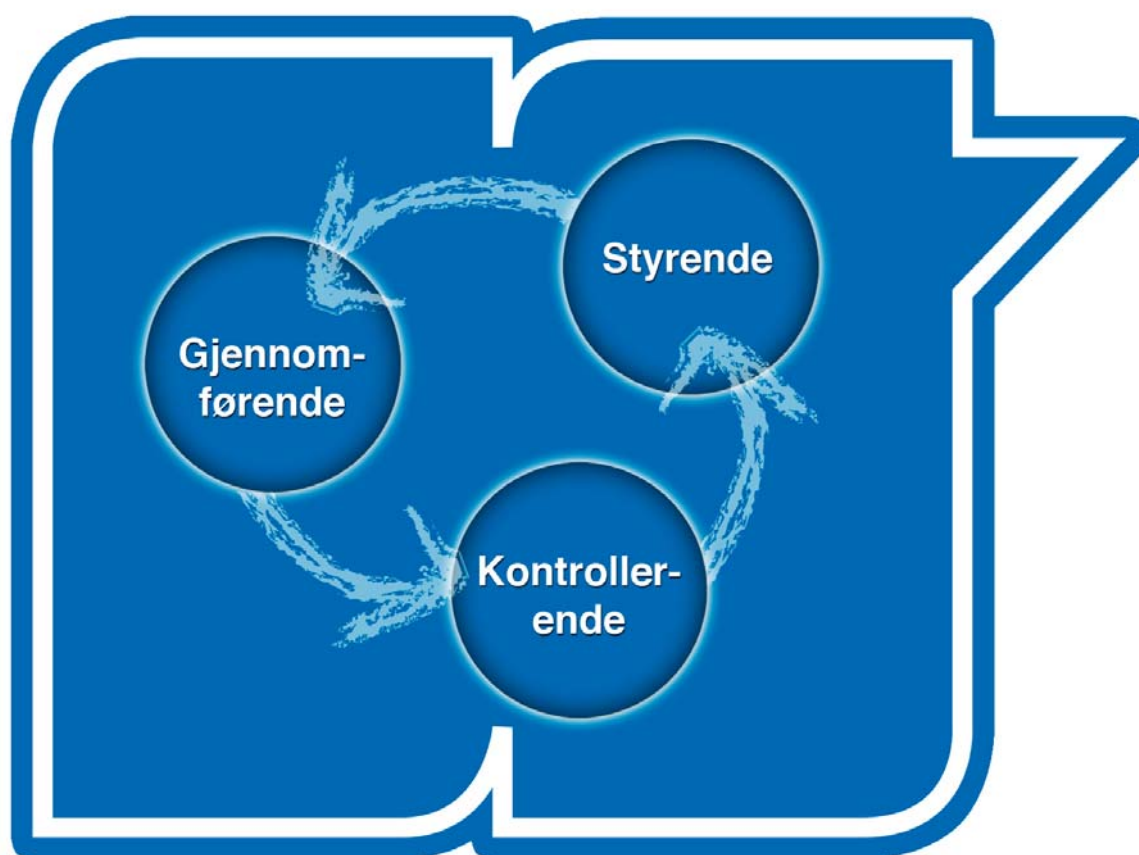


Internkontroll og informasjonssikkerhet

Veileder 07/01

Publisert 15.02.2007



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



De fleste virksomheter behandler personopplysninger i en eller annen form. Dette innebærer at de må følge personopplysningsloven og ha rutiner for sin bruk av opplysningene.

Denne veilederen hjelper deg som er ansvarlig for virksomheten gjennom oppgavene med å bygge opp internkontroll slik at virksomheten din behandler personopplysninger lovlig, sikkert og forsvarlig.

For virksomheter som kun behandler personopplysninger om egne ansatte og kunder finnes det en egen veileder.

Veilederen gir kunnskap og beskriver et løp for virksomheten som er enkelt og oversiktlig. Veilederen gir eksempler på plikter som virksomheten må oppfylle og rutiner som kan tilpasses eget behov. Det er likevel viktig at ansvarlig leder setter seg inn i lov og forskrift, og selv tenker gjennom konsekvensene for egen virksomhet. Hvilke plikter gjelder for virksomheten og hvilke rutiner er nødvendig?

Til slutt beskrives overgang til driftssituasjon og krav til kontrollrutiner og vedlikehold av internkontrollen. Dersom det ikke finnes rutinemessig oppfølging og kontroll, vil kvalitet på håndtering av personopplysninger og informasjonssikkerheten reduseres over tid. Rutinemessig avvikshåndtering og ledelsens årlige gjennomgang av internkontroll og informasjonssikkerhet er derfor viktige tiltak for varig og god internkontroll.

Innholdsfortegnelse

1	Innledning.....	7
1.1	Bakgrunn.....	7
1.2	Hensikten med dokumentet.....	7
1.3	Omfang og målgruppe for dokumentet.....	7
1.4	Forklaring til teksttyper.....	8
2	Bakgrunnskunnskap	9
2.1	Hva er internkontroll? Og informasjonssikkerhet?.....	9
2.2	Hva er personopplysningsloven og -forskriften?.....	10
2.3	Hva er personopplysninger og sensitive personopplysninger?.....	10
2.4	Hva er et personvernombud?	11
2.5	Internkontrollens dokumentasjon	12
2.6	Prosesen for å etablere internkontroll.....	13
2.7	Vedlikehold av internkontrollen	14
3	Innledende oppgaver	15
3.1	Skaff kunnskap.....	15
3.1.1	Generelt.....	15
3.1.2	Henvisninger til ytterligere informasjon.....	15
3.2	Virksomhetsleder er behandlingsansvarlig.....	16
3.3	Prosjekt for innføring av internkontroll	17
3.4	Støtteverktøy - kontroll mot personopplysningsforskriften.....	17
3.5	Virksomhetens behandlinger	19
3.6	Behandlinger og behandlingsgrunnlag	21
3.6.1	Identifisere formål.....	21
3.6.2	Fastsette behandlingsgrunnlaget	21
3.6.3	Vurdere om formål er i samsvar med hjemmel	22
3.7	Overordnede rammer	23
3.8	Identifisere plikter	25
4	Håndteringsrutiner	26
4.1	Generelt om håndteringsrutiner	26
4.2	Håndtering av samlede personopplysninger	27
4.2.1	Rutine for iverksettelse eller opphør av behandling	27
4.2.2	Overholdelse av melde- og eventuell konsesjonsplikt.....	27

4.2.3	Rutine for sletting av personopplysninger	29
4.2.4	Rutiner for utlevering av personopplysninger til andre	30
4.2.5	Rutiner for sikring av kvalitet av personopplysninger.....	31
4.3	Rutiner relatert til person	32
4.3.1	Innhenting og kontroll av samtykke.....	32
4.3.2	Oppfyllelse av plikt til informasjon	32
4.3.3	Rutiner for innsyn, retting og supplering	32
4.3.4	Ivaretagelse av eventuell reservasjonsrett.....	35
4.3.5	Innsyn i privat e-post og private filområder.....	35
5	Informasjonssikkerhet	38
5.1	Innledning	38
5.2	Sikkerhetsmål og sikkerhetsstrategi.....	38
5.2.1	Innledning	38
5.2.2	Sikkerhetsmål	39
5.2.3	Sikkerhetsstrategi	39
5.3	Ledelsens gjennomgang	40
5.4	Sikkerhetsorganisasjon.....	42
5.5	Akseptabelt risikonivå.....	42
5.6	Gjennomføre risikovurdering.....	44
5.6.1	Generelt	44
5.6.2	Mer om uønskede hendelser.....	45
5.6.3	Mer om konsekvens	46
5.6.4	Overordnet vurdering av beskyttelsesbehov	47
5.6.5	Mer om sannsynlighet	48
5.6.6	Vurdering av kategoriserte hendelser	48
5.7	Har vi akseptabel risiko?	50
5.7.1	Beskrivelse	50
5.8	Rutiner for informasjonssikkerhet	51
5.8.1	Konfigurasjonsstyring	51
5.8.2	Brukersikkerhet	51
5.8.3	Logging	52
5.9	Velge sikkerhetstiltak.....	53
5.9.1	Beskrivelse	53
5.10	Gjennomføre sikkerhetstiltak	55
5.10.1	Beskrivelse	55

6	Oppfølging.....	56
6.1	Avvikshåndtering og egenkontroll.....	56
6.1.1	Behandling av avvik	56
6.1.2	Egenkontroll av rutiner og tekniske tiltak.....	59
6.2	Rutiner for rapportering og forslag til tiltak	60
6.2.1	Læring og prosessforbedring	60
6.2.2	Avvikshåndtering, egenkontroll og forslag til forbedring	60
7	Referanser.....	61
	<i>Vedlegg 1 Definisjoner</i>	<i>62</i>
	<i>Vedlegg 2 Oversikt over maler</i>	<i>64</i>

1 Innledning

1.1 Bakgrunn

De fleste virksomheter behandler personopplysninger i en eller annen form. Dette innebærer at de må følge personopplysningsloven og ha rutiner for sin bruk av opplysningene og tilfredsstillende beskyttelse av opplysningene.

Denne veilederen hjelper deg som er ansvarlig for virksomheten, gjennom oppgavene med å bygge opp internkontroll slik at virksomheten din behandler personopplysninger lovlig, sikkert og forsvarlig. Veilederen er delt i flere dokument. Dette dokumentet gir deg innledende veiledning og bakgrunnskunnskap, mens tilhørende maler kan du fylle ut og endre slik de til sammen blir virksomhetens internkontroll.

Behandling av personopplysninger medfører plikter for virksomheten og rettigheter for den registrerte. Ulike opplysninger og ulike formål medfører at ingen virksomheter er like og hver virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin situasjon. Tilsvarende 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 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.

Virksomheten plikter etter personopplysningsloven å ha kontroll på sin håndtering av personopplysninger. For virksomheten bør samfunnsplikten til å sørge for at opplysninger om enkeltpersoner håndteres med nødvendig respekt også være en grunn til å ha ryddighet. I tillegg kan det å gi et godt inntrykk rundt håndtering av personopplysninger gi virksomheten en positiv merverdi, på samme måte som manglende ryddighet kan virke negativt på virksomhetens omdømme.

1.2 Hensikten med dokumentet

Hensikten med dette dokumentet er å veilede virksomheter gjennom arbeidet med å innføre internkontroll for forsvarlig og sikker behandling av personopplysninger på en enkel og oversiktlig måte.

