Personvern, informasjonssikkerhet og internkontroll - oppsummering

Lover og regler:

- Regelverk: **Personopplysningsloven** og **personopplysningsforskriften**.
- Personopplysningsloven stiller **krav til internkontroll** (§ 14).
- Etablering av internkontrollen (planlagte/systematiske tiltak, rutiner, dokumentert) skal sikre at regelverket blir etterlevd.
- **Grunnkrav § 11**: Behandlingsgrunnlag må foreligge (§§ 8 og 9), personopplysninger kan bare brukes til et uttrykkelig angitt og saklig formål (f. eks. lovpålagte oppgaver). Tilstrekkelige og kun relevante opplysninger for formålet, korrekte og oppdaterte opplysninger. Opplysningene slettes (§ 28) når det ikke lenger er bruk for dem (blir i enkelte tilfeller «overstyrt» av arkivloven og andre særlover).
- For behandling av personopplysninger er det ofte **meldeplikt** og i noen tilfeller **konsesjonsplikt**.
- En del **plikter** (for kommunen) **og rettigheter** (for den registrerte) følger av reglene.
- **Fødselsnummer** og bruken av disse: § 12 (må være saklig behov for bruk).
- Sannsynligvis er **kunnskapen om personopplysningsloven med forskrift begrenset**?
- **Nye personvernregler kommer.** EUs forordning for personvern blir norsk lov i 2018.

Noen definisjoner:

- **Personopplysninger**: All informasjon og alle vurderinger som kan knyttes til en bestemt enkeltperson.
- **Sensitive personopplysninger**: Informasjon om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, strafferettslige forhold, helseforhold, seksuelle forhold og medlemskap i fagforeninger. Særlig beskyttelsesbehov for denne typen opplysninger.
- **Informasjonssikkerhet:** Å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger.

Mål:

- Unngå **krenkelser av personvernet** (og tilliten).
- Alle personopplysninger skal være **tilfredsstillende sikret, dvs. tilfredsstillende informasjonssikkerhet** (§ 13, rom for tolkinger rundt akseptabelt nivå).

Noen roller:

- **Behandlingsansvarlig**
- **Sikkerhetsansvarlig**
- Enkelte ansatte kan ha blitt tildelt **systemansvar og/eller er systemeier / dataeier**.
- **Enhetsledere** har gjerne et særskilt ansvar for oppfølging i sin enhet.
- Hvis eksterne aktører foretar databehandling på vegne av virksomheten/behandlingsansvarlig: Det MÅ (pliktig) foreligge **databehandleravtale**.

Datatilsynet:

- **Datatilsynet** fører kontroll og tilsyn, og de kan straffe med f. eks. bøter hvis informasjonssikkerheten er for dårlig og/eller internkontroll ikke er innført.
- Mye informasjon tilgjengelig på deres nettside: http://www.datatilsynet.no/

Ledelsen:

- **Ledelsen** (virksomhetsleder) har et spesialt overordnet ansvar for personvern og informasjonssikkerhet.
- Virksomhetsleder kan ikke **delegere** selve ansvaret til andre, selv om enkelte praktiske arbeidsoppgaver kan delegeres

Informasjonssikkerhet:

- Mange **sikkerhetstrusler**.
- **Informasjonssikkerhet** skal ivareta tre hensyn **(KIS)**:
    - Sikre personopplysningene **konfidensialitet** (hindre tilgang for uvedkommende)
    - Sikre personopplysningene **integritet** (hindre endring/sletting fra uautoriserte personer)
    - Sikre personopplysningene **tilgjengelighet** (sikre tilgjengelighet til enhver tid for dem som har rett til/behov for opplysningene).
- **Akseptkriterier**: Lokale definisjoner av tilfredsstillende informasjonssikkerhet (akseptabelt risikonivå).
- Andre begrep: Ledelsens gjennomgang, sikkerhetsmål, sikkerhetsstrategi, sikkerhetsorganisasjon, sikkerhetstiltak, revisjon. Se eventuelt informasjon hos Datatilsynet.
- **Datatilsynet har laget til en omfattende samling med maler** som kan benyttes som utgangspunkt/utfylling for å komme i gang med internkontroll (informasjonssikkerhet).

Oversikt over personopplysninger som behandles av organisasjonen:

- **Hvilke personopplysninger** virksomheten behandler må identifiseres.

Risikovurdering/risikoanalyse:

- **Risikovurdering** skal foretas jevnlig (1 gang i året) og ved behov (ved endringer).
- Skal avdekke aktuelle/potensielle uønskede hendelser som har en negativ effekt på personvernet til ansatte eller tjenestemottakere.
- Risikovurdering:
    - **Kartlegge** uønskede hendelser som kan inntreffe (trussel).
    - **Vurdere** hendelsenes risiko (sannsynlighet og konsekvens)
    - **Prioritere** sikkerhetstiltak (prioritere tiltak til hendelser med stor risiko, dvs. høy sannsynlighet og stor skadevirkning).

Oppfølging:

- Utarbeide **reglement, rutiner m. m.**
- **Avvikshåndtering**, avviksbehandling og **egenkontroll**.
- **Avviksmelding** / avviksskjema.
- Nødvendig: System og rutiner for å kunne **rapportere avvik.**

Normen og Feide:

Verdt å nevne i forbindelse med offentlig sektor:

- Normen for helsesektoren m. m.: "Hva er **Normen**? Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Normen) er et omforent sett av krav til informasjonssikkerhet, basert på lovverket, og er utarbeidet av representanter for sektoren. Alle aktører i sektoren som er tilknyttet Norsk Helsenett, er avtalerettslig forpliktet til å følge Normen.» Vi er Norsk Helsenett-kunder.
- **Feide** (Felles Elektronisk IDEntitet.) for oppvekst/skole: For å kunne ta i bruk og "koble seg på" Feide kreves det inngåelse av en kontrakt. Vertsorganisasjonen må tilfredsstille en del krav (behandling av person-opplysninger, IKT-reglement, teknisk løsning, førstelinjesupport) for å kunne ta i bruk Feide. Vi bruker Feide.
- Lenker: http://www.normen.no og https://www.feide.no/

Nye personvernregler fra 2018:

- EU har våren 2016 vedtatt ny **personvernforordning** som vil bli iverksatt fra mai **2018**. Den nye personvernlovgivningen vil også gjelde for Norge (jf. EØS-avtalen).
- EU har sett behovet for et bedre personvern og et modernisert regelverk, slik at det ikke blir rett fram for vilkårlig og planløs behandling av personopplysninger

Noen sentrale momenter rundt de nye reglene fra 2018:

- **Innebygd personvern** som utgangspunkt for nye løsninger (den mest personvernvennlige innstilling som standard).
- **Borgerne/innbyggerne får nye rettigheter**, f. eks. dataportabilitet.
- Krav om **personvernombud** i mange virksomheter, blant annet i alle kommuner.
- **Vurdere personvernkonsekvenser og risiko** før igangsetting av (større) tiltak.
- Strengere krav til **avvikshåndtering**.
- **Nye plikter til virksomheter og databehandlere**.
- Forståelig **personvernerklæring** blir et krav.

Og:

- Fortsatt blir det behov for å inngå **Databehandleravtaler** med eksterne leverandører som behandler personopplysninger på vegne av en virksomhet.
- **Bøtene/gebyrene** som kan skrives ut for manglende personvern blir mye større enn dagens.

Mer informasjon: https://www.datatilsynet.no/forordning

Dokument utarbeidet av Bjørn Roger Rasmussen (http://www.brr.no/).