikkerhet. Ikke glem at internkontrollen også skal sikre de registrertes rettigheter og en ryddig behandling.

Regelverket stiller ikke formelle strukturkrav til internkontroll, men det er krav om at tiltakene skal dokumenteres. Listen er ikke uttømmende, og punktene må ses på som eksempler som kun skal tas med dersom de er aktuelle for virksomheten.

### Styrende dokumenter

#### JURIDISKE FORHOLD
- ❑ stadfesting av behandlingsansvarlig
- ❑ kartleggig av behandlinger
- ❑ identifisere formål med behandlingene
- ❑ hjemmelsgrunnlag for behandlingene
- ❑ vurdere om formålet med behandlingen er i samsvar med hjemmelsgrunnlaget
- ❑ identifisering av krav/plikter
- ❑ mål/policy – eller overordnede rammer for behandling av personopplysninger om egenkontroll og avviksbehandling

#### INFORMASJONSSIKKERHET
- ❑ sikkerhetsmål
- ❑ sikkerhetsstrategi
- ❑ sikkerhetsorganisasjonen
- ❑ overordnet om konfigurasjonskontroll
- ❑ egenkontroll og avviksbehandling

### Gjennomførende aktiviteter

#### JURIDISKE FORHOLD
#### RUTINER FOR
- ❑ innsyn, retting og supplering
- ❑ oppfyllelse av plikt til informasjon
- ❑ innhenting og kontroll av samtykke
- ❑ vurdering av opplysningens kvalitet
- ❑ sletting av personopplysninger
- ❑ ivaretakelse av eventuell reservasjonsrett
- ❑ melde- og konsesjonsplikt
- ❑ prosedyre for iverksettelse eller opphør av behandling

### Informasjonssikkerhet

#### STADFESTING AV
- ❑ organisering av sikkerhetsarbeidet
- ❑ informasjonssystem - beskrivelse
- ❑ sikkerhetskopiering
- ❑ tilgang til informasjonssystemet
- ❑ konformitetserklæring fra den ansatte

#### RUTINER FOR
- ❑ bruk av Internett
- ❑ bruk av elektronisk post
- ❑ utskrift og kopiering
- ❑ makulering av dokumenter
- ❑ sikkerhet og orden på eget kontor
- ❑ adgangskontroll
- ❑ innleid teknisk personell og håndverkere
- ❑ bruk av hjemmekontor
- ❑ bruk av bærbar datamaskin

### Kontrollerende aktiviteter

#### JURIDISKE FORHOLD
- ❑ prosedyre for periodisk kontroll
- ❑ håndtering av avvik
- ❑ rapport fra periodisk kontroll og forslag til tiltak

#### INFORMASJONSSIKKERHET
- ❑ prosedyre for periodisk kontroll
- ❑ prosedyre for kontroll av fysisk sikkerhet
- ❑ prosedyre for kontroll av logisk sikkerhet
- ❑ håndtering av avvik
- ❑ rapport fra periodisk kontroll og forslag til tiltak

**DATATILSYNET** Gateadresse: Tollbugata 3, Oslo | Postadresse: postboks 8177, dep 0034 Oslo
E-post: postkasse@datatilsynet.no | Telefon: 22 39 69 00 | Faks: 22 42 23 50

Datatilsynet