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, ref. [1], tilpasset mindre virksomheter som kun håndterer personopplysninger om egne ansatte og om kunder (dvs. opplysninger om for eksempel kontaktpersoner ved salg og leveranse av varer).

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

1.4 Forklaring til teksttyper

Sitater fra personopplysningsloven og -forskriften er skrevet *i kursiv*.

Referanser til maldokumenter er skrevet i uthevet Arial skrifttype, eksempelvis **Driftsrutiner**.

2 Bakgrunnskunnskap

Bakgrunnskunnskap	Innledende oppgaver	Håndteringsrutiner	Informasjonssikkerhet	Oppfølging
-------------------	---------------------	--------------------	-----------------------	------------

2.1 Hva er internkontroll? Og informasjonssikkerhet?

Personopplysningsloven stiller krav til internkontroll i form av 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 kan beskrives som:

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

Internkontroll kan beskrives veldig kort ved å dokumentere svarene på noen få sentrale spørsmål:

- Hvem er ansvarlig i virksomheten?
- Hvilke opplysninger håndterer virksomheten, og hvorfor?
- Hva gir virksomheten lov til å håndtere opplysningene?
- Hvilke plikter medfører dette etter regelverket?

Deretter må virksomheten lage og gjøre kjent de rutiner som er nødvendige for å etterleve disse pliktene. Til slutt må man sørge for at rutinene blir fulgt, og at de holdes oppdatert.

Informasjonssikkerhet dreier som om å håndtere risiko relatert til informasjonsverdier. En virksomhet må først identifisere hvilke informasjonsverdier den besitter, inkludert personopplysninger. Deretter må det gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende. Så planlegger man og gjennomfører ved behov sikkerhetstiltak for å skape et tilfredsstillende sikkerhetsnivå for beskyttelse av verdiene. Tilslutt utarbeider man kontrollrutiner som gjennomføres jevnlig for å kontrollere at tiltakene virker etter hensikten. Denne fremgangsmåten og rutinene kan organiseres og dokumenteres i et styringssystem for informasjonssikkerhet.

Et slikt styringssystem er en del av internkontrollen. På dette området er det imidlertid utviklet standarder for å håndtere dette ryddig med minst mulig ressursforbruk. For å gjøre oppgavene i forbindelse med informasjonssikkerhet enklere for deg, beskrives informasjonssikkerhet i eget kapittel nedenfor.

2.2 Hva er personopplysningsloven og -forskriften?

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvern hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene.

Personopplysningsforskriften gir utfyllende og mer detaljerte krav om behandling av personopplysninger.

Eksempler på handlinger som normalt er krenkelser av personvernet:

- At personopplysninger behandles skjult for oss.
- At flere og mer inngående personopplysninger enn nødvendig samles inn.
- At personopplysninger ikke slettes når det ikke lengre er behov for de.
- At den registrerte ikke får innsyn i opplysningene om seg selv.
- At personopplysningene som behandles er feilaktige.
- At personopplysningene tilflyter uvedkommende.

2.3 Hva er personopplysninger og sensitive personopplysninger?

Personopplysninger

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson.

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson. For eksempel en persons navn, adresseinformasjon og lønn, referanseuttalelser om en person hos et rekrutteringsfirma, oppgavebesvarelser fra skoleelever, klientopplysninger ved krisesentre, skyldneropplysninger i inkassoselskaper, kundeopplysninger i nettbokhandler og klientopplysninger i advokatselskaper. Noen av de nevnte opplysningene vil også være sensitive personopplysninger.

Sensitive personopplysninger

Sensitive personopplysninger er personopplysninger innenfor bestemte kategorier som beskrevet i loven. Dette omfatter opplysninger 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

Sensitive personopplysninger:

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

Årsaken til at det er en egen kategori for sensitive personopplysninger, er at det knytter seg et særlig behov for vern rundt disse. De sensitive personopplysningene ses normalt på som mer inngripende for den enkelte, og regelverket stiller strengere vilkår for at disse kan behandles. Misbruk eller spredning av sensitive personopplysninger vil også normalt få større konsekvenser for den enkelte, og det er et behov for ekstra sikring av slike opplysninger.

2.4 Hva er et personvernombud?

Personvernombud

Den viktigste oppgaven til et personvernombud er å være en ressursperson, både for den behandlingsansvarlige og for de som er registrert.

Personvernombudet bør være en som kjenner virksomheten, hvilke formål som ligger til grunn for behandlingen, hvilke fremgangsmetoder som benyttes og hvilke behandlingssystem som er innført.

Et personvernombud kan både innad i virksomheten og utad fremstå som en person med spesialkompetanse og kan bistå i for eksempel opplæring og klagesaksbehandling. Utnevnelsen av personvernombud åpner også for lettelser i forhold til den lovpålagte meldeplikten til Datatilsynet. Det kan være en stor fordel for en virksomhet å ha en slik person som man kan henvende seg til med spørsmål rundt behandling av personopplysninger. Virksomhetens leder kan ikke være personvernombud.

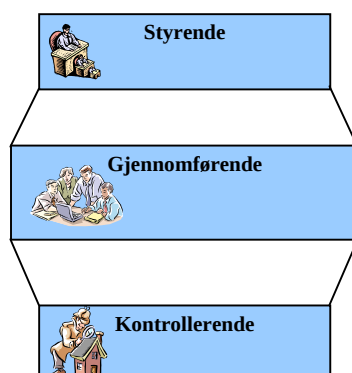
Mer informasjon om dette finner du på www.datatilsynet.no/personvernombud.

2.5 Internkontrollens dokumentasjon

Denne veilederen viser anbefalt fremgangsmåte for å iverksette internkontroll og sørge for tilfredsstillende informasjonssikkerhet. Veilederen henviser til et sett av maler med dokumenter som skal fylles ut og som er nødvendig for å dokumentere internkontroll. Dokumentasjonen er delt i 3 emner:

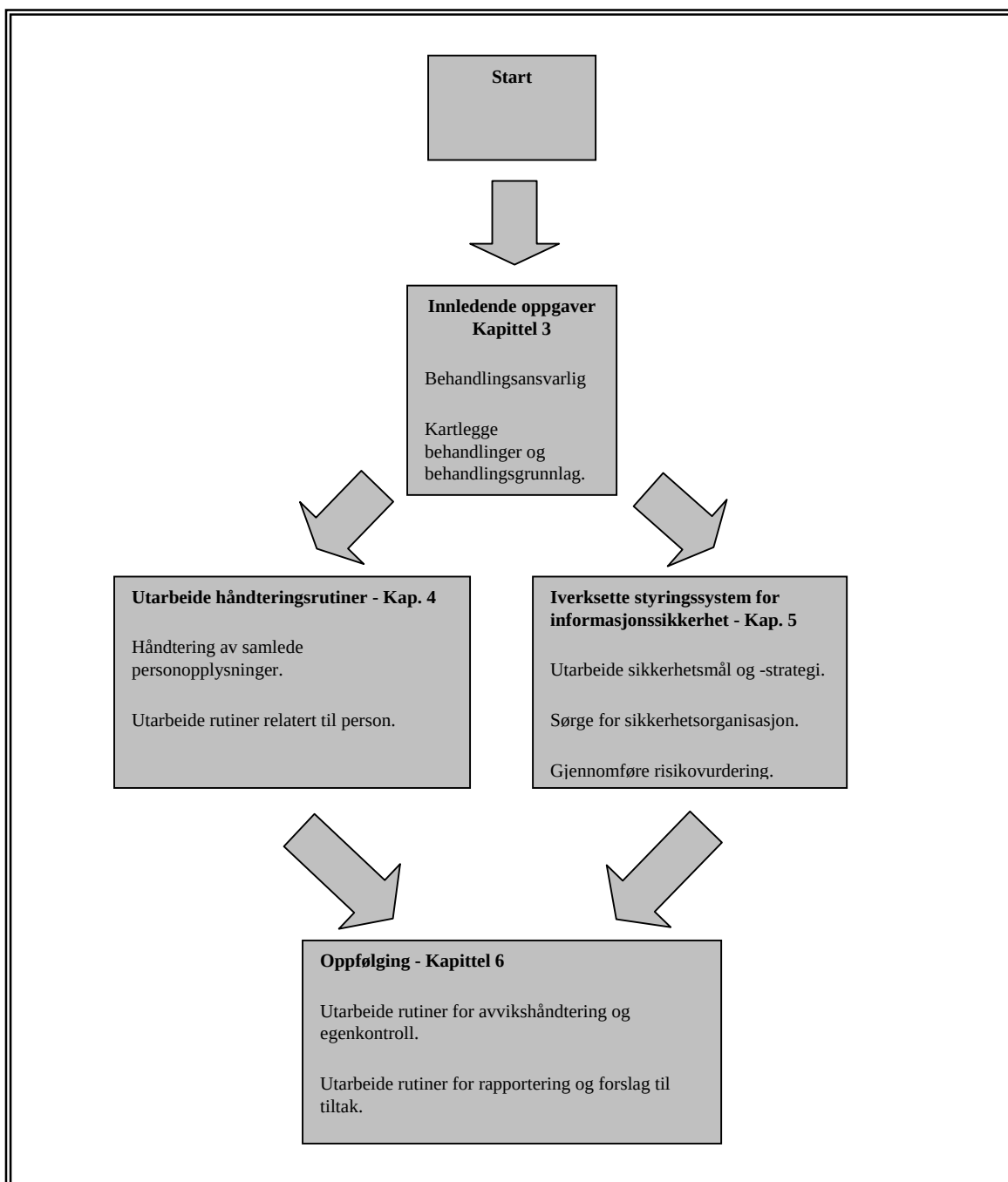
- Styrende dokumentasjon som ledelsen er ansvarlig for å utarbeide.
- Gjennomførende dokumentasjon med rutiner og tiltak for daglig drift.
- Kontrollerende dokumentasjon med rutiner for oppfølging, korrigering og forbedring av internkontroll og informasjonssikkerhet.

Se vedlegg 2 (bakerst i veilederen) for en oversikt over dokumentene som inngår i settet med maler. Bruk denne oversikten som en referanse gjennom arbeidet.



