

Internkontroll etter personopplysningsloven – vanlige spørsmål og svar

Internkontroll handler om å arbeide systematisk for at ens egen virksomhet opptrer i samsvar med de lover og forskrifter som gjelder for virksomheten. Her er de vanligste spørsmålene Datatilsynet får om internkontroll, satt opp slik at man også får veiledning i oppbygging av et internkontrollsystem.

Jeg må altså vite hvilke lover og forskrifter som gjelder for min virksomhet?

- *Ja, dette er et av kjernepunktene i internkontroll. Din bransjeorganisasjon vil ofte kunne ha en oversikt over relevant regelverk for din type virksomhet.*

Når du vet hvilke lover/forskrifter som gjelder for din virksomhet kommer neste viktige kjernepunkt – hvilke bestemmelser er relevante for min virksomhet?

Jeg må altså på et vis sortere ut de bestemmelsene som er relevant for oss?

- *Ja, det er riktig. Men før du greier å få dette til kan det være at du må gjennomført kartlegging av behandlinger (som vi skal*

I personopplysningsloven er det stilt krav om etablering av internkontroll. Disse kravene er ytterlig supplert i personopplysningsforskriftens kapittel 2 og 3. Kapittel 2 handler om å ivareta tilfredsstillende sikring av personopplysninger, men kapittel 3 utdyper minimumskrav til rutiner.

Hvorfor er det både lover og forskrifter?

- *Lovene som fastsettes av Stortinget er ofte ganske generelle. Det vil derfor ofte være forskriftshjemmel i en lov. Hensikten vil da kunne være å utdype og presisere hele eller deler av lovteksten med en forskrift. Vi sier derfor at forskriften er forankret i og hjemlet i lov.*

Hvilke regelverk er relevante i forhold til personvern?

For de aller fleste virksomheter vil det være personopplysningsloven og personopplysningsforskriften som er relevant i forhold til personvern.

For virksomheter som arbeider innen helsesektoren og/eller med helseregistre vil også helseregisterloven være relevant. Det vises til annen veiledning mht. denne. I den grad din virksomhet også har en konsesjonspliktig behandling av personopplysninger, vil ovennevnte også suppleres med eventuelle vilkår gitt ved konsesjon

Er loven og forskriften alt jeg trenger å forholde meg til?

- *Ja, i forhold til personvern er det riktig, med mindre andre særlover for din type virksomhet er relevant. Driver du for eksempel et legekantor vil også helseregisterloven være relevant.*

Ansvar

Personopplysningsloven utpeker et subjekt som ansvarlig – den behandlingsansvarlige. Hvem er dette?

Behandlingsansvarlig er den som bestemmer formålet med behandling av personopplysningene og hvilke hjelpemidler som skal benyttes. Det vil si at den behandlingsansvarlige også har bestemmelsesrett over opplysningene og selve behandlingen av dem. Det er også den behandlingsansvarlige som er ansvarlig for at behandlingen er lovlig; den som kan saksøkes og pådra seg straffeansvar for overtredelse av lovens bestemmelser.

Behandlingsansvarlig, er det den som har den daglige ledelsen?

- *I praksis vil det være virksomhetens øverste administrative leder som er behandlingsansvarlig. Det er naturlig at gjennomføringen delegeres til en med daglig ansvar. Uansett sitter den øverste ledelsen fortsatt med ansvaret.*

Behandlinger

Personopplysningsloven bruker begrepene behandling og formål. Disse til begrepene er meget sentrale i regelverket.

Med behandling menes enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller kombinasjon av slike bruksmåter.

Med formål menes den tilsiktede hensikten med behandlingen.

Hvis jeg driver salg og har et kunderegister?

- *Da vil behandlingen i dette tilfellet være selve kunderegister, mens formålet kan være kundeadministrasjon*

En virksomhet vil kunne ha flere behandlinger som hver seg må ha et definert formål. All behandling av kundeopplysningene skal være i samsvar med dette definerte formålet.

Siden det er deg som behandlingsansvarlig som både bestemmer hvilke behandlinger som foretas og formålet – har du i utgangspunktet stor frihet. Men – regelverket forutsetter at du har støtte i lovverket (hjemmel) for å kunne foreta behandlingen. Har du ikke dette vil behandlingen være ulovlig. Se spesielt personopplysningsloven §§ 8 og 9.

Hvordan starter jeg arbeidet?

Det aller første som må på plass er å konstatere at din virksomhet faktisk behandler personopplysninger og at dette regelverket dermed er relevant.

Så må behandlingsansvaret plasseres. Ansvaret hører normalt hjemme hos øverste administrative leder – selv om det kan være fagpersoner eller mellomledere lenger nede i systemet som starter behandlingen.

Det neste naturlige skritt er å kartlegge behandlingene som foretas i virksomheten. Tenk hele tiden på begrepene *behandling – formål – støtte i regelverk (hjemmel)*. Disse elementene må henge sammen – for hver eneste behandling.

Du mener altså at vi må gjøre dette for hele virksomheten?

- Ja, enhver behandling må identifiseres. Deretter må du definere formålet med samt finne hjemmel for behandlingen.

