

OVERHOLDELSE AV PERSONVERNREGELVERKET

Det ikke nok å forsøke å være innenfor personvernregelverket i det daglige arbeidet og gjøre enkelte tiltak. Det må planmessig arbeid til, effektive tiltak, etablering av rutiner og prosedyrer, og så må det kunne vise at arbeidet, tiltak og vurderinger er gjort. Dette for at krav etter regelverket, som personopplysningsloven, personvernforordningen (GDPR) og annen lovgivning som regulerer personopplysninger følges.¹ Nedenfor er en oversikt over hva som bør gjøres i alle virksomheter, med aktuelle rutiner og dokumentasjon.

I. TILTAK SOM BØR GJØRES. FREMGANGSMÅTE

Følgende fremgangsmåte og tiltak kan gjennomføres for å arbeide mot å overholde personvernregelverket. Merk at man vil helt «innenfor» (bli «compliant»), så arbeidet med å følge personvernregelverket er et kontinuerlig arbeid.

- 1. Oversikt/kartlegging.** Tidlig i prosessen må det kartlegges behandlingen av personopplysninger som gjøres, slik at man vet hvilke krav som gjelder for behandlingen og hvilke tiltak, herunder rutiner og dokumentasjon, en må ha for å følge regelverket, hvilket forhold man har til databehandlere og overføring av personopplysninger til tredjeparter og -land (ut av EØS), hvordan rettighetene til de personopplysningene gjelder (de registrerte) skal følges, informasjon som skal gis (som i personvernerklæring) mv.

Kartlegging av behandlingen av personopplysninger gjøres bl.a. gjennom behandlingsoversikten som skal lages etter GDPR artikkel 30. Databehandlere skal lage egen behandlingsprotokoll etter GDPR artikkel 30 (2).

- 2. Rutiner/prosedyrer.** Det må rutiner og prosedyrer til for å sikre at behandlingen av personopplysninger gjøres riktig i det daglige arbeidet. Dette er det som omtales som «internkontroll» og følger av GDPR artikkel 24. Nødvendige rutiner/prosedyrer må lages og implementeres (se neste punkt). For rutiner som er aktuelle, se del II nedenfor.

Styret (eller tilsvarende) har ansvar for at det skal etableres rutiner, og daglig ledelse (som daglig leder) har det operative ansvaret for å utarbeide og implementere rutine i virksomheten som en del av ansvaret denne har for at regelverket overholdes.

- 3. Informasjon/opplæring:** Organisasjonen, som ansatte og andre som har oppgaver knyttet til behandling eller er ellers i befattning med personopplysninger, må være kjent med og kunne personvernregelverket og de rutiner/prosedyrer som skal følges. Det må derfor gis informasjon om regelverk og rutiner og gjennomføres opplæring.
- 4. Informasjon til de det behandles personopplysninger om/personvernerklæring.** De det behandles personopplysninger om (de registrerte) skal ha informasjon om behandlingen som gjøres. En del av dette personvernerklæring på nettsider eller at det informeres på annen måte. Ansatte og andre interne må også informeres enten ved egen personvernerklæring eller på annen måte.
- 5. Sikre dokumentasjon:** Arbeidet med å overholde regelverket må dokumenteres (ellers foreligger det ingen «bevis» på arbeidet). Dette omfatter tiltak, vurderinger, rutiner/prosedyrer mv. Dokumentasjon bør samles på et bestemt område slik at dette er tilgjengelig når det er behov.

¹ Se bl.a. hva Datatilsynet gir råd om knyttet til rutiner og dokumentasjon: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet-internkontroll/etablere-internkontroll/>

6. **Gjennomføre kontroller.** Det må gjøres kontroller for at man skal avdekkes om regelverket, rutiner/prosedyrer mv. følges. Dette er også en del av internkontrollen. Følges ikke regelverket, rutiner mv., må det behandles som avvik, se neste punkt.
7. **Avviksbehandling/personvernbrudd.** Oppdages det brudd på regelverket, rutiner/-prosedyrer eller annet som kreves for lovlig behandling av personopplysninger, må dette håndteres som avvik og det må gjøres tiltak for å utbedre avviket for å redusere følgene av og risikoen for nytt avvik. Hendelser, beslutninger og aktiviteter/tiltak knyttet til avviket må dokumenteres. Avvik av en viss alvorlighet for personvernet skal varsles til Datatilsynet, og eventuelt til de registrerte.
8. **Rapportering.** Ledelsen og eventuelt styret bør få rapporter slik at de som har det øverste ansvaret er kjent med status og hendelser. Slik rapportering kan gjelde status på personvernarbeidet, personvernbrudd og erfaringer, eventuelle endringer i rutiner og risikovurderinger, gjennomføring av kontroller og resultatet, og annet relevant for overholdelse av personvernregelverket og sikring av personopplysninger.
9. **Videre arbeid.** Overholdelse av personvernregelverket (og annet regelverk) er et kontinuerlig arbeid. Etter tiltakene ovenfor er gjennomført må arbeidet fortsette.

