Nye personvernregler i 2018 - GDPR i helsesektoren

Veronica Jarnskjold Buer, senioringeniør

05.12.2017

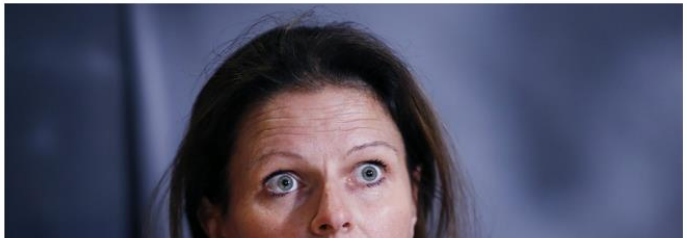
Datatilsynet

Innrømmer mangel på oversikt over IKT-sikkerhet i Helse Sør-Øst

Helseminister Bent Høie (H) innrømmer at man ikke har overs
som har tilganger til norske pasientjournaler, eller hvilke land
det haster å få svar på hvem som har tilgang til sensitive pasi

– Jeg har vært forbannet og fortvilet

HAMAR (NRK): Toppsjef Cathrine Lofthus har vært forbannet over at sjefer og ansatte har skjult informasjon om dårlig IT-sikkerhet og manglende personvern i Helse Sør-Øst



Anne Cecilie Remen
Journalist

Line Tomter
Journalist

Fortsatt ingen avklaring om IT og pasientdata i Helse Sør-Øst

t seg for hvordan de skal løse IT-problemene. I
oretaket store ekstrautgifter. Milliardprosjektet er
et skrotes.

Anne Cecilie Rem
Journalist

Line Tomter
Journalist

Oppdatert 14.09.20
07:46

Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT

Flere lover ble brutt og det ble gjort mangelfulle vurderinger av sikkerhet og risiko før Helse Sør-Øst vedtok å outsource IT-infrastrukturen. Det slår Datatilsynet fast i en ny rapport.

kritisk informasjon om IKT-sikkerheten, og om hvordan IT-ansatte hadde full tilgang til sensitive pasientjournaler, i strid med regelverk og avtaler.

FOTO: ESPEN ANDERSEN / NRK

› NRK har satt opp en egen

Datatilsynet

Kort om skytjenester

- Er det egentlig noe nytt?
  - ASP, fjerndrift, stormaskin, hosting, …
- Outsourcing rokker ikke ved ansvarslinjene:
  - Virksomhet versus Leverandør
  - Behandlingsansvarlig versus databehandler
- Behandlingsansvarlig har plikter overfor de registrerte, databehandleren og Datatilsynet.
- Databehandler har plikter overfor behandlingsansvarlige regulert i databehandleravtale (dagens regelverk)og Datatilsynet.
- **Skytjenester betyr ikke fravær av kontroll og ikke bortsetting av ansvar (i så fall er det uforenlig med regelverket)**

Behandlingsansvarlig må gjøre risikovurdering forut for outsoucing

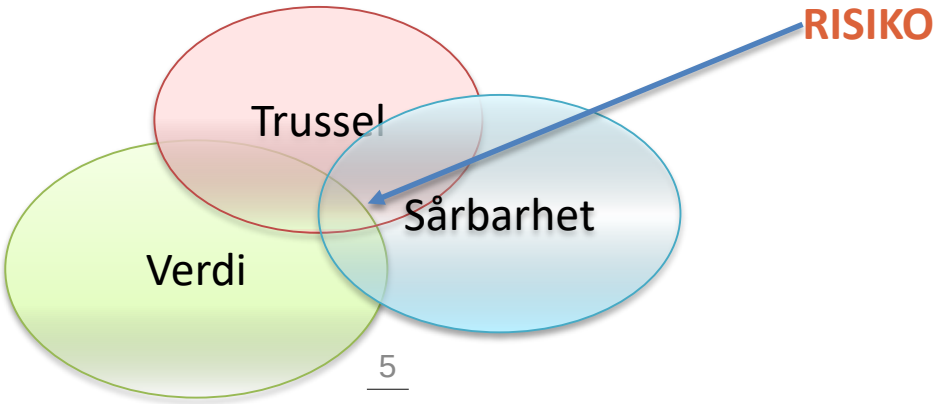
Hva setter du ut?

