

Etablering av internkontroll

Personopplysningsloven (pol) stiller krav om at den som behandler personopplysninger skal etablere et system for internkontroll (pol §14). Det innebærer at virksomheter som omfattes av loven må iverksette systematiske tiltak for å sørge for at loven og tilhørende regelverk er kjent og følges. For de fleste virksomheter er følgende regelverk relevant:

- Personopplysningsloven
- Personopplysningsforskriften
- Eventuelle vilkår gitt i konsesjon fra Datatilsynet

For noen sektorer som for eksempel offentlig forvaltning, helsesektoren, politi- og domstoler, kan særlover, forskrifter og rundskriv komme til anvendelse.

Ledelsen har ansvar

Ledelsen er ansvarlig for at det settes i gang aktiviteter for å etablere internkontroll i virksomheten. Ledelsen har et spesielt ansvar for å utarbeide policy, målsetning, identifisere forpliktelser, klarlegge intern organisering og ikke minst tydelig identifisere ansvar og myndighet. Ledelsen har også ha ansvar for at det etableres prosedyrer og instruksjoner basert på en risikovurdering i forhold til personvern. Ledelsen må ta stilling til hvilke rutiner som er påkrevd for å sikre samsvar mellom den etablerte systematikken og aktivitetene som faktisk utføres i virksomheten.

Dokumentasjonen over systemet for internkontroll skal være tilgjengelig for de ansatte i virksomheten og Datatilsynet.

Ved etablering av internkontroll bør virksomheten oppnå:

- Bedre informasjonssikkerhet, informasjonskvalitet og effektiviseringsgevinst
- System for kvalitetsikring av at offentlig regelverk følges
- Sikre at virksomheten driver forsvarlig og innenfor lovverket
- Gi fastsatte prosedyrer og instruksjoner som bidrar til at ledelsen sikrer at de ansatte arbeider i samsvar med virksomhetens mål/policy
- Bidra til at avvik blir oppdaget og korrigert
- Redusere sjansen for alvorlige feil som skyldes manglende oppfølging av lovverket.

Struktur

Det er nyttig å etablere en struktur for internkontrollsystemet. Dette gjør det lettere for aktørene som skal bidra i prosessen til å forstå hvilken funksjon systemet skal ha. Dokumentasjon av internkontrollsystemet skal vise den reelle situasjonen i virksomheten. Berørte parter derfor bør delta i utformingen.

Noen ganger medfører innføring av nytt regelverk at prosedyrer og instruksjoner må endres. Det er viktig at dette faktisk skjer i virksomheten og ikke bare i systembeskrivelsen.

Et internkontrollsystem består gjerne av:

- **Styrende dokumentasjon** som gir en systembeskrivelse som inneholder policy og målsetning, identifiserte krav og plikter, intern organisering, ansvar og myndighet.
- **Gjennomførende dokumentasjon** som beskriver bedriftsprosedyrer og arbeidsinstruksjoner. Denne dokumentasjonen skal sikre at aktivitetene i virksomheten er i samsvar med eller ligger innenfor myndighetskravene.
- **Kontrollerende dokumentasjon** er dokumenter som har til formål å verifisere at aktivitetene har foregått i samsvar med fastsatte prosedyrer og instruksjoner. Eksempler er rapporter, sjekklister, logg mv.

Styrende dokumentasjon er overordnet i sin form og er spesielt ledelsesorientert. *Gjennomførende dokumentasjon* er i hovedsak prosedyrer og rutiner og instruksjoner, det vil si en konkret beskrivelse av hvordan en gitt situasjon skal håndteres. *Kontrollerende dokumentasjon* kan betraktes som et ”sikkerhetsnett” som bidrar til at styringsdokumentene følges og at eventuelle avvik lettere oppdages. Dokumentene skal ikke være statiske, men endre seg i tråd med virksomhetens utvikling og den rettslige utvikling.

Den samlede dokumentasjonen utgjør virksomhetens internkontrollsystem.

Styrende dokumentasjon

Styrende dokumentasjon bør omhandle:

- Virksomhetens mål og policy i forhold til personopplysningsloven (pol). Se spesielt pol § 1
- Identifisering av at tiltenkt lagring og behandling av personopplysninger samsvarer med lovens grunnkrav, se § 11. Det legges spesielt vekt på saklig behov og konkret definering av formål, herunder at opplysningene som lagres samsvarer med formålet.
- Identifisering av hvilke plikter som er relevant for vedkommende virksomhet.
- Organisering av virksomheten. Intern delegering av ansvar og myndighet skal være entydig definert.
- En beskrivelse av hvordan virksomheten ivaretar informasjonssikkerheten. Se pol § 13, forskriften kap 2. Virksomhetens sikkerhetsmål skal beskrive bruk av informasjonsteknologi.
- En beskrivelse av hvordan ledelsen vil sørge for at virksomhetenes aktiviteter er i samsvar med kravene i regelverket. En slik beskrivelse vil normalt ende opp i behov for gjennomførende dokumentasjon og kontrollerende dokumentasjon.

Gjennomførende dokumentasjon

Gjennomførende dokumentasjon bør omhandle:

- Tiltak som er foreslått som følge av en risikovurdering i virksomheten, for eksempel tiltak for å oppnå tilstrekkelig informasjonssikkerhet. Konfidensialitet, integritet og tilgjengelighet (avhengig av behov) skal sikres. Det legges vekt på at konfigurasjon i systemer hvor personopplysninger lagres eller bearbeides må kunne dokumenteres og at det gjennom denne dokumentasjon kan verifiseres at virksomhetens mål og policy for informasjonssikkerhet er implementert.
- Prosedyrer
- Arbeidsinstrukser

Vær oppmerksom på personopplysningslovens bestemmelser vedrørende konfidensialitet, integritet og tilgjengelighet, jf pol § 13 og forskriftens kapittel 2.