Endringer vil skje i behandling og personopplysninger som behandles, registrerte det behandles personopplysninger om, rammeforhold som i teknologi og organisatoriske forhold, risikoen ved behandling, det vil skje avvik, gjøres nye erfaringer knyttet til behandling eller rutiner, endringer i regelverk og hvordan dette praktiseres, mv.

Dette gjør at man må gjøre nye vurderinger, som risikovurderinger, endringer i hvordan regelverket overholdes, oppdatering av, endringer i og nye rutiner og dokumentasjon, endringer i informasjon som gis til registrerte, ytterligere kontroller, rapportering mv.

Tiltak som nevnt ovenfor kan følge av hendelser, som avvik, eller ved regelmessig gjennomgang av behandling, rutiner, dokumentasjon mv. Gjennomganger bør også gjøres regelmessig, men ikke sjeldnere enn årlig.

DEL I RUTINER/PROSEDYRER OG DOKUMENTASJON

Som nevnt ovenfor er rutiner og prosedyrer avgjørende for å sikre at regelverket, herunder personvernforordningen, følges. I tillegg skal tiltakene kunne «påvises», dvs. kunne vises er gjennomført, og for dette er dokumentasjon nødvendig. Nedenfor følger en oversikt over rutiner/prosedyrer og annen dokumentasjon kan være aktuell. Det må allikevel vurderes hva som kreves i den enkelte virksomhet ut fra behandlingen av personopplysninger som gjøres.

A. Dokumentasjon (rutiner) som alle virksomheter bør/må ha:

1. Generelle/overordnede rutiner/styringsdokumenter for behandling av personopplysninger. Bør inneholde strategiske, operative og kontrollerende elementer, men som suppleres av rutinene nedenfor. Disse overordnede rutinene, sammen med øvrige rutiner, utgjør internkontrollen for behandling og sikring av personopplysninger.
2. Behandlingsprotokoll (eventuelt inkludert risikovurderinger og krav til sletting, hvis ikke dette er inntatt i egne dokumenter) etter GDPR artikkel 30.
3. Dokumentasjon på eventuelle gjennomførte risikovurderinger/vurderinger av personvernkonsekvenser (DPIA), herunder kontakt med Datatilsynet i denne forbindelse.
4. Informasjon om behandling av personopplysninger/personvernerklæring for eksterne, som kunder mv.
5. Informasjon om behandling av personopplysninger/personvernerklæring for interne, som ansatte mv.

6. Rutine for lagringstid og sletting av personopplysninger (kan også være omfattet av eller bør koordineres med behandlingsprotokoll og/eller personvernerklæring).
7. Dokumentasjon på inngåtte databehandleravtaler, ofte i form av selve avtalene.
8. Rutine for håndtering av personvernbrudd (avvik) og varsling av Datatilsynet/registrerte.

B. Dokumentasjon (rutiner) som virksomheter bør vurdere å ha ut fra hvilken behandling som gjøres av personopplysninger. Noen rutiner eller deler kan være overlappende og kan være dekket i de generelle rutinene i punkt A.1 ovenfor.

1. Generelt og behandlingsgrunnlag

- a. Rutine for kartlegging av personopplysninger, føring og endring av behandlingsprotokoll etter GDPR artikkel 30.
- b. Rutine for ny, endret eller opphørt behandling av personopplysninger.
- c. Dokumentasjon på avgitte samtykker, med bekreftelse på aksept av samtykke, når samtykke ble innhentet og innholdet i det konkrete samtykket, eventuelt rutine for bruk av samtykker.
- d. Dokumentasjon på vurderinger av om det foreligger berettiget interesse etter GDPR artikkel 6 (1) f), samt mal for slike vurderinger.
- e. Dokumentasjon på vurderinger for behandling til annet formål enn opplysningene opprinnelig ble innsamlet for.
- f. Dokumentasjon på råd og vurderinger fra eksterne rådgivere.

