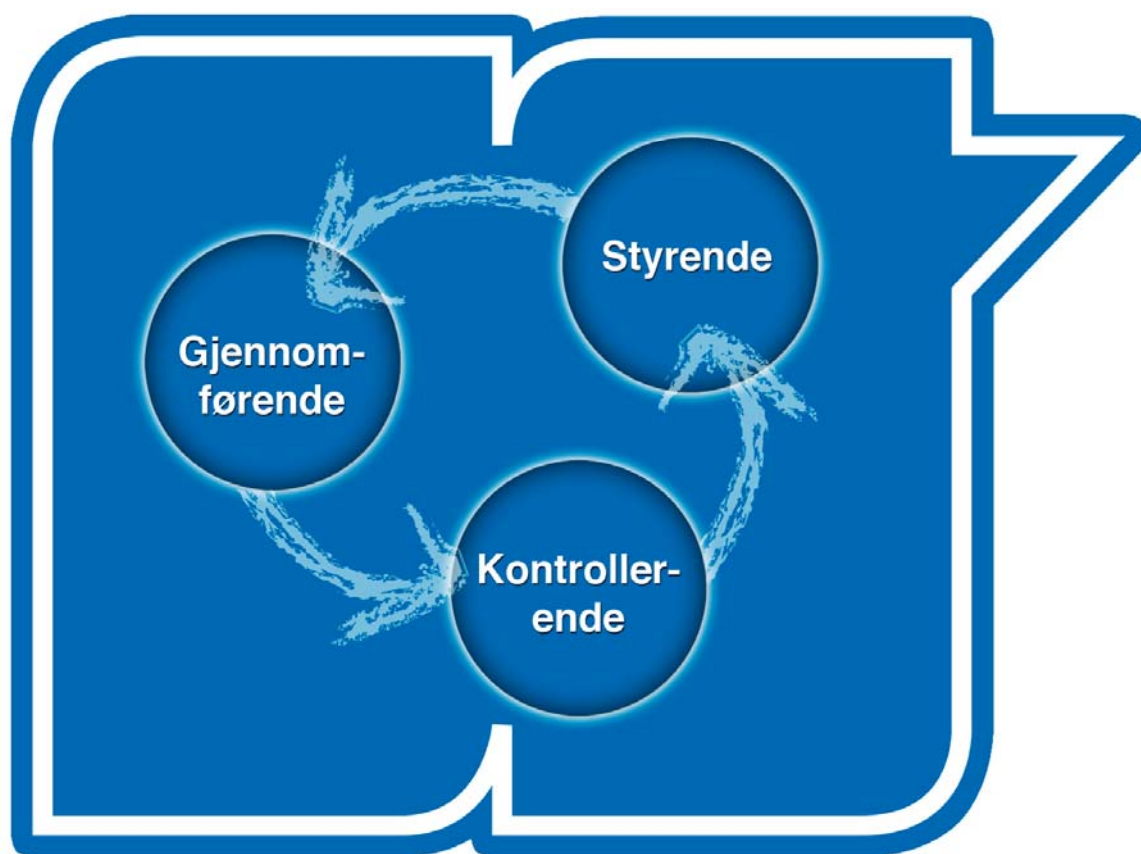


Internkontroll i mindre virksomheter - introduksjon

Veileder 07/02a (del 1 av 2)

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

Innholdsfortegnelse



1	Innledning	4
2	Bakgrunnskunnskap	5
2.1	Hva er internkontroll? Og informasjonssikkerhet?	5
2.2	Hva er personopplysningsloven og -forskriften?	6
2.3	Hva er personopplysninger og sensitive personopplysninger?	6
3	Informasjonssikkerhet	8

1 Innledning

De fleste virksomheter behandler opplysninger som kan knyttes til enkeltpersoner (personopplysninger), og må følge personopplysningsloven. Virksomhetene må ha rutiner for sin bruk av opplysningene og tilfredsstillende beskyttelse av opplysningene.

Denne veilederen er laget spesielt for mindre virksomheter med få personopplysninger. Den skal hjelpe deg gjennom prosessen med å bygge opp et internkontrollsystem slik at virksomheten din behandler personopplysninger lovlig, sikkert og forsvarlig.

