Helse Sør-Øst RHF

Gode og likeverdige helsetjenester til alle som trenger det, når de trenger det, uavhengig av alder, bosted, etnisk bakgrunn, kjønn og økonomi.

Veileder
GDPR i prosjekter

Prosjektstyringsmodell for Helse Sør-Øst

Versjon Q1 2018

HELSE SØR-ØST

Innholdsfortegnelse

HELSE SØR-ØST

Innledning

Overordnede krav i GDPR

HELSE SØR-ØST

Definisjoner

- **Den registrerte** – Den som får opplysninger om seg behandlet
- **Behandling** – Alle operasjoner, enten automatiserte eller manuelle, som gjøres på personopplysninger. Innsamling, overføring, lagring, og så videre
- **Personopplysninger –** All informasjon som kan knyttes til en identifisert eller identifiserbar person.
- **Sensitive personopplysninger (Særlige kategorier av personopplysninger) –** Opplysninger om rase eller etnisk opprinnelse, politiske meninger, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap, behandling av genetisk eller biometriske opplysninger med formålet å entydig identifisere en person, helseopplysninger, eller opplysninger om seksuelle forhold eller seksuell orientering.

HELSE SØR-ØST

Definisjoner

- **Personvernkonsekvensvurdering (DPIA) –** En prosess for å hjelpe til å identifisere og håndtere risikoer knyttet til behandling av personopplysninger

- **Innebygd Personvern –** Et prinsipp som sørger for at personvern er en sentral funksjon i og tas hensyn til i alle utviklingsfasene i et system/løsning

- **Dataminimering** – At så lite data som nødvendig samles inn for å oppfylle formålet med behandlingen, og at opplysninger ikke brukes til andre formål enn de ble samlet inn for

HELSE SØR-ØST

Hvorfor er det viktig å ivareta GDPR i prosjekter?

- Brudd på personvernet kan få svært alvorlige konsekvenser både for oss og for de registrerte
  - Brudd på personvernet kan være **svært belastende** for dem som får opplysningene sine på avveie, og føre til for eksempel **økonomiske tap**
  - Helseforetak kan få **store bøter og tape omdømme**

HELSE SØR-ØST

Overordnede krav i GDPR for prosjekter

1. Innebygd personvern må være med helt fra starten

2. I mange tilfeller skal det gjøres en personvernkonsekvensvurdering (DPIA)

3. Alle er ansvarlige for å ivareta personvernet til de som får opplysningene sine behandlet

HELSE SØR-ØST

GDPR i de forskjellige prosjektfasene

HELSE SØR-ØST

GDPR i de forskjellige prosjektfasene

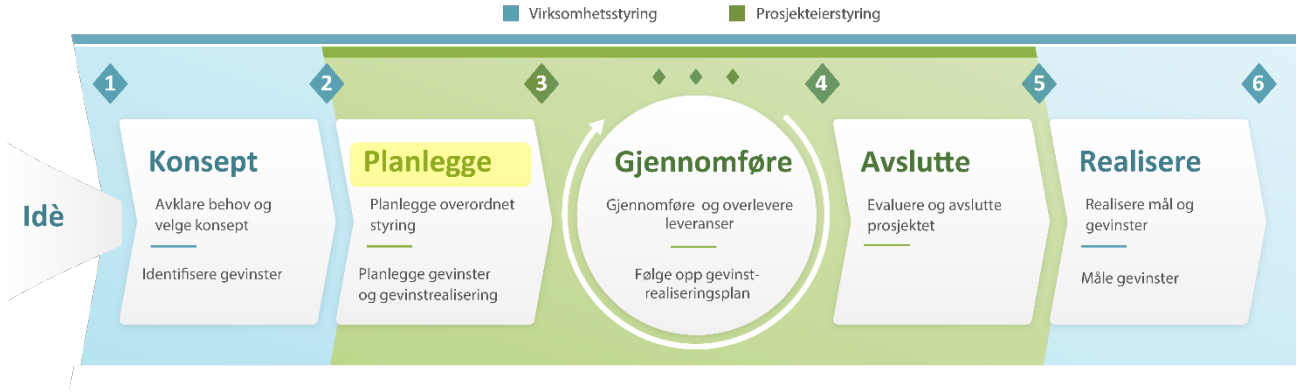
Konseptfasen

- Kartlegg hvilke krav om personvern og informasjonssikkerhet som er relevante å følge. Kravene finnes i det regionale styringssystem for informasjonssikkerhet og eventuelle lokale krav
- Behovene for personvern og informasjonssikkerhet må avklares
- Vurder om konseptet krever en personvernkonsekvensvurdering (*)
- Begynn å vurdere hvordan innebygd personvern kan ivaretas allerede her
- Etabler GDPR beslutningslogg (Hva som er vurdert, hva som er besluttet, når og av hvem)