2. De registrertes rettigheter

- a. Informering av og krav om informasjon fra de registrerte/personvernerklæring, herunder sjekklister for informasjon og personvernerklæring.
- b. Håndtering av krav om innsyn (utlevering av personopplysninger) fra registrerte.
- c. Håndtering av krav om retting fra registrerte.
- d. Håndtering av krav om sletting fra registrerte (om ikke dekket av rutinene for sletting generelt).
- e. Håndtering av krav om begrensning i behandling fra registrerte.
- f. Håndtering av krav om dataportabilitet fra registrerte.
- g. Håndtering av krav om avslutning av behandling (protest/innsigelse) fra registrerte.

3. Interne forhold. Se også nedenfor om sikring av personopplysninger.

- a. Rutine for behandling av personopplysninger ved rekruttering/ansettelse.
- b. Rutine for opplæring i og implementering av rutiner og personverntiltak.
- c. Rutine for innsyn i ansattes epost/personlige områder.
- d. Rutine for tiltredelse/fratredelse (onboarding og offboarding) og dokumentasjon på gjennomgang ved tiltredelse/fratredelse (sistnevnte lagres i HR-dokumentene).
- e. Rutine for bruk av eksterne konsulenter, andres tilgang til systemer mv.
- f. Rutine for informasjonshåndtering, som lagring av informasjon, dokumenter mv., håndtering av ustrukturert informasjon.
- g. Rutine for ansattes mv. bruk av sosiale medier (eventuelt offentlige ytringer).
- h. Rutine for bruk av bilder og video, for ansatte, eksterne mv.
- i. Rutine for bruk av kunstig intelligens.
- j. Dokumentasjon på vurdering av om personvernombud skal etableres, rutiner for personvernombud (hvis aktuelt) og dokumentasjon på råd fra personvernombud.

4. Sikring av personopplysninger (informasjonssikkerhet)

- a. Rutine og mal for risikovurdering/vurdering av personvernkonsekvenser (DPIA).
- b. Sikkerhetsinstruks (herunder it-sikkerhetskrav) for ansatte, eventuelt egen for it-avdeling, utvikling, testing, driftsrutiner mv.
- c. Konfidensialitetserklæring for ansatte, innleide og andre, herunder mal for erklæringer.
- d. Krav til sikkerhetstiltak, tekniske og organisatoriske, for egen virksomhet, leverandører, databehandlere (underdatabehandlere) mv., herunder beredskapsplaner
- e. Rutine for tilgang til bruker/kundedata, logger, sikkerhetskopier mv.
- f. Rutine for kameraovervåking.
- g. Rutine for fysisk adgangskontroll (teknisk/systemmessig adgangskontroll bør dekkes av it-sikkerhetspolicy).

5. Databehandlerforhold, tredjeparter og overføring

- a. Rutine for bruk av databehandler, dokumentasjon av databehandleravtaler som er inngått (se også punkt A.7), dokumentasjon på gjennomført revisjon av databehandler, og mal for databehandleravtale.
- b. Rutine for behandling av personopplysninger som databehandler samt mal for databehandleravtale.
- c. Rutine om og avtaler om overføring av personopplysninger mellom behandlingsansvarlige og andre.
- d. Rutine om felles behandlingsansvar, med dokumentasjon av avtaler og mal.
- e. Rutine for overføring av personopplysninger til land utenfor EØS (tredjeland) og dokumentasjon på vurderinger om slik overføring kan skje, samt mal for slike vurderinger.

6. Markedsføring mv.

- a. Rutine for arrangementer mv.
- b. Rutine for markedsføring, nyhetsbrev, sosiale medier mv.
- c. Rutine for bruk av informasjonskapsler, cookies mv.

7. Kontroll og avvik

- a. Rutine for avvik og personvernbrudd, herunder for varsling av Datatilsynet og de registrerte samt mal for avviksrapportering og for melding til Datatilsynet.
- b. Rutine og dokumentasjon på kontroller for å sikre at regelverket, rutiner mv. overholdes.
- c. Rutine for rapportering til ledelse/styre, herunder mal for rapportering som kan omfatte endringer i behandling og/eller risikobilde, oppdatering av rutiner, personvernbrudd/avvik mv.
- d. Personvernlogg, hvor hendelser føres inn, som mottatte krav fra de registrerte, personvernbrudd/avvik, vurderinger som er gjort, kontroller som er gjennomført, endringer i behandling som har ført til endringer i rutiner og dokumentasjon, rapporter for ledelse/styre mv.

Rutinene ovenfor må tilpasses virksomheten og behandlingen som gjøres av personopplysninger, og det må vurderes om det er behov for andre rutiner enn ovennevnte, som pga. virksomheten er underlagt spesielt regelverk, som ved behandling av helseopplysninger, eller andre forhold knyttet til virksomhetens behandling av personopplysninger.