Hvorfor er det så viktig å kartlegge behandlingene? Dette er et nødvendig grunnlag for å avgjøre hvilke bestemmelser (paragrafer) i regelverket som er relevante for din virksomhet. Det er selvfølgelig like viktig å konstatere hvilke bestemmelser som ikke har relevans for virksomheten og som man dermed kan se bort fra. Virksomheten vil etter en slik prosess ha et oversiktlig, håndgripelig og ryddig forhold til hvilke krav som gjelder for egne aktiviteter.

Hvordan kan jeg vite om en bestemmelse er relevant eller ikke?

- Dette er nok det som vil føles vanskeligst i starten. Du må nemlig foreta en grundig gjennomgang av lov og forskrift. Noen bestemmelser vil gjelde for alle behandlinger, mens ytterlig andre kun gjelder for helt bestemte formål. Dette fremgår av regelverket, blant annet kan du ta utgangspunkt i overskriftene til de enkelte deler av regelverket.

Når du nå sitter med:

- Plassering av behandlingsansvaret,
- har kartlagt behandlinger, definert formålet med behandlingene og

funnet hjemmel for disse behandlingene,

- på grunnlag av ovennevnte foretatt en gjennomgang av lov/forskrift og identifisert hvilke bestemmelser som er relevant

kan arbeidet med å etablere rutiner som skal sikre at alle aktiviteter skjer i samsvar med regelverket.

Hvilken form bør mitt internkontrollsystem ha?

Det kan ofte være nyttig å etablere en fast struktur for systemet eller man kan utarbeide en disposisjon for et internkontrollsystem. Dette gjør det lettere for de som skal bidra i prosessen til å forstå hvilken funksjon de ulike rutinene har.

Et internkontrollsystem kan bestå av følgende tre hoveddeler:

- **Styrende del**, dvs. en beskrivelse som inneholder omtale av behandlingsansvar, behandlinger, mål/strategi, identifiserte krav/plikter (*behandling – formål - hjemmel*), ansvar og myndighet samt intern organisering.
- **Gjennomførende del**, hvor de praktiske rutinene inngår. Kort sagt; hvem skal gjøre hva, på hvilken måte, til hvilken tid, under hvilke omstendigheter og hvilket resultat skal oppnås
- **Kontrollerende del**, her inngår sjekklister, egenkontroll, rapporter. Kort sagt; følger vi systemet vårt, hvilke avvik har vi og hvordan kan disse rettes opp.

Må vi dele systemet vårt inn i tre deler?

- Nei, dere bestemmer selv formen systemet skal ha. Datatilsynet gir imidlertid anbefaling på hvordan et slikt system kan se ut.

Disse tre delene vil være en overordnet disposisjon (listen er ikke uttømmende). Innen hver av disse ”hovedavsnittene” vil de enkelte elementer komme inn. Legg merke til at *styrende del* er overordnet i sin form og vil være spesielt ledelsesorientert. Legg også merke til at *gjennomførende del* i hovedsak er prosedyrer og rutiner/instrukser, dvs. konkret hvordan en gitt situasjon skal håndteres. Videre kan *kontrollerende del* betraktes som et ”sikkerhetsnett” som bidrar til at systemet holdes i hevd og at eventuelle avvik oppdages og lukkes. Den samlede dokumentasjonen som nevnt oven vil kunne utgjøre virksomhetens internkontrollsystem.

Hva bør være innholdet i internkontroll

Det er behandlingsansvarlig som er ansvarlig for at det settes i gang aktiviteter slik at det etableres internkontroll i virksomheten. Behandlingsansvarlig har et spesielt ansvar knyttet til styrende del. Videre følge det et oppfølgingsansvar og godkjenningssprosedyre for øvrige deler.

Hva mener dere med oppfølgingsansvar?

- Vel, behandlingsansvarlig sitter uansett med det overordnede ansvar. Det vil imidlertid ofte være slik at vedkommende må delegerer oppbygging av hele eller deler av systemet til linjeledelsen. Behandlingsansvarlig må da følge opp fremdrift på vanlig måte.

På Datatilsynets temasider om internkontroll finnes en sjekkliste som inneholder punkter til et internkontrollsystem for en middels stor virksomhet. I større organisasjoner vil et system kunne være mer omfattende, mens det for en mindre virksomhet kan være mindre.

Datatilsynet anbefaler at du vurderer og eventuelt sjekker ut de nevnte punktene og vurderer om de er relevante for din virksomhet.

Hvor omfattende bør systemet være?

- Dette er det du selv som kan gi best svar på fordi du kjenner virksomheten best. Personopplysningsforskriftens kapittel 2 og 3 har imidlertid noen minimumskrav som må oppfylles.

Implementering

Dette er kanskje den mest krevende delen av arbeidet – å få systemet kjent og implementert i virksomheten. Her er kontrollerende del av systemet av stor betydning – i starten vil virksomheten ofte ha mange avvik. Etter hvert som avvik identifiseres og lukkes vil etterlevelse av systemet bli en del av virksomhetskulturen.

Hvordan bør jeg håndtere avvik?

- Nærmeste leder kan påpeke avviket på generell basis og vise at dette tar ledelsen på alvor. Ved gjentatte avvik på samme forhold kan dette tas opp mer konkret.