

GDPR

Status og veien videre

Inge V. Bakken

12. April 2018

○ Respekt ○ Faglig dyktighet ○ Tilgjengelighet ○ Engasjement

GDPR

- EUs personvernforordning (GDPR – Generell Data Protection Regulations)
- Om arbeidet så langt ved SSHF.

Noen hovedelementer i ny personvernlovgivning

- Forordningen begynner å gjelde 25. mai 2018
- Forordningen erstatter gjeldende personverndirektiv 95/46/EF («95 direktivet») som er inntatt i EØS-avtalen og gjennomført i den nåværende personopplysningsloven.
- Ny personopplysningslov kan ikke tre i kraft før forordningen er innlemmet i EØS-avtalen gjennom en beslutning i EØS-komiteen. Slik beslutning er ennå ikke truffet.

Personvernprinsipp (art 5)

1. Lovlig (krav om rettsgrunnlag)
2. Formålsbegrensning (kun til angitt formål)
3. Dataminimering (ikke flere opplysninger enn nødvendig)
4. Riktighet (korrekte data/krav til evnt korrigerings)
5. Lagringsbegrensning (oppbevaring kun så lenge det er nødvendig ut fra formålet)
6. Sikker lagring (vern mot uautorisert eller ulovlig behandling)
7. Ansvar (behandlingsansvarlig skal påse at 1-6 sikres)

EU's personvernforordning (GDPR)

- Hovedsakelig en videreføring der gjeldende rett forsterkes og videreutvikles.
- Oppfyller vi eksisterende lovkrav, så er vi godt rustet.

Nye og skjerpede regler om rettigheter for den registrerte:

- Informasjon om hva som er registrert
- Dataportabilitet
- Retting, art 16:
- Sletting, («right to be forgotten»), art 17
- Rett til å kreve begrensninger av behandlingen av personopplysningene, art 18
- Rett til å motsette seg behandling, art 21

Forsterkede internkontrollplikter for virksomheten

- Må dokumentere etterlevelse (økt økonomisk risiko ved svikt)
- Tydelig ledelsesforankring på øverste adm nivå
- Krav til styrende, gjennomførende og kontrollerende dokumentasjon.
- Krav om å vurdere personvernkonsekvenser-risikoavhengig.
- Krav om innebygd personvern i valgte tekniske og organisatoriske løsninger (den minst personverninngrepene løsning)
- Avvikshåndtering og kontroll
- Krav om personvernombud

Roller og ansvar

- Dataansvarlig (DA)
 - Den som alene eller sammen med andre bestemmer formålet med behandlingen og hvilke midler som skal brukes, art 4
 - DA skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. artikkel 32.

- Databehandler (DB)
 - Den som behandler personopplysninger på vegne av DA, art 4
 - Snakker om andre virksomheter, ikke egne ansatte, dvs at DB ikke ville hatt tilgang til de aktuelle opplysninger hvis det ikke var for oppdraget.
 - Databehandleravtaler

Personvernombudet (PO)

- Gi råd og veiledning til datasansvarlig
- Kontaktpunkt mot datatilsynet.
- Holde seg orientert om utviklingen innen personvern.
- Uavhengighet – rapportere direkte til høyeste ledelsesnivå, art 37-39
- Lovpålagt taushetsplikt.
- Påse at behandlingsansvarlig har et tilfredsstillende system for internkontroll.
- Bistå de registrerte med å ivareta deres rettigheter etter reglene om behandling av personopplysninger.
- Påpeke brudd på personopplysningsloven overfor behandlingsansvarlig.

Særlovgivningen innen helsefeltet

- Behandling av pasientopplysninger er i stor grad regulert gjennom særlovgivning herunder helsepersonelloven og pasientjournalloven

Oppgaver framover og status:

Etablere tilfredsstillende internkontroll:

- Skaffe oversikt over de krav vi må etterleve og informere om i organisasjonen.
- Kontroll på prosesser der vi behandler personopplysninger
- Etablere styrende dokumenter som bl.a beskriver: Personvernpolicy, strategiske føringer, målsettinger, ansvarslinjene/roller
- Etablere nødvendige prosedyrer for å sikre korrekt håndtering av personopplysninger. (Bl.a om samtykke, info til de registrerte, om retting og sletting)
- Etablere rutiner for avvikshåndtering, kontroll og dokumentasjon.
- Personvernombud – melde til DT at dette er etablert

Kontroll på prosesser der vi behandler personopplysninger, eksempler:

- Ansatte
- Leverandører/kunder
- Medisinskteknisk utstyr
- Applikasjoner
- Pasienter
- Pårørende.
- Anskaffelser