Figur 1 Dokumentasjon for internkontroll

2.6 Prosessen for å etablere internkontroll



Figur 2 Oppgaver i prosessen

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

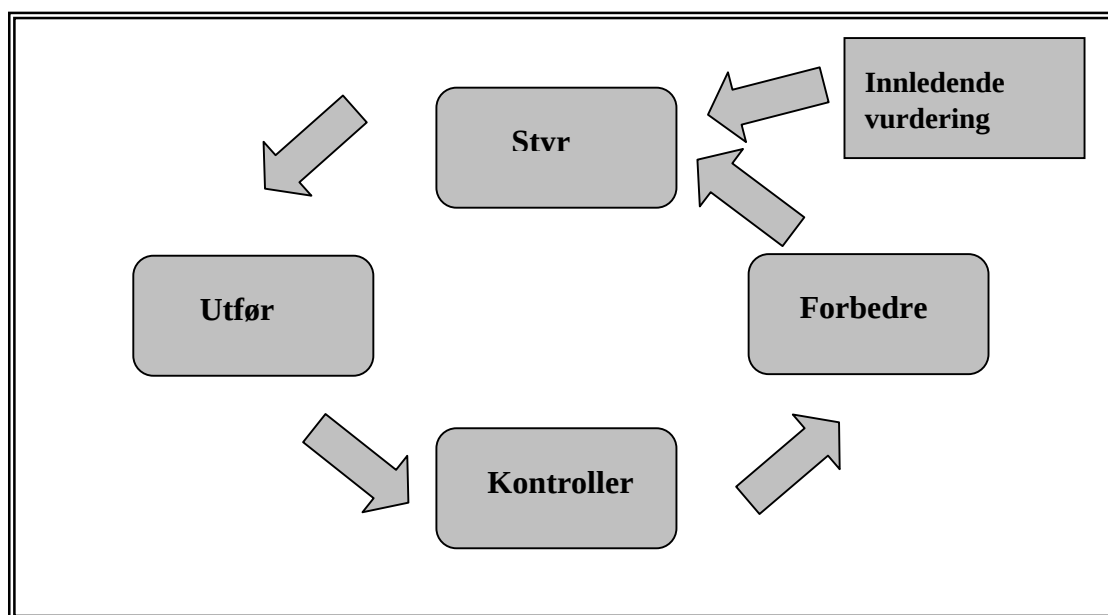
Kapittel 3 beskriver oppgaver som det er nødvendig å gjennomføre før man kan utarbeide rutiner og vurdere nødvendige sikkerhetstiltak. Oppgaver i kapittel 3 bør ferdigstilles før man forsetter med 4 og 5.

Kapittel 4 beskriver krav til rutiner for håndtering av personopplysninger samt gir eksempler på rutiner. Oppgaver i kapittel 4 kan gjennomføres i parallell med oppgaver i kapittel 5.

Kapittel 5 beskriver etablering av styringssystem for informasjonssikkerhet samt gir eksempler.

Kapittel 6 beskriver etablering av rutiner for oppfølging, drift og vedlikehold av rutineverk og sikkerhetstiltak. Også dette kapitlet gir eksempler på rutiner som kan tilpasses egen virksomhet.

2.7 Vedlikehold av internkontrollen



Figur 3 Innføring, oppfølging, drift og vedlikehold

Etter at internkontrollen er etablert, må man sørge for at den holdes ved like og blir tilpasset organisasjonen og omgivelsene. Faktorer som man må ta hensyn til, er for eksempel:

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

3 Innledende oppgaver

Bakgrunnskunnskap	Innledende oppgaver	Håndteringsrutiner	Informasjonssikkerhet	Oppfølging
-------------------	---------------------	--------------------	-----------------------	------------

3.1 Skaff kunnskap

3.1.1 Generelt

En virksomhet må ha et minimum av kunnskap selv og må ellers sørge for å ha tilgang til nødvendig kunnskap om personopplysningsloven og personopplysningsforskriften. Dette er nødvendig for å kunne starte med innføring av internkontroll.

Krav til internkontroll i en virksomhet omfatter for det første krav til kunnskap om gjeldende regler for behandling av personopplysninger. Videre skal virksomheter som behandler personopplysninger, identifisere plikter som virksomheten er pålagt å overholde.

3.1.2 Henvisninger til ytterligere informasjon

Annen relevant informasjon fra Datatilsynet:

- Temahefte - Internkontroll og informasjonssikkerhet.
- Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.
- Veileder - Risikovurdering av informasjonssystemer.

Informasjon fra Lovdata:

- Personopplysningsloven
- Personopplysningsforskriften
- Helseregisterloven

Sjekkpunkt: Kunnskap

- ☐ Virksomhetsleder har et minimum av kunnskap selv og eventuelt tilgang til nødvendig kunnskap eller kompetanse om personopplysningsloven og personopplysningsforskriften.

3.2 Virksomhetsleder er behandlingsansvarlig

Den som er ansvarlig for at personopplysningsloven følges og at internkontroll etableres, er den behandlingsansvarlige. Normalt er den behandlingsansvarlige representert med virksomhetens daglige leder eller administrerende direktør.

Som for resten av regelverket, er det den behandlingsansvarlige, altså virksomhetslederen, som er ansvarlig for at kravene til internkontroll etterleves.

Kravet til internkontroll i personopplysningsloven er: "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." Den behandlingsansvarliges ansvar omfatter blant annet å

- bestemme formålet med behandlinger av personopplysninger.
- påse at det er utarbeidet rutiner både for oppfyllelse av virksomhetens plikter og de registrertes rettigheter.

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

- Sikkerhetsmål og sikkerhetsstrategi.
- Sikkerhetsorganisasjon.
- Dokumenterte rutiner og tekniske tiltak for oppfyllelse av sikkerhetsstrategi.

Ansvaret omfatter også at det årlig avsettes tilstrekkelige ressurser, både personalmessige og økonomiske, slik at tilfredsstillende internkontroll opprettholdes.

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

Sjekkpunkt: Virksomhetsleder

- ☐ er bevisst på rollen og medfølgende ansvar som behandlingsansvarlig.
- ☐ har 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 vil i så fall utarbeide en plan for innføringen og være ansvarlig for å nå et definert resultat til et visst tidspunkt.

Leveransene prosjektet skal levere, er beskrevet i "Sjekkpunkt"-tekstboksene videre i denne veilederen. Forventet dokumentasjon ser man av oversikten i vedlegg 2.

Sjekkpunkt: Prosjekt for innføring (Opsjon)

- ☐ Prosjektleder har blitt utnevnt.
- ☐ Det er utarbeidet prosjektplan med leveranser, milepeler og ressurspersoner.
- ☐ Berørte avdelinger har blitt informert.
- ☐ De ulike avdelingene har akseptert planlagt ressursbruk.
- ☐ Det er besluttet hvem som skal godkjenne leveransene.

3.4 Støtteverktøy - kontroll mot personopplysningsforskriften

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

Datatilsynet har gjort tilgjengelig et verktøy som støtter gjennomføring av oppgavene for oppfyllelse av 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.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Paragrafer og ledd i personopplysningsforskriften (POF)	Datatilsynets kommentarer til forskriften	Krav utledet fra paragrafene i POF	Oppgavetype	Ansvar	Status	Begrunnelser for annen status enn 'OK'								Virksomhetens dokumenter
1	§ 2-1	§ 2-1 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
2	§ 2-1	§ 2-1 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
3	§ 2-2	§ 2-2 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
4	§ 2-2	§ 2-2 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
5	§ 2-3	§ 2-3 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
6	§ 2-3	§ 2-3 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
7	§ 2-3	§ 2-3 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
8	§ 2-3	§ 2-3 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		
9	§ 2-3	§ 2-3 kommentarer				Budsjett	Personell	Kultur	Teknologi	Tid	Skilte	Andre		

Figur 4 Eksempel på skjermbilde fra kontrollverktøy

En kort veiledning til bruk av verktøyet er som følger:

- Det er radene med hvit bakgrunn som skal fylles ut for de ulike oppgavene.
- Kolonne A inneholder hyperlink til paragrafer og ledd i personopplysningsforskriften.
- Kolonne B inneholder hyperlink til Datatilsynets kommentarer til forskriften.
- Kolonne C er krav utledet fra paragrafene i personopplysningsforskriften.
- I kolonne D velges oppgavetype som; Rammeverk, organisatorisk sikkerhetstiltak, teknisk sikkerhetstiltak, oppfølgingsaktivitet eller forbedringsarbeid.
- I kolonne E er det mulig å registrere ansvarlig person eller rolle.
- Kolonne F gir mulighet for å angi status; OK, delvis, ikke OK.
- I kolonne G-N kan eventuelle begrunnelser for at kravet ikke er helt eller delvis oppfylt legges inn.

I kolonne O noteres relevante dokumenter, rutiner, prosedyrer, etc. som er relevante for sikkerhetskravet. Disse kan med fordel legges inn som hyperlinker slik at det vil være enkelt å finne riktig dokumentasjon (en link pr. rad i regnearket - utvid med flere rader ved behov).

Se også veiledning som er tilgjengelig under egen "flik" i verktøyet.

3.5 Virksomhetens behandlinger

Virksomheten skal ha en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse.

Oversikten kan føres i dokumentet **Styringsdokument internkontroll**.

Oversikten er sentral for at virksomheten skal være i stand til å ivareta pliktene sine. Oversikten danner også grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi, og vil være underlag ved risikovurderinger.

Oversikten over personopplysninger som behandles skal 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:

1. Dersom kartlegging gjelder en større virksomhet, kan sikkerhetsansvarlig eller prosjektleder sende ut forespørsel om behandling av personopplysninger til hver avdelingsleder. 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.

Eksempel på oversikt over personopplysninger som behandles:

Informasjon Formål	Behandlings- grunnlag	Melding/ Konsesjon	Klassi- fikasjon	Sikr. tiltak	Lagring og kommuni- kasjon	Opplysn. omfang	Av- deling	System-/ dataeier
Lønn og personal: - lønnsopplysn. - personalopplysn.			Person- opplysning- er			Ca. 130 ansatte		
Barnevern: - vurdering og tiltak			Sensitive person- opplysning- er			Ca. 68 barn og foresatte		
Helse opplysninger: - pasientjournal			Sensitive person- opplysning- er			Ca. 413 pasienter		
Elevadministrasjon - elever / foresatte - lærere			Person- opplysning- er			Ca. 219 søkere		
Hendelsesregister: - logg over brudd			Person- opplysning- er			Arkivlogg, nettverks- logg og serverlogg, PC-logger		
Kunde- opplysninger - Salgs- og leveransekontakter			Person- opplysning- er			Ca. 8000		

Sjekkpunkt: Det er utarbeidet en skriftlig oversikt over alle personopplysninger som behandles i virksomheten

- ☐ identifisert med behandling / formål.
- ☐ kategorisert i personopplysninger og sensitive personopplysninger.
- ☐ med beskrivelse av hvilke dataelementer som omfattes.
- ☐ med avdeling som utfører behandlingene og ansvarlige som "eier" opplysningene.

