GDPR og Personopplysningsloven
Det kommer nye personvernregler og ny Personopplysningslov i 2018. Dette dokumentet beskriver overordnet hva dette innebærer.

Hva er GDPR

- General Data Protection Regulation a.k.a. EUs Personvernforordning
- En "forordning" er obligatorisk for medlemslandene og skal implementeres i lokale lover.
- Gjelder for alle som håndterer personopplysninger, dvs alle virksomheter som har ansatte, kunder (for eksempel klienter eller elever) eller medlemmer.
- Erstatter tidligere lovverk og er pliktig å følge.
- Trer i kraft 25. mai 2018.

Hovedfokus
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the **protection of natural persons** with regard to the **processing of personal data** and on the **free movement of such data**, and repealing Directive 95/46/EC (General Data Protection Regulation).

Altså, økt fokus på at personopplysninger tilhører personen selv, at personopplysninger skal beskyttes mot misbruk og at enkeltpersoner skal kunne ta med seg sine opplysninger fra en "leverandør" til en annen.

Ansvar

- Virksomhetens ledelse (daglig leder) har det juridiske ansvaret for å oppfylle kravene i GDPR og å utforme nye rutiner.
- Det operasjonelle ansvaret kan delegeres til en personvernansvarlig (person) eller et personvernombud (person).
- Alle i organisasjonen må kjenne til og følge de nye reglene.
- Man må kunne vise at man tar ansvar.

Roller

- **Registrert**
  Person det er registrert opplysninger om.
- **Behandlingsansvarlig**
  Firma eller organisasjon som bestemmer formålet og grunnlaget for å håndtere personopplysninger, og som vanligvis har kundeforholdet til «den registrerte».
- **Personvernombud**
  Person hos behandlingsansvarlig med spesielt ansvar for personvern og datasikkerhet.
- **Databehandler**
  Ekstern part som håndterer personopplysninger på vegne av behandlingsansvarlig.

Datatilsynets forventninger

- At man vet hvem «sine registrerte» er.
- At man vet noe om hva personvern er.
- At man vet hvilke opplysninger man har om de registrerte og hvor disse opplysningene kommer fra.
- At man vet hvorfor man trenger akkurat disse opplysningene om de registrerte.
- Om man vet om man kan gjennomføre oppgavene med færre opplysninger.
- At man vet hvem i sin organisasjon som beslutter om opplysninger skal slettes/rettes og hvem som faktisk gjør det.
- At man vet hvor man finner informasjon om internkontrollsystem og rutiner for informasjonssikkerhet og hvordan dette kan hjelpe en i arbeidshverdagen.

Generelt om lagring og bruk av personopplysninger
For at man skal få lov til å lagre og håndtere personopplysninger i det hele tatt skal det foreligge et **formål** og et **grunnlag**. Begge deler skal dokumenteres og kunne fremvises ved innsynskrav fra enkeltpersoner eller ved tilsyn.

- Det skal kun lagres opplysninger som er nødvendig for formålet.
- Opplysningene skal slettes når de ikke lenger er nødvendige for formålet, unntatt for å
  - Forsvare et rettskrav.
  - Ivareta viktige samfunnsinteresser.
  - Oppfylle andre lovkrav.
- Personopplysninger kan kun håndteres når det foreligger et grunnlag.
- Innhenting og håndtering av personopplysninger er kun tillatt dersom
  - Den registrerte har gitt samtykke.
  - Det foreligger grunnlag i lov.
  - Det er nødvendig for å oppfylle en avtale.
  - Det er påkrevet gjennom en rettslig forpliktelse.
  - Det er nødvendig for å beskytte avgjørende interesser for virksomheten eller den den registrerte (berettiget interesse).
  - Det er nødvendig for å utføre oppgaver av offentlig interesse eller oppgaver som utføres av regjering, skattemyndigheter, politi eller andre offentlige instanser.
- Det skal finnes en oversikt over alle aktiviteter som håndterer personopplysninger.