HELSE SØR-ØST

* Dette er forklart lenger ned i presentasjonen

GDPR i de forskjellige prosjektfasene



Planleggingsfasen

- Avgjør om det valgte konseptet krever en personvernkonsekvensvurdering, dokumenter beslutningen og gjennomfør vurderingen ved behov
  - Ved høy risiko for personvern må man kontakte relevante personvernombud i virksomhetene, for å bli enige om videre fremdrift.
  - Ved middels eller lav risiko skal prosjekteier beslutte om risikoen er akseptabel uten tiltak, eller om tiltak skal iverksettes for å redusere risikoen

- Utarbeid egne eller bruk eksisterende relevante sjekklister for innebygd personvern (Se vedlegg)

- Oppdater GDPR beslutningslogg (hva som er vurdert, hva som er besluttet, når og av hvem)

HELSE SØR-ØST

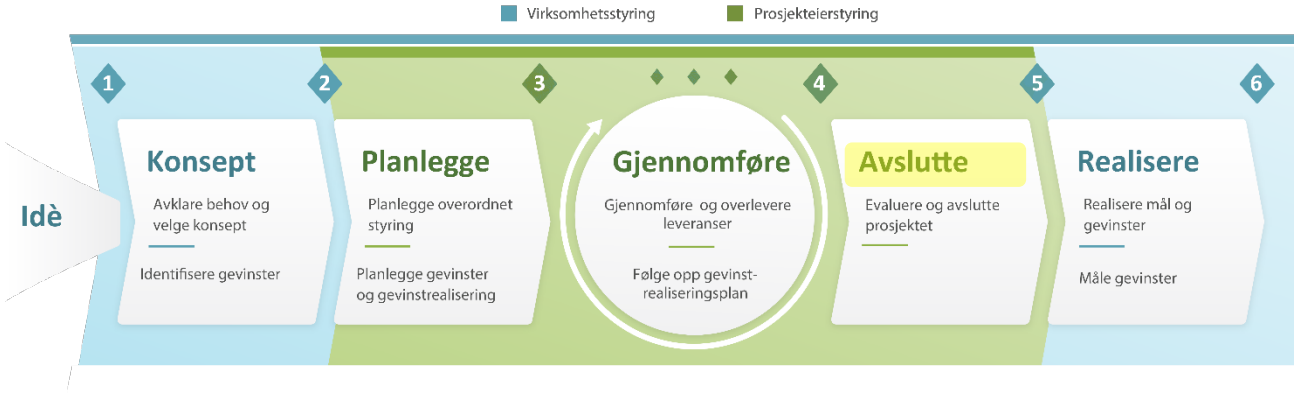
GDPR i de forskjellige prosjektfasene

Gjennomføringsfasen

- Personvernkonsekvensvurderingen holdes oppdatert
- Personvern bygges hele tiden inn i løsningen
- Sjekklister følges og fylles ut
- Nødvendige kontrakter inngås (for eksempel databehandleravtaler)
- Oppdater GDPR beslutningslogg (hva som er vurdert, hva som er besluttet, når og av hvem)

HELSE SØR-ØST

GDPR i de forskjellige prosjektfasene



Avslutningsfasen

- Dokumenter beslutningene i BP4 i GDPR beslutningslogg
- Arkiver personvernkonsekvensvurdering, innebygd personvern og GDPR beslutningslogg

HELSE SØR-ØST

GDPR skal være et tema i beslutningspunkter

BP 2

- Verifisere at behovene for personvern og informasjonssikkerhet er kartlagt
- Beslutte om konseptet krever en personvernkonsekvensvurdering

BP 3

- Beslutte hvilke innebygd personvern-tiltak som skal gjennomføres
- Beslutte om personvernkonsekvens-vurdering må gjennomføres
- Beslutt hvilke sjekklister for innebygd personvern som skal følges

BP 4

- Verifisere at personvernkonsekvens-vurderingen er oppdatert
- Verifisere at nødvendige kontrakter er inngått
- Verifisere at relevante sjekklister er fulgt og utfylt

BP 5

- Verifisere at arkivverdige dokumenter er arkivert

HELSE SØR-ØST

Personvernkonsekvensvurdering (DPIA)

- **Personvernkonsekvensvurdering –** En prosess for å hjelpe til å identifisere og håndtere risikoer knyttet til behandling av personopplysninger.