3.6 Behandlinger og behandlingsgrunnlag

3.6.1 Identifisere formål

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

Behandlingenes overordnede formål dokumenteres i dokumentet **Sikkerhetsmål og –strategi**.

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 standpunkt karakter og utstede vitnemål.

3.6.2 Fastsette behandlingsgrunnlaget

Det er ikke tillatt å behandle personopplysninger uten at det finnes et behandlingsgrunnlag. Personopplysningsloven § 8 gir vilkår for å behandle personopplysninger;

Personopplysninger (jf. § 2 nr. 1) 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 registrerte, 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, eller

f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Personopplysningsloven § 9 gir vilkår for å behandle sensitive personopplysninger;

"Sensitive personopplysninger (jff. § 2 nr. 8) 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, eller*
- 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 ... "*

3.6.3 Vurdere om formål er i samsvar med hjemmel

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

Hvis en av behandlingene ikke faller innenfor eksisterende behandlingsgrunnlag, må virksomheten avvike behandlingen eller sørge for at det etableres et behandlingsgrunnlag, eksempelvis ved innhenting av samtykke.

Formål, behandlingsgrunnlag og tilhørende meldekrav i forhold til type personopplysninger føres i dokumentet **Styringsdokument internkontroll**. Overordnede formål med behandlinger skal beskrives i sikkerhetsmål i dokumentet **Sikkerhetsmål og sikkerhetsstrategi**.

Sjekkpunkt: Behandlinger

- ☐ Alle virksomhetens behandlinger av personopplysninger med formål er identifisert.
- ☐ Virksomheten har gjennomgått alle behandlinger og vurdert behandlingsgrunnlaget.
- ☐ Behandlinger som ikke har behandlingsgrunnlag er avvirket, alternativt er det sørget for et behandlingsgrunnlag for disse.
- ☐ Overordnet formål med behandlinger er beskrevet i Sikkerhetsmål og –strategi.

Eksempel på oversikt over personopplysninger som behandles:

Informasjon Formål	Behandlings- grunnlag	Melding/ Konsesjon	Klassi- fikasjon	Sikr. tiltak	Lagring og kommu- nikasjon	Opplysn. omfang	Av- deling	System-/ dataeier
Lønn og personal: - lønnsopplysn. - personalopplysn.	Person- opplysnings- loven, § 8f	Unntatt i forskriften	Person- opplysning- er			Ca. 130 ansatte		
Barnevern: - vurdering og tiltak	Barnevern- loven, § 3-1	Meldt 14.01.2004	Sensitive person- opplysning- er			Ca. 68 barn og foresatte		
Helse opplysninger: - pasientjournal	Helse- personellov en § 39 flg.	Meldt 14.01.2004	Sensitive person- opplysning- er			Ca. 413 pasienter		
Elevadministrasjon - elever / foresatte - lærere	Opplærings- loven § 13- 5		Person- opplysning- er			Ca. 219 søkere		
Hendelsesregister: - logg over brudd	Person- opplysnings- loven, § 13	Unntatt i forskriften	Person- opplysning- er			Arkivlogg, nettverks- logg og serverlogg, PC-logger		
Kunde- opplysninger - Salgskontakter - Leveranse- kontakter	Person- opplysnings- loven, §		Person- opplysning- er			Ca. 8000		

3.7 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 dokumentet **Styringsdokument internkontroll**. Begrunnelsene gjelder behovet for å behandle personopplysningene for å kunne levere virksomhetens tjenester. De overordnede føringene er krav og plikter som virksomheten blir underlagt på grunn av behandlingen av personopplysninger og eventuelt krav og plikter gjennom andre lover og forskrifter.

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 dokumentet **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 eller hvordan:

- 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.
- Brannmur 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 ved virksomheten.

Andre føringer er krav til hendelseshåndtering, egenkontroll, avviksbehandling og ledelsens gjennomgang som kan beskrives under strategier i dokumentet **Sikkerhetsmål og -strategi**.

Sjekkpunkt: Overordnede rammer

- ☐ Ledelsens begrunnelse for behandling av personopplysninger og føringer for internkontroll og bruk av informasjonsteknologi i virksomheten er beskrevet i dokumentene **Styringsdokument internkontroll** og **Sikkerhetsmål og -strategi**.

Disse områdene er nærmere beskrevet senere i denne veilederen.

3.8 Identifisere plikter

Behandling av personopplysninger medfører plikter for virksomheten. Ulike opplysninger og ulike formål medfører at ingen virksomheter er like og hver virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin situasjon. Tilsvarende gjelder for vedlikehold av internkontrollen - hver virksomhet må tilpasse kontrollrutinene slik at rutiner og tiltak gjenspeiler behovene over tid.

I kapittel 4 er det beskrevet krav til ulike rutiner og eksempler på utforming. Det er viktig å være klar over at for mange virksomheter vil rutinene i kapittel 4 ikke være fullstendige i forhold til virksomhetens behov. For eksempel kan en virksomhet ha behov for rutiner i forhold til aidentifisering av personopplysninger eller i forhold til hvordan den gjennomfører anonymisering.

Virksomheten er pålagt gjennom personopplysningslovens §14 og -forskriftens kapittel 3 å identifisere alle plikter som den er underlagt og så utarbeide rutiner og tiltak som er tilpasset og fullstendige i forhold til pliktene.

Vær oppmerksom på at også andre regelverk kan stille krav om internkontroll for andre formål enn å sikre forsvarlig håndtering av personopplysninger. 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.

Sjekkpunkt: Identifisering av plikter

- ☐ Alle plikter som virksomheten er underlagt som følge av behandling av personopplysninger, er identifisert.
- ☐ Utarbeidelse av rutiner utover de som er beskrevet i kapittel 4 i henhold til behov, er planlagt for utarbeidelse og iverksettelse.

4 Håndteringsrutiner

Bakgrunnskunnskap	Innledende oppgaver	Håndteringsrutiner	Informasjonssikkerhet	Oppfølging
-------------------	---------------------	--------------------	-----------------------	------------

4.1 Generelt om håndteringsrutiner

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. Kapitlet gir eksempler som en virksomhet kan ta utgangspunkt i for egen etablering av rutiner. Andre rutiner utover dette kan vise seg nødvendige etter risikovurdering.

Rutiner for

- iverksettelse og opphør av behandling,
- overholdelse av melde- og eventuell konsesjonsplikt,
- sletting av personopplysninger,
- utlevering av personopplysninger til andre,
- sikring av kvalitet av personopplysninger,
- innhenting og kontroll av samtykke,
- oppfyllelse av plikt til informasjon,
- innsyn, retting og supplering,
- ivaretagelse av eventuell reservasjonsrett og
- innsyn i privat e-post og private filområder

kan beskrives i dokumentet **Rutiner for håndtering av personopplysninger**.

Dette rutinedokumentet tilhører kategorien gjennomførende dokumentasjon. Se vedlegg 2 for en oversikt over de ulike kategoriene av dokumentasjon samt hvilke dokumenter som inngår i kategoriene.

Håndteringsrutinene bør utformes i henhold til en felles mal for at de skal bli enkle å bruke og for at det skal være enkelt 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.

Følgende er elementer i rutine for iverksettelse av behandling og må konkretiseres av den behandlingsansvarlige:

- 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 4.4.4.
- Gjennomføre risikovurdering.
- Gjennomføre nødvendige sikkerhetstiltak.
- Utarbeide rutiner for oppdatering av nye rutiner.

Følgende er elementer i rutine for opphør av behandling og må konkretiseres av den behandlingsansvarlige:

- Kontroller at oversikten over opplysninger stemmer.
- Er det grunnlag for videre oppbevaring med et nytt behandlingsgrunnlag?
- Slette lagrede relaterte personopplysninger.

4.2.2 Overholdelse av melde- og eventuell konsesjonsplikt

Meldeplikt

All behandling av personopplysninger er i utgangspunktet meldepliktig, ref. personopplysningsloven §31. En del behandlinger er imidlertid unntatt i personopplysningsforskriften. Dette gjelder blant annet kunderegistre, personalregistre og foreningers medlemsregistre. Det stilles vilkår til fritaket fra meldeplikt. Krav til rutiner og sikkerhetstiltak gjelder selv om behandlingen er unntatt meldeplikt.

Eksempel - Rutine for melding av behandling av personopplysninger

- Den behandlingsansvarlige skal gi melding til Datatilsynet før 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.
- Det er unntak dersom man har personvernombud, se kapittel 2.4, Personvernombud.
- Det skal gis ny melding tre år etter at forrige melding ble gitt selv om det ikke har skjedd endringer av behandlinger.

Datatilsynet har opprettet en tjeneste på sitt nettsted for innsending av elektronisk meldeskjema. Denne tjenesten er rask og enkel å bruke og gir kvittering for innsending via oppgitt e-postadresse.

Konsesjonsplikt

Noen behandlinger er konsesjonspliktige, og skal dermed ikke meldes. Meldeplikten blir 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, i stedet gjort konsesjonspliktige ved forskrift. Dette dreier seg om behandling av personopplysninger innen telesektoren, i 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 finnes i §§ 33 – 35 i personopplysningsloven og i kapittel 7 i personopplysningsforskriften.

Datatilsynet har opprettet en tjeneste på sitt nettsted for nedlasting av søknadsskjema. Denne tjenesten gir tilgang til skjema i pdf-format samt et veiledningsdokument og er rask og enkel å bruke. Skjema og veileder for utfylling finnes på Datatilsynets nettsted.

Eksempel - Rutine for søking om konsesjon for konsesjonspliktig 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 Rutine 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 er nødvendig å lagre lenger. Krav til sletting kan inntreffe på grunn av en organisatorisk endring, f.eks. bortfall av formål eller på grunn av at et tidskrav for lagring utløper.

Det kan være grunner relatert til historiske, statistiske eller vitenskapelige formål som åpner for lengre lagring under visse forutsetninger. Se nevnte paragraf for detaljer.