- Du må vurdere hvilke verdier som skal settes ut, og på hvilket nivå.
  - verdivurdering
- Personopplysninger har høy omsetting
  - Jo mer du vet om en person desto høyere utbytte
  - Cyberkrim og svindelsaker – høyest ranking
  - Personopplysninger er inngangsport for all nettkriminalitet

Datatilsynet

Risikovurdering

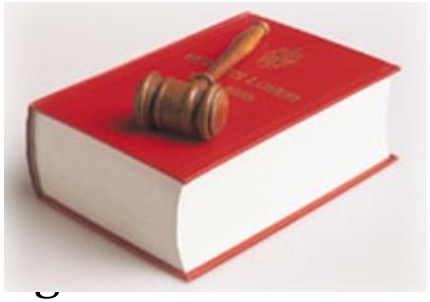
- Hvem er mine trusselaktører/hva er mine trusler?
- Hvor sårbar er min virksomhet mot de trusler eller trusselaktører som truer mine verdier?
- Tre innganger:
  - Cyber gate – epost, ddos, ..
  - Human gate – sosial manipulering, …
  - Fysical gate – låste dører, vakter, …
- Sårbarhet er skalerbart
- Risikovurdering er hvor sårbar er dine verdier for gitte trusler



Risikovurdering skal håndteres av behandlingsansvarlige (dvs ledelsen)

- Når en utkontrakterer IKT-tjenester ut av Norge *bør* følgende tema om landet det utkontrakteres til inngå i risikoanalysen:
  - Finansiell stabilitet
  - Politisk stabilitet
  - Levestandard
  - Teknisk infrastruktur
  - Tilgang på kompetanse - utdanningssystem
  - Reguleringer – lover – regler – politi - rettsvesen
  - Relevante hendelser i landet

Viktige lovkrav ved bruk av skytjenester



- Internkontroll
  - pol § 14 og pof kapittel 3
- Informasjonssikkerhet
  - pol § 13 og pof kapittel 2 (herunder risikovurdering og sikkerhetsledelse)
- Databehandlere
  - pol §§ 15 og 13
  - pof § 2-15 og hele kapittel 2
- Andre relevante krav
  - pol § 11 b) «uttrykkelig angitt formål»
  - pol §§ 29, 30 - overføring til utlandet
- Vurdering av personvernkonsekvenser (utredningsinstruksen, ansvarlig DFØ)

pol = personopplysningsloven | pof = personopplysningsforskriften

Etter PVF

- Innebygd personvern og informasjonssikkerhet (art 25)
- Vurdering av personvernkonsekvenser (art 35)
- Risikoanalyse (32)
- Internkontroll (30)
- Informasjonssikkerhet (32)
- Databehandleravtale (art 24)
- Revidering av databehandlere (art 24)
- Formål, oversikt, virkemiddel (art 24)

- Åpner for personopplysninger på tvers innen EU/EØS
  - Tilsvarer ikke at du kan bruke hvem som helst utenfor Norge, på lik linje med at du ikke kan benytte hvem som helst i Norge.

Ledelsesansvar – Behandlingsansvarliges plikt

- Ledelsen/behandlingsansvarlig skal fremlegges risikovurderingen (og vurdering av personvernkonsekvenser)
- Disse skal sees opp i mot ledelsens besluttede risikoapetitt/risikotoleranse
  - Merk at personvernprinsipper og den registrertes rettigheter kan ha nulltoleranse (dvs ledelsen kan ikke endre den)
- Ledelsen skal gjøre en beslutning om utsetting på grunnlag av disse vurderingene.
- Der vurdering av personvernkonsekvenser er fremdeles høy for den registrerte skal det foreligge en drøftelse med DT (dette punktet er etter pvf)

Personvernprinsipper og den registrertes rettigheter

Personopplysninger – hva er det? (art 4)

- enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»);
- en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks.
  - et navn,
  - et identifikasjonsnummer,
  - lokaliseringsopplysninger,
  - en online-identifikator eller
  - ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet

Hva er person(opplysnings)vern?

”**Den enkeltes rett til å ha kontroll med egne personopplysninger**”

Selvbestemmelse – rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem, til hvilke formål.

Informasjon – hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som brukes, av hvem og til hvilke formål

Hva er person(opplysnings)vern?

”**Den enkeltes rett til å ha kontroll med egne personopplysninger**”

Selvbestemmelse – rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem, til hvilke formål.

Informasjon – hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som brukes, av hvem og til hvilke formål

Person(opplysnings)vern er mer enn informasjonssikkerhet – du må sikre at personvernprinsipper og den registrertes rettigheter ivaretas.

Hvem har plikter og rettigheter

- De **registrerte** har **rettigheter**
- Behandlingsansvarlig, databehandler, underleverandører har **plikter**

Gamle personvernprinsipper i ny drakt art 5

Lovlig, rimelig og gjennomsiktig
Rettslig grunnlag. Respekter de registrertes interesser og rimelige forventninger. Informasjon skal gis på en tilgjengelig og forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til spesifikke, uttrykkelig angitte og legitime formål. Opplysningene skal ikke brukes til andre uforenlige formål

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig for formålet.

