1 Opplæring

Sjekklisten er dynamisk, ikke uttømmende og skal oppdateres regelmessig. Dersom du har innspill til noen av punktene, vil vi gjerne høre fra deg.

Hva bør det gis opplæring i?

Det bør gis opplæring i

- personvernforordningen generelt, og spesielt
  - personvernprinsippene, artikkel 5
  - behandlingens lovlighet, artikkel 6
  - vilkår for samtykke, artikkel 7 og 8
  - behandling av særlige kategorier av personopplysninger, og straffbare forhold, artikkel 9 og 10
  - kapittel III om den registrertes rettigheter, artikkel 12-23
  - kapittel IV om behandlingsansvarliges og databehandleres plikter, artikkel 24-43, spesielt
    - innebygd personvern og personvern som standardinnstilling
    - protokoller over behandlingsaktiviteter
    - sikkerhet ved behandlingen
    - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten og underretning av den registrerte
    - vurdering av personvernkonsekvenser og forhåndsdrøftinger
    - personvernrådgiver, utnevne, stillingsbeskrivelse, avklaring av oppgaver
    - atferdsnormer og sertifisering
- lov og regelverk relatert til fagområdet for programvaren som skal utvikles (for eksempel pasientjournalloven, kommunikasjonsvernforordningen (ePrivacy), IKT-forskriften)
- obligatoriske krav fra næringslivet/sektor/bransje
- virksomhetens egne krav til informasjonssikkerhet
- virksomhetens egen internkontroll
- roller og organisering av arbeidet med personvern og informasjonssikkerhet
- rammeverk for informasjonssikkerhet (for eksempel ISO27001, Standard of Good Practice (SoGP))
- rammeverk for utvikling (for eksempel Microsoft Security Development Lifecycle (SDL), ISO27034
- sikkerhetstesting (for eksempel OWASP Top 10, OWASP Testing Guide, OWASP ASVS walkthrough)
- trussel- og risikovurdering (for eksempel STRIDE, DREAD, Microsoft Threat Modeling Tool)
- dokumentasjonskrav

Hvem bør ha opplæring?

- Alle ansatte bør ha basiskunnskap om personvern og informasjonssikkerhet.
- Ledelsen bør ha kunnskap om vurdering av personvernkonsekvenser, risikovurderinger, ledelsens ansvar og håndtering av risiko for personvern og informasjonssikkerhet.
- Prosjektledere bør ha kunnskap om innebygd personvern og innebygd sikkerhet.
- Utviklere bør ha kunnskap om sikker koding, innebygd personvern og innebygd sikkerhet.
- Arkitekter bør ha kunnskap om sikkerhetsarkitektur, innebygd personvern og innebygd sikkerhet.
- Testere bør ha kunnskap om sikkerhetstesting, innebygd personvern og innebygd sikkerhet.

- Leverandører bør ha kunnskap om sikker drift og forvaltning, innebygd personvern og innebygd sikkerhet, databehandleravtalen, hendelseshåndtering og beredskap

Hvordan bør opplæringen gis?

Opplæringen bør gis

- ved oppstart av arbeidsforhold
- som regelmessig oppdatering
- ved oppstart av (utviklings)prosjekt

Det kan for eksempel gis opplæring

- gjennom differensiert opplæringsprogram på ulike nivå fra grunnleggende ferdigheter (som er et minimum og obligatorisk) til spesial- og/eller dybdekunnskap (som kan være for dedikerte ansatte)
- via ulike opplæringsformer og verktøy (slik som klasserom, kursmateriell, workshop, e-læring, konkurranser, en-til-en samtaler, sertifiseringer, kursing, metaforer (bobby-tables som er lett å huske), One-Pager, film, belønning og lignende)
- gjennom oppdatering til ansatte etter internkontroll
- gjennom oppdatering til ansatte etter penetrasjonstesting
- ved å kontrollere at ansatte leser virksomhetens sikkerhetspolicy som omfatter krav om innebygd personvern
- som regelmessig fast punkt på agendaen i utviklerforum eller fagforum

Hvorfor skal det gis opplæring?

- Personvernforordningen setter krav til at det skal treffes egnede tekniske og organisatoriske tiltak for å sikre fysiske personers rettigheter og friheter. Opplæring er et organisatorisk tiltak og er en plikt som gjenspeiles i personvernforordningen, i artiklene 24, 25, 28, 32 og 39 (1) b).
- Opplæringen skal være forankret hos ledelsen, og dermed i organisasjonen.