Veilederen er delt i to dokument. Del 2 - "eksempel" - er dokumentet som du selv redigerer slik at dette blir virksomhetens dokumentasjon for internkontroll. Denne delen, del 1, gir deg bakgrunnskunnskapen du trenger før du bruker del 2. I tillegg beskriver del 1 oppgaver rundt informasjonssikkerhet.

Virksomheter som kan bruke denne veilederen, håndterer kun personopplysninger om egne ansatte og om virksomhetens kunder. Med kundeopplysninger menes her opplysninger relatert til handel og ikke medlemsopplysninger, klientopplysninger eller lignende.

Øvrige virksomheter må bruke den generelle veilederen "internkontroll og informasjonssikkerhet" sammen med tilhørende maler.

Vær oppmerksom på at virksomheten også kan være underlagt andre regelverk som stiller krav om internkontroll, eksempelvis for helse, miljø og sikkerhet (HMS). 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.

2 Bakgrunnskunnskap

Før du går i gang med å tilpasse eksemplet (del 2) til din virksomhet, bør du lese denne bakgrunnsinformasjonen.

2.1 Hva er internkontroll? Og informasjonssikkerhet?

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak. Tiltakene skal 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.

Den første delen av internkontrollen får man på plass ved å dokumentere svarene på noen få sentrale spørsmål:



Figur 1 Sentrale spørsmål

Deretter må virksomheten lage de nødvendige rutinene for de ulike pliktene, og gjøre rutinene kjent for medarbeiderne. Til slutt må man sørge for at rutinene blir fulgt, og at de holdes oppdatert.

Informasjonssikkerhet handler om å sikre verdiene som finnes i informasjonen vi håndterer (informasjonsverdier). Virksomheten skal sørge for tilfredstillende informasjonssikkerhet ved å håndtere risiko knyttet til informasjonsverdier. Styring av informasjonssikkerheten er en del av internkontrollen.

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 som de skal.
- 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 virksomhetene vil også behandle 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 følsomme 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.

3 Informasjonssikkerhet

Før du går i gang med å utarbeide tiltak for informasjonssikkerhet til din virksomhet, bør du lese denne bakgrunnsinformasjonen.

Informasjonssikkerhet handler om å sikre verdiene som finnes i informasjonen vi håndterer (informasjonsverdier). Virksomheten skal sørge for tilfredsstillende informasjonssikkerhet ved å håndtere risiko knyttet til informasjonsverdier.

Virksomheten må identifisere hvilke informasjonsverdier den har, 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 skal organiseres og dokumenteres som en del av internkontrollen.

Konfidensialitet, integritet og tilgjengelighet

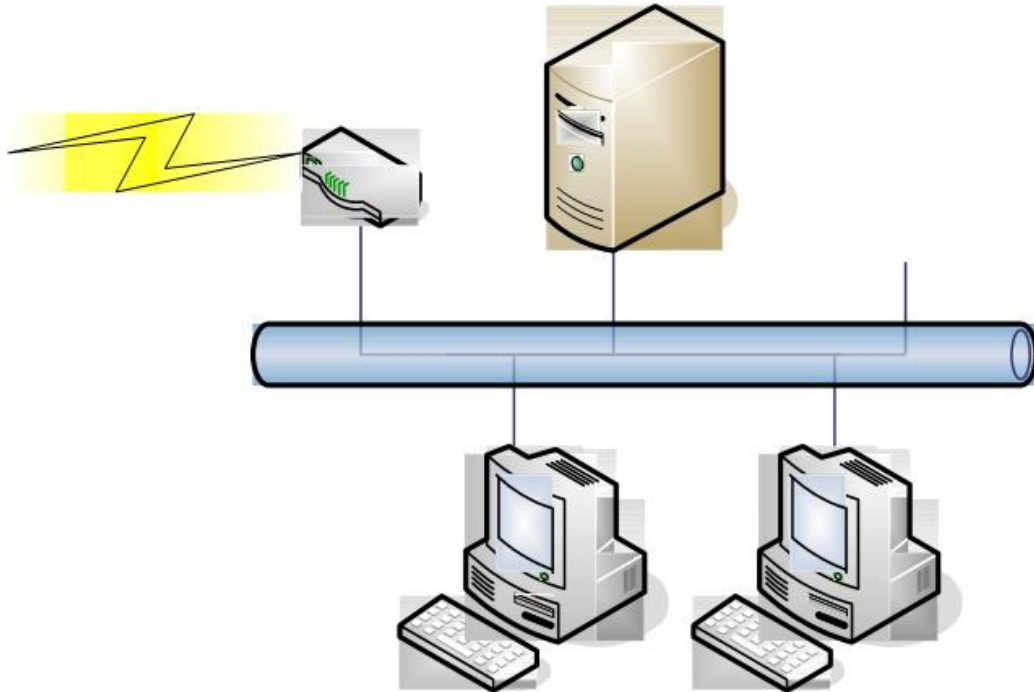
Vi ønsker å beskytte opplysningene med hensyn til:

- konfidensialitet, at uvedkommende (interne og eksterne) ikke får tilgang på opplysningene,
- integritet, at opplysningene ikke endres uten av dette er tilsiktet og gjøres av rettmessige brukere, og
- tilgjengelighet, at opplysningene er tilgjengelige for autoriserte brukere ved behov.

Konfidensialitet, integritet og tilgjengelighet benevnes med K, I og T i tabellene senere.

Konfigurasjonsbeskrivelse

Konfigurasjonsbeskrivelser (nettverkstegninger, skisser over plassering av enheter i skap og beskrivelse av oppsett av ulikt utstyr) skal være oppdaterte og gjenspeile gjeldende konfigurasjon. Endringer av systemet og dokumentasjonen skal loggføres, og utdatert dokumentasjon skal oppbevares.



3-1 Nettverkstegning

Alt IT-utstyr bør merkes og registreres i et eget register. Registeret kan inneholde:

- utstyrsnavn,
- serienummer/versjonsnummer,
- opplysninger om oppsett og innstillinger,
- dato for når det er tatt i bruk og
- dato for når det ble tatt ut av bruk.

Det skal finnes oppdatert oversikt over status på koblingsnivå og teknisk konfigurasjon.

Kopi av systemkonfigurasjon på rutere/annet nettverksutstyr skal tas ved endringer eller inngå som del av periodisk rutine.

Systemkonfigurasjoner og konfigurasjonsbeskrivelser skal inngå i rutiner for sikkerhetskopiering.

Risikovurdering

Virksomheten skal gjennom risikovurderinger vurdere om personopplysningene er tilfredsstillende sikret med hensyn til konfidensialitet, integritet og tilgjengelighet. For å gjøre dette kan virksomheten:

- 1) identifisere mulige uønskede hendelser,
- 2) vurdere konsekvensene av mulige uønskede hendelser,
- 3) vurdere sannsynligheten for at uønskede hendelser kan inntreffe (gjærne representert med hvor lett hendelsen kan inntreffe), og
- 4) vurdere om virksomheten kan akseptere hendelsen.

Risiko er kombinasjonen av konsekvensene en uønsket hendelse kan medføre, og sannsynligheten for at denne skal oppstå. Under større forhold vil konsekvens og sannsynlighet gjerne graderes, og risiko vil bli representert som produktet av konsekvens og sannsynlighet: Risiko = Konsekvens(hendelse) X Sannsynlighet(hendelse).

For hendelser som ikke vurderes som akseptable, skal virksomheten iverksette tiltak. Øvrige hendelser velger virksomheten å akseptere.

Virksomheten skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i informasjonssystemet eller endringer i trusselbildet.

Resultater av risikoanalysen og vurdering av tiltak skal dokumenteres. Sikkerhetstiltak i form av rutiner og tekniske tiltak skal dokumenteres.

Virksomhetens ledelse har ansvar for iverksetting av risikovurdering. Resultat fra analysen rapporteres til virksomhetens ledelse.