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

- Vurdere krav til sletting av personopplysninger ved endringer i tjenester som ytes av virksomheten, ved endringer i organisering og ved endringer av informasjonssystemer.
- Vurdere krav til sletting av personopplysninger månedlig basert på oversikt over opplysninger og lagringstid.
- Behandlingsansvarlig har ansvar for godkjenning av sletting av utvalgte opplysninger.
- Utstede arbeidsordre for sletting av utvalgte opplysninger i alle kopier.
- Verifisere sletting ved kontroll av logger for sletting av opplysninger i alle kopier.

Eksempel på rutine for sletting:

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

1) Salgssjef er ansvarlig for personopplysninger om kunder. Salgssjef skal:

- sørge for at personopplysninger relatert til kundeforholdet slettes etter 3 års inaktivitet i kundeforholdet. Dette gjelder 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 og
- 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 et 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 og
- 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 ny behandling som krever behandlingsgrunnlag etter personopplysningsloven. Dersom ikke annet behandlingsgrunnlag finnes, må den behandlingsansvarlige som ønsker å utlevere data, ha samtykke fra de(n) registrerte for å utlevere opplysningene.

Utlevering omfatter ikke bruk av eksisterende personopplysninger til ny behandling innenfor samme virksomhet. I dette tilfellet må man sørge for et behandlingsgrunnlag. Utlevering omfatter heller ikke oversendelse av personopplysninger til databehandlere.

Utlevering etter dette kapitlet omfatter ikke innsyn i egne personopplysninger. Innsyn er behandlet i kapittel 4.3.3.

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

- Virksomhetsleder kan delegere myndighet til leder eller medarbeider i virksomheten som skal godkjenne utlevering av personopplysninger. Dersom dette ikke er gjort, skal kun virksomhetsleder selv godkjenne utlevering. Slik delegering av myndighet skal være dokumentert.
- 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 personopplysningslovens §8 eller §9 (inkl. §8).

4.2.5 Rutiner for sikring av kvalitet av personopplysninger

Opplysningene skal holdes korrekte og oppdaterte i forhold til formålet med behandlingen (personopplysningsloven §11).

Eksempel - Fremgangsmåte for oppdatering av personopplysninger fra registrerte

- Teknisk funksjon i nettsted som krever at bruker bekrefter, eventuelt oppdaterer, egne kontaktopplysninger ved pålogging - en gang pr. halvår .

Sjekkpunkt: Virksomheten har dokumenterte rutiner for

- ☐ iverksettelse og opphør av behandling av personopplysninger.
- ☐ overholdelse av meldeplikt og eventuelt konsesjonsplikt.
- ☐ sletting av personopplysninger.
- ☐ 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, jf. personopplysningsloven § 2 nr. 7. Loven stiller ingen formkrav til samtykket, men Datatilsynet anbefaler at det innhentes skriftlig. Skriftlighet vil lette bevisproblemer i situasjoner hvor det reises tvil om hva den registrerte har samtykket til.

Et samtykke kan trekkes tilbake når som helst.

Eksempel - Innhenting av samtykke før registrering på netthandelssted

- Kunde går inn på netthandelssted for å lese produktnyheter.
- Nettstedet sender et vindu/skjerm bilde 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

Den behandlingsansvarlige er pålagt å informere den registrerte om behandlingen før den tar til (personopplysningsloven §§ 19 og 20). Informasjon skal gis av eget tiltak, uten at den registrerte krever det, og uten kostnader for den registrerte, jf. personopplysningsloven § 17.

4.3.3 Rutiner for innsyn, retting og supplering

Innsyn

Rett til innsyn i personopplysninger er beskrevet i personopplysningsloven § 18:

"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 behandlingsansvarliges plikter,*
- c) formålet med behandlingen,*
- d) beskrivelser av hvilke typer personopplysninger som behandles,*

e) hvor opplysningene er hentet fra, og

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, og

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."

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

"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, og

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."

Plikt til å informere når det samles inn opplysninger fra andre enn den registrerte, er beskrevet i personopplysningsloven § 20:

"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, eller
- c) det er på det rene at den registrerte allerede kjenner til informasjonen varslet 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."

Virksomheten skal ha rutine for behandling av forespørsel om innsyn fra registrert.

Følgende er elementer i rutine for behandling av forespørsel om innsyn og må konkretiseres av den behandlingsansvarlige:

- Mottak av forespørsel om innsyn for mulig registrert person.
- Eventuelt be om skriftlig bekreftelse på forespørsel.
- Formidling av forespørselen til aktuelle system- eller dataeiere.
- Melding til forespørter dersom forespørselen ga negativt resultat.
- Dersom forespørter er registrert; skrive ut eventuelt utarbeide i henhold til intern rutine, informasjon fra aktuelle systemer som spesifisert i personopplysningsloven §18, a) - f).
- Samle informasjon fra aktuelle systemer og oversende til den som forespør.

Retting og supplering

Personopplysninger skal være tilstrekkelige og relevante for formålet med behandlingen (personopplysningsloven § 11). 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 av 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 rutine for retting når det avdekkes feil internt i virksomheten.

Følgende er elementer i rutine for behandling av forespørsel om retting og supplering og må konkretiseres av den behandlingsansvarlige:

- Mottak av forespørsel om retting eller supplering for registrert.
- Formidling av forespørsel til aktuelle system-/dataeiere.
- Verifisere korrekthet av forespurte endringer av opplysninger.
- Hvis verifisert, utstede arbeidsordre for oppdatering av system(er).
- Bekrefte skriftlig til den som forespurte om endringer som er gjort.

4.3.4 Ivaretagelse av eventuell reservasjonsrett

Maskinell behandling

I den grad den behandlingsansvarlige utfører fullt automatiserte avgjørelser i forhold til den registrerte, kan den registrerte kreve manuell behandling av saken/avgjørelsen med mindre den registrertes personverninteresser varetas på tilstrekkelig måte og avgjørelsen er hjemlet i lov eller knytter seg til oppfyllelse av kontrakt.

Den behandlingsansvarlige skal ha rutiner for manuell behandling dersom det er aktuelt.

Direkte markedsføring

Den registrerte kan kreve sitt navn sperret mot bruk til direkte markedsføring uavhengig av medium. Sperring kan kreves både i det sentrale reservasjonsregisteret og i markedsførers adresseregister.

Dersom den behandlingsansvarlige driver med direkte markedsføring, skal han ha rutiner for å unngå å kontakte personer som har reservert seg mot dette.

Følgende er elementer i rutine for sperring av navn i markedsførers adresseregister og må konkretiseres av den behandlingsansvarlige:

- Mottak av forespørsel om sperring av navn i markedsførers adresseregister.
- Før bruk av adresseregister og senere kvartalsvis; markedsfører skal "vaske" sitt adresseregister mot sentralt reservasjonsregister.
- Markedsfører skal utføre sperringer som er blitt forespurt av den registrerte direkte samt sperringsendringer som overføres fra sentralt register.
- Ved direkte markedsføring ved hjelp av adresseregister; markedsfører skal opplyse mottakere om hvem som har gitt personopplysningene som ligger til grunn.

4.3.5 Innsyn i privat e-post og private filområder

I utgangspunktet er det ikke adgang for arbeidsgiver til å gjøre innsyn i ansattes personlige e-postkasse og filer på personlige filområder. For e-post forutsetter dette at den ansatte har e-postadresse med eget navn eller initialer ved virksomheten eller annen adresse ved virksomheten som bare disponeres av henne.

Det er arbeidsgiver som stiller til rådighet utstyr for den ansatte og er ansvarlig for at IT-løsninger brukes iht. lover, forskrifter og interne rutiner. Virksomhetsleder har derfor anledning til innsyn i virksomhetsrelatert e-post under visse forutsetninger. Forutsetninger og rutiner beskrevet i dette kapitlet, gjelder så langt det passer også for filer på personlig filområde.

Det er anbefalt at den ansatte har en egen mappe i e-postsystemet og egen katalog på personlig filområde merket "Privat" for henholdsvis privat e-post og private filer. E-post i andre mapper og filer i andre kataloger ansees som virksomhetsrelaterte. Dette bør være avtalt skriftlig (i sikkerhetsinstruks) med den ansatte.

I følgende situasjoner kan innsyn likevel være aktuelt:

A) Ved fravær dersom

- det er god grunn til å tro at det er kommet virksomhetsrelaterte meldinger i e-postkassen som arbeidsgiver trenger av driftshensyn.
- den ansatte samtykker eller virksomheten har skriftlige retningslinjer som de ansatte er kjent med og som klart og tydelig sier hvilke fraværssituasjoner som kan innebære innsyn.

B) Ved opphør av arbeidsforholdet dersom

- det er behov for å sortere ut virksomhetsrelatert e-post før innholdet slettes og e-postkassen avsluttes i tråd med skriftlige retningslinjer.
- dette er avtalt med den enkelte.

C) Ved begrunnet mistanke om at

- e-post har et innhold som er straffbart.
- e-post som inngår som et ledd i gjennomføringen av en straffbar handling.
- det sendes e-post som medfører et grovt brudd på plikter som følger av arbeidsforhold, reglement eller annet skriftlig regelverk knyttet til ansettelsesforholdet.

Dersom et av vilkårene i punkt C er oppfylt, kan det også gjøres innsyn i privat e-post på den personlige e-postkassen. Ved mistanke om straffbare forhold bør politiet kontaktes. Dersom bare punkt A og B er oppfylt, kan arbeidsgiver ikke foreta innsyn i privat e-post.

Se www.datatilsynet.no for utfyllende informasjon. Reguleringen på dette området er under endring.

Eksempel på rutine for innsyn i e-post

Arbeidstakeren skal varsles før innsyn.

Disse tre punktene skal i tillegg gjennomføres:

1. Arbeidstakeren må få tilbud om å være tilstede ved åpningen selv, eller selv få utpeke en representant som kan være tilstede.
2. Metoden for innsyn må være beskrevet før man setter i gang.
3. Innsynet skal dokumenteres, inklusive hvorfor innsynet ble foretatt, hvem som fattet beslutningen, hvem som var tilstede, metode for innsyn og resultatet.

Datatilsynet anbefaler:

- Ha klare og tydelige retningslinjer om bruk av virksomhetens datasystem. Legg særlig vekt på tiltak som kan hindre behovet for innsyn. Dette kan for eksempel være bruk av såkalt fraværsassistent ved planlagt fravær. Videre må det tydelig gå frem om det skal være tillatt å benytte den personlige e-post adressen til privat bruk.
- Dersom virksomheten tillater privat bruk, må man unngå uklare ord og fraser i beskrivelsen av omfang (som ”rimelig privat bruk er tillatt” og ”begrenset privat bruk”). Vær konkret!
- Definer hva som anses som et grovt brudd på plikter i virksomheten.
- Lag egne e-postadresser til tillitsvalgte som kan benyttes i deres tillitsverv.