Korrekte og oppdaterte
Opplysningene skal være korrekte og om nødvendig ajourførte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Rutiner for lagring og sletting
Personopplysninger skal ikke lagres lengre enn det som er nødvendig for formålet. Automatiske sletterutiner.

Integritet og konfidensialitet
Personopplysninger sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, ødeleggelse eller skade. Det skal brukes egnede tekniske og organisatoriske tiltak.

Ansvarlighet
Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, at regelverket blir etterlevd

De registrertes rettigheter

- **Informasjon (art 12-14)**
  - Hvordan og hvorfor
- **Innsyn (art 15)**
  - Beholde kontroll over egne opplysninger

Forutsetning for de resterende rettigheter

- **Korrigering (art 16 & 19)**
  - Unøyaktige opplysninger, Varsling av tredje part
- **Sletting/Retten til å bli glemt (art 17 & 19)**
  - Ikke nødvendige opplysninger, samtykket trekkes tilbake, registrerte motsetter seg, ulovlig behandling, lovhjemmel
- **Rett til at personopplysninger begrenses (ny, art 18 &19)**
  - den registrerte ønsker at opplysninger skal slettes eller bestrider at opplysningene er korrekte

De registrertes rettigheter

- **Dataportabilitet (ny, art 20)**
  - Den registrerte kan ha krav på å ta med seg opplysningene sine til en annen virksomhet dersom behandling er basert på samtykke eller avtale
- **Innsigelse (ny, art 21)**
  - rett til å protestere på visse typer behandlinger
- **Automatiserte avgjørelser, inkludert profilering (ny, art 22)**
  - Avgjørelser basert på algoritmer, er snevret inn etter de nye reglene. Eks. benytter algoritmer for å utarbeide profiler om et individ som igjen avgjør kredittverdighet, adgang til å ta opp lån, forsikringspremier, og så videre.

PVF

Nøkkelen til etterlevelse (*accountability*)

Artikkel 5 (2) 'Ansvarlighet'
Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes.

- Mindre forhåndskontroll – bortfall av melde- og konsesjonsplikt
- Flere (og til dels tydeligere) rettigheter og plikter
- Risikobaserte tiltak (DPIA, forhåndsdrøftelse, etterkontroll)
- Strengere sanksjoner

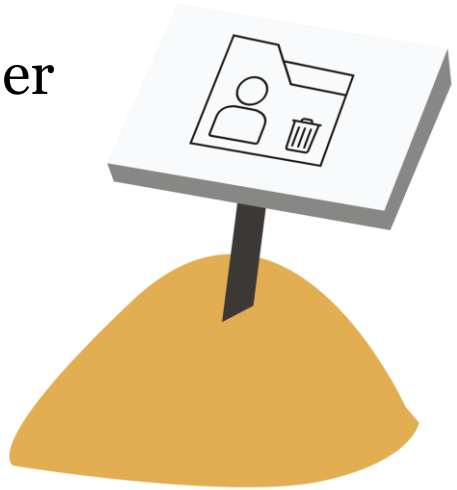

Source: LinkedIn

Alle skal gi god informasjon om hvordan de behandler personopplysninger

- Informasjonen skal være lett tilgjengelig
- Klart språk som er tilpasset leserens nivå
- Stilles krav til hvilke opplysninger som skal gis

Alle må kunne oppfylle borgernes nye rettigheter

- Retten til å bli glemt
- Rett til at personopplysninger begrenses
- Systemer må oppfylle krav til dataportabiliet
- Strengere regler for automatiserte avgjørelser
- Håndtere henvendelser fra borgere innen 1 måned