- Når skal det gjøres en personvernkonsekvensvurdering?
  - Det finnes flere forskjellige vilkår som kan hjelpe til å avgjøre når en personvernkonsekvensvurdering skal gjennomføres. Se vedlegg side 16.
  - Det viktigste vilkåret er at en behandling anses å medføre en høy risiko for rettighetene til de registrerte.

- Personvernkonsekvensvurdering skal påbegynnes helt i starten av prosjektet.
  - Selv om noen av behandlingsaktivitetene fortsatt er ukjente skal den uansett påbegynnes.
  - Personvernkonsekvensvurderingen er en kontinuerlig prosess og skal holdes oppdatert gjennom hele livssyklusen.

HELSE SØR-ØST

Innebygd Personvern

- **Alle nye systemer og løsninger skal ha personvern som en sentral, integrert del av seg.**
  - Dette betyr at personvern må være planlagt helt fra starten av, og en viktig del av alle faser i et prosjekt.

- **Systemer og løsninger skal ha personvernfremmende standardinnstillinger**
  - Dette gjelder blant annet mengden personopplysninger man samler inn, omfang av behandlingen, lagringstid og opplysningenes tilgjengelighet.

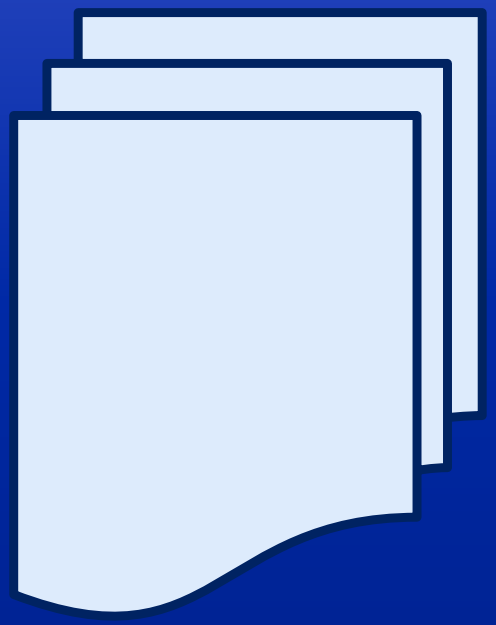
- **Datatilsynet har på sine nettsider en oversikt over syv punkter som bør være med for å oppnå tilfredsstillende innebygd personvern – Se vedlegg**

HELSE SØR-ØST

Dataminimering

- **Det skal ikke samles inn flere opplysninger enn det som er nødvendig for å gjennomføre behandling**
- **Opplysningene som samles inn skal kun brukes til sitt definerte formål**
  - Hvis opplysningene skal brukes på noe annet må det foreligge en hjemmel for dette, for eksempel den registrerte sitt samtykke

HELSE SØR-ØST



Vedlegg

HELSE SØR-ØST

Vilkår som sannsynliggjør behovet for en personvernkonsekvensvurdering

1. Evaluering eller profilering – særlig hvis det gjelder blant annet individets arbeidsprestasjoner eller helse
2. Automatiserte avgjørelser med rettslig bindende resultat
3. Systematisk overvåkning – opplysninger innhentet fra for eksempel nettverk eller overvåkning av offentlige områder
4. Sensitive eller andre svært personlige opplysninger
5. Behandling med stort omfang – enten stort omfang av berørte subjekter, datamengde, varighet eller geografisk utstrekning
6. Sammenstilling av flere datasett fra to eller flere kilder
7. Opplysninger om sårbare subjekter – barn, psykisk syke, og lignende.
8. Behandling ved hjelp av ny teknologi eller innovative løsninger
9. Når behandlingen i seg selv hindrer subjektene å påropе seg sine rettigheter eller benytte en tjeneste

Hvis to eller flere av disse vilkårene er oppfylt skal det gjennomføres en personvernkonsekvensvurdering

HELSE SØR-ØST

Punkter hentet og oversatt fra Artikkel 29 Working Party sin veileder – kan leses her

Overordnede punkter for innebygd personvern

1. Vær i forkant – forebygg fremover å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

HELSE SØR-ØST

Les mer utdypende her

Sjekklister for innebygd personvern i forbindelse med systemutvikling

1. Opplæring
2. Kravsetting
3. Design
4. Koding
5. Test
6. Produksjonssetting
7. Forvaltning

HELSE SØR-ØST

Mer informasjon

Faglig kontaktpunkt

personvern@sykehuspartner.no

HELSE SØR-ØST

HELSE SØR-ØST

Nyhetsbrev og sosiale medier: www.helse-sorost.no/sosialemedier