Det er spesielt viktig å entydig definere hvem som har ansvaret for hva. Gjennomførende dokumentasjon vil i volum ofte utgjøre den største delen av internkontrollsystemet.

Eksempel på prosedyre

Eksempel på en prosedyre kan være ”prosedyre for utlevering av informasjon, der den registrerte har bedt om innsyn” eller ”prosedyre ved etablering av kameraovervåkning”. En prosedyre kan igjen bestå av flere arbeidsinstrukser.

Eksempel: Prosedyre for etablering av kameraovervåkning

Følgende rutiner/instrukser kan pekes ut :

- *Instruks for vurdering av formål og saklighet ved tv-overvåkning*
- *Instruks for å sikre arbeidstakers medbestemmelse ved etablering av tv-overvåkning. (Denne instruks kan komme som følge av annet lovverk, for eksempel arbeidsmiljøloven)*
- *Instruks for å sikre varsling av tv-overvåkning til publikum*
- *Instruks om utlevering av opptak, jf pol*
- *Instruks om sletting av opptak, jf. pol*

Gjennomførende dokumentasjon er et knippe av mekanismer som skal sikre at aktiviteten i virksomheten samsvarer med virksomhetens definerte mål og policy for personvern og reglene for øvrig.

I forhold til ansatte i virksomheten kan gjennomførende dokumentasjon være et sett med interne kjøreregler som sikrer at virksomheten ikke begår lovbrudd med noen av sine aktiviteter.

Kontrollerende dokumentasjon

Kontrollerende dokumentasjon bør omhandle::

- Sjekklistor
- Skjema for avviksrapportering
- Rapporter
- Logg

Kontrollerende dokumentasjon består ofte av to deler: En del som brukes under interne revisjoner og en del som brukes i det daglige arbeidet. Skjema for avviksrapportering er for eksempel ment til bruk dersom det oppdages aktiviteter som ikke samsvarer med fastlagte prosedyrer og/eller instruks

Det er et klart skille mellom gjennomførende og kontrollerende dokumentasjon. Det første skal sikre at aktivitetene er i samsvar med mål og policy. Det siste skal bidra til at avvik fra mål og policy oppdages og rettes.

Avviksrapportering

Ledelsen kan gjennom sitt aktive engasjement bidra til at de ansatte forstår hvor viktig det er at avvik oppdages og at dette vil forhindre tilsvarende i framtiden. Det er viktig at ledelsen viser at avviksrapportering tas på alvor.

Eksempel 1:

En ansatt oppdager at det ikke er satt opp skilt i området som tv-overvåkes, eller at skiltene er så godt skjult at de ikke kan sees. Han rapporterer dette gjennom skjema for avviksrapportering. Dette skal utløse korrigerende tiltak fra ledelsens side. Korrigerende tiltak kan være:

- *Nye skilt anskaffes og monteres opp*
- *Det kartlegges årsak til avvik og vurderes om prosedyren eller instruksjonen er mangelfull. Eventuelle justeringer foretas.*
- *Hvis det ikke er mangler ved prosedyre/instruks tas saken opp med rette vedkommende*
- *Ledelsen gir tilbakemelding til rapportør om at avviket er lukket*

Eksempel 2:

Som et ledd i virksomhetens årlige internrevisjon oppdages det at det ikke er satt opp skilt i området som tv-overvåkes, eller at skiltene er så godt skjult at de ikke sees. Avviket identifiseres i rapporten, også antatt årsak til avviket. Forslag til korrigerende tiltak forslås overfor ledelsen.

- *Nye skilt anskaffes og monteres opp*
- *Det bør foretas en nærmere kartlegging av årsak til avviket, og vurderes om prosedyren eller instruksjonen er mangelfull.*
- *Hvis det ikke er mangler ved prosedyre/instruks, anbefales det at saken tas opp med rette vedkommende.*

I avsnittet under er det gitt et eksempel på en rutine som er fastsatt med bakgrunn i pol § 18 (rett til innsyn).

Rutine for plikt til å gi ansatte innsyn i opplysninger om seg selv

Lovgrunnlag for innsyn: Personopplysningsloven § 18.

Normen:

Den ansatte skal få følgende informasjon

- 1. hvilke opplysninger om den registrerte som behandles, og*
- 2. sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.*

Dersom den ansatte ber om det, skal informasjonen i pol § 18, første ledd bokstav a - f utdypes i den grad dette er nødvendig for at den ansatte skal kunne vareta sine interesser.

Disse opplysningene skal ikke gis til den ansatte når det er nødvendig å holde dem tilbake for intern saksforberedelse.

Hva skal gjøres:

Det skal på forespørsel fra den ansatte tas utskrift av alle opplysninger om henne hos virksomheten. Sammen med denne utskriften skal den ansatte få utdelt informasjon som beskriver behandlingen i henhold til punktene over. Dersom det er registrert opplysninger om den ansatte som det ikke kan gis innsyn i, skal de holdes tilbake.

Hvem skal gjøre dette:

Saksbehandlerne i personalavdelingen kan gi innsyn i disse opplysningene. Ved tvil om innsynretten, skal lederen av personalavdelingen konsulteres.

Når skal det gjøres:

Informasjonen skal gis den ansatte så fort som mulig, og senest innen 14 dager etter forespørselen.