Eksempel på en enkel risikovurdering med hensyn på personopplysninger

Hendelse	Kategori K I T	Konsekvens	Sannsynlighet	Vurdering
1. Utenforstående får tilgang til lokalene gjennom innbrudd, tyveri av PC'er og servere	K, T	Kan medføre uopprettelig økonomisk tap ved tilgang til kundeopplysninger - Tap av omsetning og kunder under nedetid	Det er lav sannsynlighet for innbrudd grunnet alarm tilknyttet vaktelskap.	Akseptabel
2. Ansatte får tilgang til andre ansattes personalmapper ved å låse seg inn på kontoret til personalansvarlig	K, I	Kan føre til tap av anseelse eller integritet for den enkelte ansatte.	Kan med letthet gjennomføres ved bruk av standard kontornøkler.	Ikke akseptabel
3. Utilgjengelighet av personalsystem i 24 timer	T	Kan medføre økonomisk tap for de ansatte ved forsinket utbetaling - reparerbart	Moderat sannsynlighet. Frafall av Internett eller nedetid i informasjonssystem.	Akseptabel

4. Brann i virksomhetens lokaler	T	Kan medføre økonomisk tap ved tap av omsetning og kunder	Sannsynlig med tap og betydelige skader på grunn av manglende sikkerhetskopier utenfor huset, brannvarsling med linje til brannvesenet og brannsikring i datarom.	Ikke akseptabel
5. Vannskade	T	Kan medføre økonomisk tap ved tap av omsetning og kunder	Lav sannsynlighet for vannskade grunnet ingen vannrør umiddelbart over datarom, metalldeksler over servere og fordi bygningen ikke er flomutsatt.	Akseptabel

Virksomheten vil ofte ha behov for å utdype hendelser, mulige konsekvenser og sannsynlighetsbetraktningen i tillegg til det som føres i tabellen. Spesielt for å utdype allerede etablerte tiltak eller kjente svakheter.

Oppfølging av risikovurdering

Hendelser som er identifisert med en ikke-akseptabel risiko:

Hendelse nr.	Tiltak	Ansvar	Frist
2	Skaffe låsbart arkivskap til personalansvarlig og revidere rutine for håndtering av personalsaker.	Sikkerhetsansvarlig	1. juni 2007
4	4.1 Ta daglig sikkerhetskopi med lagring hver uke utenfor bygning.	IT-driftsansvarlig	1. april 2007
4	4.2 Brannvarslingssystem med linje direkte til brannvesen.	Sikkerhetsansvarlig	1. juli 2007
4	4.3 Brannslukningsanlegg i datarom.	Sikkerhetsansvarlig	1. juli 2007

Eksempel på relevante tekniske sikkerhetstiltak:

Gitt at virksomheten kun behandler personopplysninger for å administrere forholdet til sine ansatte og forholdet til sine kunder, er følgende eksempler på tekniske tiltak for å beskytte personopplysninger i en liten eller mellomstor bedrift:

Fysisk sikkerhet

- Det er installert tyverialarm.

- Besøkende skal registreres ved ankomst og avslutning av besøk og skal bære synlig besøkskort. Besøkende skal hentes av ansatt ved ankomst, følges av ansatt under hele besøket og følges tilbake til resepsjonen ved avslutning av besøk.

Tilgangskontroll

- Tilgangskontrollsystem er innført for tilgang til personopplysninger om ansatte og om kunder. Personalsjef autoriserer brukere som skal ha tilgang til opplysninger om ansatte, salgssjef autoriserer brukere som skal ha tilgang til kundeopplysninger.

Brannmur

- Brannmur er installert mot eksternt nettverk. Brannmur er konfigurert til kun å slippe gjennom nødvendig datatrafikk, eksempelvis e-post og web (http).

Tilgang til nettverk

- Brukere må identifisere seg med personlig brukernavn og autentisere seg med passord for å få tilgang til lokalnettverket. Passord skal ha minimum 8 tegn og bestå av store og små bokstaver og minst et tall eller et spesialtegn.
- Det trådløse nettverket er sikret med kryptering og skjult nettverksidentifikasjon.

Brukersikkerhet

- Alle brukere skal lese, forstå og signere
 - o Sikkerhetsinstruks bruker, se vedlegg 1.
 - o Taushetserklæring, se vedlegg 2.

For spesielt beskyttelsesverdige opplysninger:

Virksomheten vil normalt velge et av følgende tiltak eller beskrive en annen løsning:

- Spesielt beskyttelsesverdige opplysninger behandles manuelt og lagres i låst arkivskap.
- Spesielt beskyttelsesverdige opplysninger behandles i et informasjonssystem fysisk atskilt fra virksomhetens øvrige informasjonssystem.
- Spesielt beskyttelsesverdige opplysninger behandles i et eget IT-system hvor kun personalsjef og avdelingsledere kan logge seg på ved hjelp av terminalserver.