Sjekkpunkt: Virksomheten har dokumenterte rutiner for

- ☐ innhenting og kontroll av samtykke.
- ☐ oppfyllelse av plikt til informasjon.
- ☐ innsyn, retting og supplering.
- ☐ ivaretagelse av eventuell reservasjonsrett.
- ☐ innsyn i privat e-post og private filområder.

5 Informasjonssikkerhet

Bakgrunnskunnskap	Innledende oppgaver	Håndteringsrutiner	Informasjonssikkerhet	Oppfølging
-------------------	---------------------	--------------------	-----------------------	------------

5.1 Innledning

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til informasjonsverdier. Risiko relateres vanligvis til tre ulike aspekter ved informasjonssikkerhet, henholdsvis

- konfidensialitet (uvedkommende får ikke tilgang på opplysningene),
- integritet (opplysningene endres ikke uautorisert eller utilsiktet) og
- tilgjengelighet (opplysningene er tilgjengelige når vi trenger dem).

Håndtering av informasjonssikkerhet inngår i internkontrollen i virksomheten. Sikkerhetsdokumentasjonen følger strukturen som beskrevet i kapittel 2.5;

- Styrende dokumentasjon - som ledelsen er ansvarlig for å utarbeide.
- Gjennomførende dokumentasjon - med rutiner og tiltak for sikker drift.
- Kontrollerende dokumentasjon - med rutiner for oppfølging, korrigering og forbedring av informasjonssikkerheten.

Ved innføring av internkontroll, må en virksomhet først identifisere hvilke informasjonsverdier den besitter, inkludert personopplysninger. Deretter må det gjennomføres en risikovurdering for å vurdere trusler mot verdiene på de tre områdene beskrevet ovenfor og avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Sikkerhetstiltakenes omfang skal stå i forhold til vurdert risiko for de ulike informasjonsverdiene. Dersom risikovurderingen viser behov for tiltak utover det som finnes i dag, planlegger man og gjennomfører systematiske tiltak for å skape et tilfredsstillende sikkerhetsnivå.

Tilslutt utarbeider man kontrollrutiner som gjennomføres jevnlig for å kontrollere at tiltakene virker etter hensikten. Denne fremgangsmåten og rutinene kan organiseres og dokumenteres i et styringssystem for informasjonssikkerhet som er en del av internkontrollen.

5.2 Sikkerhetsmål og sikkerhetsstrategi

5.2.1 Innledning

Fra innledende aktiviteter er følgende fylt inn i Sikkerhetsmål og -strategi:

- Begrunnelse for behandling av personopplysninger.

- Formål med de ulike behandlinger (overordnet).
- Føringer for bruk av IT til behandling av personopplysninger .
- Føringer for organisering av sikkerhet.

Internkontrollen skal fange opp alle krav til informasjonssikkerhet i § 2.1 i personopplysningsforskriften. Dette med det formål å oppfylle personopplysningslovens krav om "tilfredsstillende" informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet.

Vi skal her utarbeide sikkerhetsmål ("hva skal oppnås") og sikkerhetsstrategi ("hvordan skal målene nås"). Grunnlaget er lagt i kapittel 3.7, Overordnede rammer.

Sikkerhetsmål og -strategi er en del av styrende dokumentasjon og ledelsens ansvar.

5.2.2 Sikkerhetsmål

Sikkerhetsmålene omfatter ledelsens beslutninger om til hva og hvordan informasjonsteknologien skal benyttes i virksomheten for å 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. Sikkerhetsmål bør i størst mulig grad være målbare men dette er ikke alltid enkelt. De skal i alle tilfelle være retningsgivende for strategier.

Eksempler:

- Krav i relevante lover og forskrifter skal etterleves.
- Beskytte selskapets informasjonsbehandling 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 en tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov.

5.2.3 Sikkerhetsstrategi

Sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette går på fordeling av arbeidsoppgavene mellom ledelse og driftspersonell, beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Forholdet mellom ledelse, driftspersonell og den enkelte bruker må avklares her. Sikkerhetsstrategi skal gjøre rede for organisatoriske og tekniske strategiske valg. Sikkerhetsstrategien 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 iht. 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.

Sjekkpunkt: Virksomheten har ferdigstilt dokumentet Sikkerhetsmål og – strategi som omfatter

- ☐ begrunnelse og formål med behandling av personopplysninger,
- ☐ ledelsens føringer for bruk av informasjonsteknologi,
- ☐ sikkerhetsmål og
- ☐ sikkerhetsstrategi.

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 gjennomføres 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 bl.a. 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 trusselbildet som bl.a. 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.

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

Rapport fra ledelsens gjennomgang 2006	Virksomhet: XX	Skrevet av: NN	Dato: 1.12.2006	Arkivref: xx.yyyy
Deltagere:				
Virksomhetsleder NN				
Sikkerhetsansvarlig NN				
IT-driftsleder NN				
Distribusjon: Møtedeltakerne				
Saknr.	Sak	Aksjon	Ansv./ frist	
1/06	Rapporter fra utførte sikkerhetsrevisjoner. Rapportene fra sikkerhetsrevisjoner ble lagt fram uten merknader			
2/06	Behandling av registrerte sikkerhetsbrudd og logger. Innbrudd på nettsted bør gi endret sikkerhetsstrategi	Det innhentes bistand til endring.	IT-driftsleder, 15.12.06	
3/06	Behandling av foreslåtte nye løsninger. Prosjektforslaget for bruk av hjemmekontor ble godkjent.			

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

Sjekkpunkt: Ledelsens gjennomgang

- ☐ Det er dokumentert rutine i dokumentet **Ledelsens gjennomgang** for ledelsens årlige gjennomgang av informasjonssystemet og informasjonssikkerheten i virksomheten.
- ☐ Ansvar for forberedelse og innkalling er plassert.
- ☐ Det er etablert mal for rapport fra mal i dokumentet **Ledelsens gjennomgang**.

5.4 Sikkerhetsorganisasjon

Personopplysningsforskriften (§ 2-7) stiller krav til at det skal bestemmes klare ansvars- og myndighetsforhold for bruk av informasjonssystemer som behandler personopplysninger. Dvs. det skal besluttes en sikkerhetsorganisasjon og denne skal dokumenteres.

Se dokumentet **Sikkerhetsorganisasjon**. Her skal sikkerhetsorganisasjonen beskrives. Det skal etableres klare ansvars- og myndighetsforhold med utgangspunkt i beslutninger tatt av virksomhetens ledelse (sikkerhetsstrategien).

Ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeid (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 ledelse og virksomheten for øvrig.

Ansvar og myndighet skal fremgå tydelig.

Sjekkpunkt: Sikkerhetsorganisasjon

- ❑ Virksomheten har dokumentert sikkerhetsorganisasjon med rollebeskrivelser, myndighet, ansvarsområder og plikter fra virksomhetsleder til driftsansvarlig for de ulike systemene som behandler personopplysninger.

5.5 Akseptabelt risikonivå

En forutsetning for å kunne ha en forsvarlig risikostyring er at det finnes noen kriterier å styre i forhold til. Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et på forhånd akseptert nivå. Akseptkriteriene vil videre påvirkes av ytre rammevilkår og lovpålagte krav.

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

Beslutning om akseptabelt risikonivå skal blant annet uttrykkes i virksomhetens sikkerhetsmål, beskrevet i dokumentet **Sikkerhetsmål og -strategi**. Sikkerhetsmålet skal, på et overordnet nivå, beskrive formålet med bruken av informasjonsteknologi og angi sikkerhetsbehov med hensyn på 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 konsekvens og sannsynlighet. Beskrivelsen må angi prioritering mellom forskjellige sikkerhetsbehov, og – på overordnet nivå – beskrive risikoreducerende tiltak.

Detaljert beskrivelse av akseptabelt risikonivå skal inngå i underlag for gjennomføring av risikovurdering.

Eksempler på beskrivelse av akseptabelt risikonivå:

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

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

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

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 et 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.

Sjekkpunkt: Akseptabelt risikonivå

- ❑ Overordnet akseptabelt risikonivå er beskrevet i Sikkerhetsmål og -strategi.
- ❑ Detaljert akseptabelt risikonivå beskrives i form av akseptable og uakseptable hendelser i forbindelse med risikovurdering - i dokumentet **Risikovurdering**.

5.6 Gjennomføre risikovurdering

5.6.1 Generelt

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.

Risikovurderingen baseres på blant annet personopplysningsforskriften §2-1, Forholdsmessige krav om sikring av personopplysninger. Opplysninger av ulike typer/kategorier skal beskyttes "godt nok". Beskyttelsestiltak koster penger og innsats samt reduserer ofte tilgjengelighet. Derfor segmenteres nettverk og systemer slik at man ikke beskytter opplysninger mer omfattende enn nødvendig (med mindre segmentering medfører større kompleksitet og høyere kostnader enn om man behandler all informasjon på samme måte).

Formålet med risikovurdering er å undersøke hvorvidt den risiko som avdekkes 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 dokumentet **Risikovurdering**.

Eksempler på elementer som inngår i risikovurdering:

- Planlegging og oppstart.
- Avgrensning av analyseobjekt.
- Beskrivelse av trusler mot informasjonssikkerheten med hensyn til:
 - konfidensialitet

- integritet
- tilgjengelighet
- Årsaksanalyse dvs. vurdering av hvordan en uønsket hendelse kan inntreffe.
- Konsekvensanalyse dvs. vurdering av de følger en uønsket hendelse kan medføre.
- Frekvensanalyse dvs. 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.

5.6.2 Mer om uønskede hendelser

En trussel er en mulig hendelse som kan inntreffe ("uønsket hendelse").

En hendelse er en handling eller tilstandsending som kan utsette verdier for risiko – i form av mangelfull konfidensialitet, integritet eller tilgjengelighet, henholdsvis

Utlevering, tap av lagringsmedier, utsending via e-post med mer

- kan tilbakeføres
- permanent

Endring

- sporbar og kan rettes
- sporbar og permanent
- ikke sporbar

Utilgjengelighet

- avgrenset tidsrom
- permanent

Eksempler på trusler / uønskede hendelser:

- Publisering av andres navn og personnummer på Internett/web 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").