Enkeltpersoners rettigheter
- Retten til innsyn.
- Retten til korrigering av uriktig eller mangelfull informasjon.
- Retten til begrensning av bruk av sine personopplysninger.
- Retten til å motsette seg bruk av sine personopplysninger..
- Retten til dataportabilitet.
- Retten til å bli glemt.

Man må dokumentere alle rutiner knyttet til enkeltpersoners rettigheter og ha kontroll på hvem som er faktisk utførende i virksomheten.

Databehandlere
En databehandler er en leverandør av systemer eller tjenester som lagrer eller håndterer personopplysninger, for eksempel HR og lønnssystemer, fakturering og regnskap, WEB-hotell, sky-tjenester, etc. Alle virksomheter må dokumentere hvilke databehandlere de bruker og at det foreligger en databehandleravtale for hver av dem som oppfyller de nye kravene.

Personvernerklæring
Det skal foreligge en personvernerklæring som beskriver av hvordan virksomheten samler inn og bruker personopplysninger. Den skal være en egen frittstående erklæring uavhengig av annen avtaletekst. Informasjonen skal være kortfattet, klar og tydelig, lett forståelig og lett tilgjengelig. Det er ekstra fokus for de som håndterer personopplysninger om barn.

Personvernerklæringen skal inneholde følgende:
- Kontaktopplysninger til den behandlingsansvarlige og personvernombudet.
- Hva slags personopplysninger som håndteres.
- Formålene med bruken og behandlingsgrunnlaget.
- Retten til å trekke tilbake eventuelt samtykke.
- Hvilke legitime interesser den behandlingsansvarlige har dersom håndteringen er basert på berettiget interesse.

- Informasjon om eventuell overføring av personopplysninger til annen part, annet land eller internasjonal organisasjon.
- Lagringstid eller kriterier for å fastsette tid.
- Den registrertes rettigheter.
- Retten til å klage til en tilsynsmyndighet.

Risiko og konsekvensanalyse
Alle virksomheter har plikt til å utrede personvernkonsekvenser når det planlegges bruk av personopplysninger som **sannsynligvis** vil utgjøre **høy risiko** for personers rettigheter, som retten til personvern. Det må derfor gjøres en risikovurdering for all bruk. Vurderingene skal dokumenteres.

I vurderingene skal det tas hensyn til arten, omfanget, sammenhengen og formålet med bruken av personopplysninger. Det må også tas hensyn til om det benyttes ny teknologi.

Avvikshåndtering
- Strengere regler enn i dag.
- Både Datatilsynet og de berørte skal varsles.
- Behandlingsansvarlig skal melde avvik til Datatilsynet innen 72 timer.
- Det stilles krav til innholdet i avviksmeldingen.
- De berørte skal varsles i klart språk.

Informasjonssikkerhet
Virksomheten skal dokumentere at den har tilstrekkelig informasjonssikkerhet i henhold til de nye kravene og at den kan håndtere risiko relatert til virksomhetens informasjonsverdier og bruk av personopplysninger:
- **Konfidensialitet**: Hindre uvedkommende i å få tilgang på opplysningene.
- **Integritet**: Ingen uautorisert eller utilsiktet endring av opplysninger.
- **Tilgjengelighet**: Opplysningene er tilgjengelige når tilgang er nødvendig.

Internkontroll
- Virksomhetene skal sette i verk egnede tiltak, både tekniske og organisatoriske, for å sikre at personopplysninger håndteres i samsvar med regelverket.
- Det skal finnes rutiner for å ivareta de registrertes rettigheter.
- Det skal finnes en oversikt over alle aktiviteter som håndterer personopplysninger.

Sanksjoner
- Brudd på behandlingsansvarliges eller databehandleres forpliktelser.
  - 10 millioner euro, eller 2% av årlig global omsetning.
- Overtredelse av grunnprinsippene, inkludert samtykke.
  - 20 millioner euro, eller 4% av årlig global omsetning.
- Overtredelse av påbud fra Datatilsynet.
  - 20 millioner euro, eller 4% av årlig global omsetning.