5.6.3 Mer om konsekvens

Konsekvensanalysen skal ta utgangspunkt i identifiserte trusler og analysere konsekvensene av at de ulike truslene / uønskede hendelsene inntreffer.

For å håndtere en infrastruktur med flere systemer som behandler personopplysninger på en effektiv måte, kan det være hensiktsmessig å kategorisere systemene og nettverk/eksterne kommunikasjongs grensesnitt i forhold til ulike beskyttelsesbehov 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

Konsekvens av en hendelse vil i første rekke være knyttet til verdienes – personopplysningenes – art. I tillegg vil konsekvens også avhenge av hvor mange personer som berøres. Personvernkonsekvens må rangeres høyere, eksempelvis ett nivå, dersom hendelsen får følger for mange mennesker. Dette selv om følger 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 med sikring av personopplysninger: Beskyttelse av liv/helse, økonomi og anseelse/personlig integritet for enkeltmennesker. Personvernkonsekvens skal derfor beskrives i forhold til disse begrepene - både kvalitativt og kvantitativt:

- K=4, hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.
- K=3, hendelsen kan føre til tap av helse, eller kan medføre uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse og integritet.
- K=2, hendelsen kan medføre betydelig økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis

kompromittering av opplysninger den registrerte oppfatte som krenkende, eller som andre kan gjøre nytte av).

- K=1, hendelsen kan medføre økonomisk tap – men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som følsomme).

5.6.4 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;

Eksempel - Elektronisk klientregister:

	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

	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. Dette er ok, 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 dokumentet **Risikovurdering** med kategori Katastrofal, Stor, Moderat eller Liten for de ulike personopplysningene.

5.6.5 Mer om sannsynlighet

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 et eller flere tekniske og organisatoriske tiltak, som ville redusere sannsynligheten for at denne hendelsen skulle inntreffe til et lavt nivå. Dersom kostnaden til tiltaket er begrenset i forhold til virksomheten omsetning og sikkerhetsbudsjett, er den enkleste tilnærmingen å bare gjennomføre tiltaket inneværende år etter intern prioritering.

Neste nivå er å vurdere "letthet" og "motivasjon" som indikasjon på sannsynlighet for at en hendelse skal inntreffe. Se eksempler nedenfor.

5.6.6 Vurdering av kategoriserte hendelser

I tabellen nedenfor vises hvordan hendelser kan kategorieres 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.

Hendelse	Kategori KIT	Konsekvens	Sannsynlighet	Risiko	Vurderes som akseptabel
Styreinformasjon på avveie	K	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	I	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	Tap av anseelse eller integritet for 1 ansatt i en 50-års periode	Akseptabel

			personell kan ikke omgå/bryte tiltakene		
Utilgjengelighet av personalsystem i 24 timer	T	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

Eksempel på tabell over akseptabel risiko;

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

Konsekvens: Sannsynlighet:	Liten	Moderat	Stor	Katastrofal
Lav			Sensitive opplysninger om en ansatt på avveie. Uautorisert endring av opplysninger om en ansatt	Sensitive opplysninger om alle ansatte på avveie *
Moderat	Utilgjengelighet av personalsystem i 24 timer	Budsjettinformasjon på avveie	Styreinformasjon på avveie	Konkurransesensitiv informasjon på avveie
Høy	Informasjon med lavt beskyttelsesbehov på avveie	En dags bortfall av sikkerhetskopiering. Ukjente mennesker i kontorlokalene		
Svært høy				

*) Kombinasjonen av katastrofal konsekvens og lav sannsynlighet må sees på som umulig å unngå fordi vi allerede er på den laveste sannsynlighetskategorien, og det kan være umulig å redusere konsekvensen. Derfor er denne kombinasjonen akseptabel, men man bør være bevisst mulige hendelser i denne kategorien og vurdere aktuelle tiltak.

Forklaring til konsekvens og sannsynlighet:

Konsekvens graderes etter hvor alvorlig hendelsen er for virksomheten eller for den registrerte. Dette kan måles i økonomiske tap, tap av liv og helse, og tap av anseelse både for virksomheten og den registre. 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 dokumentet **Risikovurdering**.

For mer informasjon om risikovurderinger, og utfyllende informasjon om konsekvens og sannsynlighet (eventuelt uttrykt ved bruk av letthetsbetraktning eller motivasjonsbetraktning), se Datatilsynets veileder "Risikovurdering av informasjonssystem" på www.datatilsynet.no.

Sjekkpunkt: Risikovurdering

Resultater av risikovurdering er dokumentert, inklusive vurdering av

- ☐ trusler/uønskede hendelser som kan inntreffe,
- ☐ konsekvensen av mulige hendelser og
- ☐ sannsynligheten for mulige hendelser.

5.7 Har vi akseptabel risiko?

5.7.1 Beskrivelse

Dette underkapitlet beskriver oppgaver i forbindelse med vurdering av om kartlagte trusler og/eller uønskede hendelser med tilhørende risiki ligger innenfor dokumentert akseptabelt risikonivå.

Gå gjennom hver uønsket hendelse og vurder om denne vil medføre uakseptable konsekvenser i forhold til akseptabelt risikonivå dersom den uønskede hendelsen skulle inntreffe.

Hvis trussel eller uønsket hendelse medfører risiko utover akseptabelt risikonivå - dvs. eksisterende sikkerhetstiltak er ikke gode nok til å oppfylle beskyttelsesbehov, må det settes inn tekniske og/eller organisatoriske tiltak.

Eksempler:

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. Trusler/uønskede hendelser

a) Autentiseringsmekanisme ved innlogging på nettsted er for enkel og personer utenfra med gode kunnskaper kan få tilgang til systemer med personopplysninger innenfor brannmur.

b) Ansatt åpner vedlegget til en spam e-postmelding som planter ondsinnet programvare på PC'en på arbeidsplassen. Deretter sendes det ut sensitive personopplysninger pr. e-post til uautorisert mottaker.

Sjekkpunkt: Akseptabel risiko

- ☐ Uønskede hendelser er vurdert med hensyn på risiko og vurdert opp mot akseptabelt nivå.
- ☐ Hendelser med uakseptabel risiko er 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 og -strategi**.

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

5.8.2 Brukersikkerhet

Sikkerhetskrav til ulike typer roller er dekket i dokumentene

- Sikkerhetsinstruks bruker,
- Sikkerhetsinstruks leder og
- 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

- §2-8: *"Autorisert bruk av informasjonssystemet skal registreres."*
- §2-14: *"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.

Ref. personopplysningsforskriftens § 7-11. *Aktivitetslogg i edb-system eller datanett:*

"Behandling av personopplysninger som følge av registrering av aktiviteter (hendelser) i et edb-system, samt behandling av personopplysninger om disposisjoner til ressurser i systemet, er unntatt fra meldeplikten etter personopplysningsloven § 31 første ledd.

Unntak fra meldeplikt gjelder bare dersom behandlingen har som formål

- a) å administrere systemet, eller*
- b) å avdekke/oppklare brudd på sikkerheten i edb-systemet.*

Personopplysninger som fremkommer som følge av behandlinger etter annet ledd, kan ikke senere behandles for å overvåke eller kontrollere den enkelte."

Hensikten med logging av autorisert bruk er å kunne spore i ettertid hvem som gjorde hva med hvilke personopplysninger 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**.

Sjekkpunkt: Rutiner for informasjonssikkerhet

- ❑ Informasjonssystemet er konfigurert i henhold til føringer i dokumentet **Sikkerhetsmål og -strategi** og resultat av risikovurdering.
- ❑ Konfigurasjonen er dokumentert i dokumentet **Beskrivelse av informasjonssystemet**.
- ❑ De ulike sikkerhetsinstruksene er gjort kjent i virksomheten og er signert av alle relevante brukere og ledere samt av sikkerhetsansvarlig.
- ❑ Rutine for logging er beskrevet i dokumentet **Driftsrutiner** og tatt i bruk i drift av informasjonssystemet.

5.9 Velge sikkerhetstiltak

5.9.1 Beskrivelse

Kapittel 2 i personopplysningsforskriften inneholder en del minimumskrav til konkrete sikkerhetstiltak som alle virksomheter som behandler personopplysninger skal ha oppfylt. For eksempel krav til tilgangskontroll, avvikshåndtering, logging 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
- Overordnet IT beredskapsplan
- Fysisk sikkerhet

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

Eksempler på aktuelle tekniske sikkerhetstiltak for personopplysninger og behandlende systemer med ulike beskyttelsesbehov (NB! Listen er ikke uttømmende):

Strategi/tiltak for sikring av informasjon			
Kat	Konfidensialitet	Integritet	Tilgjengelighet
Høy	- To faktor autentisering - Kryptering av kommunikasjon over eksterne forbindelser inkludert forretningskritisk e-post - Felter med direkte økonomisk verdi krypteres ende-til-ende - Kryptering forretningskritisk informasjon ved lagring - Direkte økonomisk verdi - Passord - Informasjon på bærbare PCer - Krypteringsnøkler - Sikkerhetsovervåking - Periodisk verifisering av sikkerhetsnivå og ved vesentlige oppgraderinger - Rutiner for sikkerhet i utvikling og testing - Bruk av proxy løsning /web front-end når tjenester skal nås fra Internett - Logging av all trafikk relatert til transaksjoner - Krypteringsnøkler skal være forskjellig mot leverandør fra krypteringsnøkler mot butikker/lagring - Dekryptering av informasjonsfelter med direkte økonomisk verdi skal bare skje etter betaling i butikk	- Tofaktor autentisering - Autentisering av brukere ved personlige brukerkonti og passord samt smartkort iht. passordpolicy - Separat autentisering av eksterne brukere i tillegg til intern pålogging ved tilgang til internt nett - Autentisering av maskin-maskin kommunikasjon over eksterne forbindelser - Digitale signaturer på forretningskritisk e-post over Internett - Digital signaturer på transaksjoner (skal vurderes for alle nye prosjekter) - Helhetlig logging - Transaksjoner initiert fra butikk skal kunne knyttes til operatør identitet	Generelt - Avbruddfri strømforsyning - Driftsovervåking (24/7) - Maskinvaremonitorering (24/7) 24/7 måling og overvåking av opptid på tilgjengelighet gjennom nettverk Høy 1 (anbefalte tiltak) - Supportavtale (24/7) HW, SW og kommunikasjon med umiddelbar respons for både hoved- og reserveløsning (vurderes) - Redundans/ reserveløsning (full, dvs. HW, SW og kommunikasjon) skal ha umiddelbar aktivering av reserveløsning ved feil på hovedsystem - Fysisk separat reserveløsning Høy 2 (anbefalte tiltak) - Supportavtale (24/7) HW, SW og kommunikasjon med responstid 2 timer for både hoved- og reserveløsning (vurderes) - Nødvendig Redundans/ reserveløsning (delvis, dvs. maskinvare og kommunikasjon) slik at systemet re-etablert etter max. 4 timer
Middels	- Kryptering av kommunikasjon over Internett eller andre eksterne IP-nett. Unntak: - Leide linjer - ISDN - Mobilkommunikasjon	- Autentisering av brukere ved personlige brukerkonti og passord iht. passordpolicy - Separat autentisering av eksterne brukere i tillegg til intern pålogging ved tilgang til internt nett - Autentisering av ISDN, analog eller mobil forbindelser ved bruk av A-nummer verifikasjon - Helhetlig logging	- Supportavtale (24/7) HW, SW og kommunikasjon med responstid 8 timer - Redundans/ reserveløsning (delvis, reservedeler tilgjengelig ila 8 timer) - Avbruddfri strømforsyning - Driftsovervåking (periodisk)
Lav	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 - Avbruddfri strømforsyning for servere - Driftsovervåking (periodisk)

Flere og mer detaljerte tiltak kan finnes i ISO 17799. (Kan kjøpes fra www.pronorm.no.)

Sjekkpunkt: Velge sikkerhetstiltak

- ❑ Det er utarbeidet beskrivelse av identifiserte sikkerhetstiltak som er nødvendige for å motstå identifiserte trusler og avverge identifiserte uønskede hendelser for å holde reelt risikonivå innenfor akseptabelt risikonivå.

5.10 Gjennomføre sikkerhetstiltak

5.10.1 Beskrivelse

I mange tilfelle 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 og komme frem til en effektiv teknisk og organisatorisk totalløsning for informasjonssikkerheten.

Samtidig må det prioriteres tiltak ut fra hvor det er identifisert størst risiko.

Det må også bygges bevissthet rundt at det skal utarbeides dokumentasjon av sikkerhetstiltakene i tillegg til av alle relevante systemer og infrastruktur.

Gjennomføring av endringene bør organiseres i en prosjektplan. Denne kan løpe over flere år for å gjennomføre alle nødvendige endringer da budsjettmessige begrensninger kan forhindre at alle nødvendige forbedringer utføres umiddelbart. Prosjektplanen vil også være et hjelpemiddel i budsjettarbeidet. Hvis ledelsen i virksomheten har godkjent prosjektplanen for utbedring av sikkerheten i forbindelse med behandling av personopplysninger, bør ledelsen også sikre nødvendige budsjetter for at den delegert ansvarlige skal kunne gjennomføre utbedringene iht. planen.

Sjekkpunkt: Gjennomføre sikkerhetstiltak

- ☐ Dokumentert aktivitetsplan for å bringe sikkerheten for behandling av personopplysninger i overensstemmelse med resultater av risikovurdering.
- ☐ Dokumentert finansieringsplan som støtter tids-/aktivitetsplan.

6 Oppfølging

Bakgrunnskunnskap	Innledende oppgaver	Håndteringsrutiner	Informasjonssikkerhet	Oppfølging
-------------------	---------------------	--------------------	-----------------------	------------

6.1 Avvikshåndtering og egenkontroll

6.1.1 Behandling av avvik

Dersom personopplysninger håndteres i strid med fastlagte rutiner eller ved mistanke om eller dokumentert brudd på informasjonssikkerhet, skal virksomheten iverksette avviksbehandling.

Formålet med avviksbehandling er å bringe avviket til opphør, gjenopprette normal tilstand, og hindre gjentakelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan personopplysninger håndteres eller informasjonssystemet benyttes, skal resultatet fra avviksbehandling benyttes som grunnlag ved gjennomgang og endring av de aktuelle rutiner. Avviksbehandling består av:

- Deteksjon av avviket.
- Rapportering; normalt utføres dette av den medarbeider som oppdager avviket. Avviket rapporteres til virksomhetens sikkerhetsansvarlig eller i henhold til annen intern organisering.
- Iverksetting av strakstiltak bl.a. med det formål å avgrense eventuelle følgeskader. Strakstiltakene kan utføres av den medarbeider som oppdager avviket, eventuelt av den medarbeider som har ansvar for håndteringsrutiner eller som har ansvar for den berørte del av informasjonssystemet.
- Iverksetting av korrigerende tiltak for permanent å gjenopprette normal tilstand. Dette utføres normalt av virksomhetens sikkerhetsansvarlig (delegert myndighet fra behandlingsansvarlig) eller, i forbindelse med avvik for informasjonssikkerhet, av IT-driftssjef.
- Vurdering, etter noe tid, av hvorvidt det korrigerende tiltak fungerer etter sin hensikt. Vurderingen utføres av henholdsvis sikkerhetsansvarlig eller IT-driftssjef.

Eksempler på situasjoner som gjør det nødvendig å iverksette avviksbehandling:

- Ved utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Ved lagring av personopplysninger uten samtykke eller annet behandlingsgrunnlag.
- Når medarbeidere benytter informasjonssystemet uten autorisasjon.

- Ved 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, strakstiltak som er utført, korrigerende tiltak som er iverksatt, resultater fra evaluering av det korrigerende tiltakets effekt over tid samt opplysninger om hvilke medarbeidere som har vært involvert i behandlingen av avviket.

Rapportering av avvik utføres normalt av de medarbeidere som oppdager avviket. Strakstiltakene kan utføres av den medarbeider som oppdager avviket, eventuelt av den medarbeider som har ansvar for håndteringsrutiner eller som har ansvar for den berørte del av informasjonssystemet. Mal for avviksskjema til utfylling finnes i dokumentet **Avviksskjema**. Se også eksempel nedenfor.

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

Eksempel på avviksskjema:

Avviksskjema	Virksomhet: XX	Sendes til: Sikkerhetsansvarlig	Saksident: xxxx
Formål: Skjemaet skal sikre at alle brudd og antatte brudd på håndteringsrutiner eller sikkerhetsrutiner blir registret og behandlet på forsvarlig måte.			
Beskrivelse av avviket: xxxxxxxx xxxxxxxx vedlegg:			
Beskrivelse av midlertidig tiltak: xxxxxxxx xxxxxxxx vedlegg:			
Melderens registrering	Navn: Xxxxxxxxxx	Utstyr/ident: xxxxxxxxxx	Dato/ kl: xxxxxxxxxx
Analyse av årsak: xxxxxxxx xxxxxxxx Vedlegg:			
Beskrivelse av iverksatte tiltak: xxxxxxxx xxxxxxxx Henv:			
Sikkerhetsansvarliges Behandling	Klassifikasjon: XXXXXXXXXX	Rapport sendes Datatilsynet: JA / NEI	Dato / underskrift: NN
Evaluert dato:			

Rutiner for avvikshåndtering dokumenteres i dokumentet **Rutiner for avvikshåndtering og egenkontroll**.

6.1.2 Egenkontroll av rutiner og tekniske tiltak

Virkksomheten skal ha rutiner for kontroll av at rutiner for håndtering av personopplysninger og for kontroll av informasjonssikkerhetstiltak er i bruk og fungerer etter hensikten. Sikkerhetsansvarlig er ansvarlig 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 dokumentet **Egenkontrollskjema**. Se også eksempel nedenfor:

Eksempel:

Egenkontrolltiltak	Eier av aktivitet	Frekvens	Resultat	Kommentarer/ tiltak
Oppfølging/revisjon av risikovurdering og valgt sikkerhetsnivå.	IT Sikkerhetsleder	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	IT Sikkerhetsansvarlig	Månedlig + Ad. hoc.		

alvorlige hendelser.				
Gjennomgang av privilegerte brukeres tilgangsrettigheter – administrator rettigheter	IT-drift, samband og telefoni	Halvårlig		

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 færrest mulig uønskede hendelser oppstår i fremtiden.

Eksempel - Rutine for læring og prosessforbedring

- Det gjennomføres faste driftsmøter hvor sikkerhet adresseres inklusiv gjennomgang av avvik for forslag til forbedring.
- Det gjennomføres halvårlige møter mellom sikkerhetsansvarlig og IT Drift hvor resultater av egenkontroll gjennomgås. Videre dokumenteres lærdom i kompetansedatabase og/eller endringslogg og forslag til forbedringer 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.

Rapport skal også omfatte erfaringer/lærdom som er gjort og forslag til forbedringer - både tekniske tiltak og prosessforbedringer.

Eksempel - Rutine for rapportering

- Månedlig rapportering til sikkerhetsansvarlig av sikkerhetshendelser, avvik og resultater fra egenkontrollaktiviteter samt erfaringer/lærdom og forslag til forbedringer.
- Årlig rapportering til ledelsens gjennomgang.

Sjekkpunkt: Rutiner dokumentert

- ☐ Rutiner for læring og prosessforbedring samt for rapportering er dokumentert i dokumentet **Rutiner for læring, prosessforbedring og rapportering**.

7 Referanser

[1] Internkontroll i mindre virksomheter - veileder 07/02a.

Vedlegg 1 Definisjoner

Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Behandling av personopplysninger	Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder.
Databehandler	Den som behandler personopplysninger på vegne av den behandlingsansvarlige.
Informasjonssikkerhet	Personopplysningsloven (§13) stiller krav om at virksomheten <i>"skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger"</i> .
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 aktivitet i virksomheten slik at driften skjer i overensstemmelse med lover og regler. Samtidig er styringssystemet medarbeiderens verktøy for å utføre oppgaver på forsvarlig og sikker måte.
Konfidensialitet	At uvedkommende ikke får ikke tilgang på opplysningene.
Personopplysning	Opplysninger og vurdering 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.
Sensitiv personopplysning	Personopplysning innenfor en av kategoriene • 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, og
- medlemskap i fagforeninger.

Tilfredsstillende
informasjonssikkerhet
(ref POL §13)

At man skal etablere sikkerhetstiltak iht. besluttet
akseptabelt risikonivå og resultatene av en risikoanalyse
som tar utgangspunkt i de personopplysningene som
virksomheten behandler og behandlingene som utføres.

Tilgjengelighet

At opplysningene er tilgjengelige når vi trenger dem.

Vedlegg 2 Oversikt over maler

	Dokumenter i internkontrollen
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