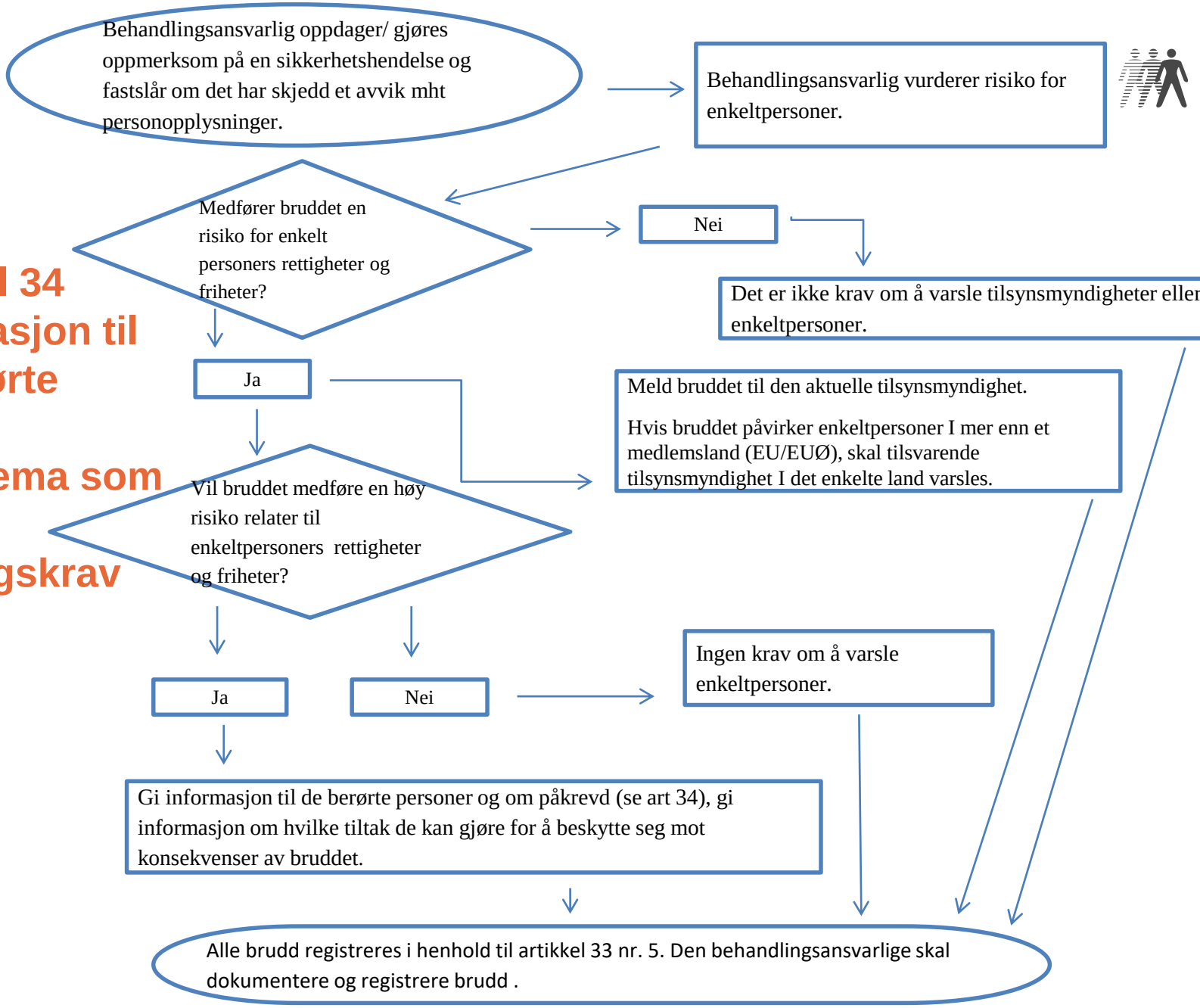
Avviksmeldinger – art. 33

- Behandlingsansvarlig må melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
- Stilles krav til innholdet i avviksmeldingen. Vårt skjema i Altinn tar høyde for dette.

- WP29 gruppens veiledning for avviksmeldinger ble godkjent i oktober Kink på våre sider.

Artikkel 34 Informasjon til de berørte

Flytskjema som viser varslingskrav

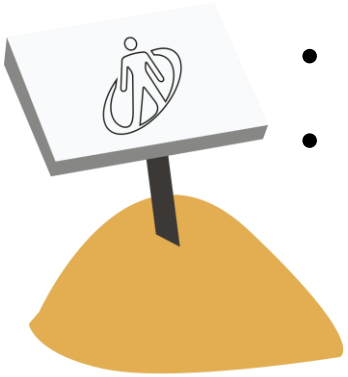


Alle databehandlere får nye plikter

- Egne rutiner for behandling av personopplysninger
- Si fra om instrukser er i strid med loven
- Underleverandører skal godkjennes
- Melde avvik til behandlingsansvarlig
- Kan bli erstatningspliktige

Mange virksomheter må opprette personvernombud

- Alle offentlige virksomheter (unntatt domstoler)
- Virksomheter som har som kjerneaktivitet å gjøre følgende i stor skala:
  - regelmessig og systematisk overvåke personer
  - behandle sensitive personopplysninger eller opplysninger om straffbare forhold
- Krav til kompetanse
- Skal involveres og rapportere til høyeste ledelsesnivå
- Ombudet skal ikke instrueres eller straffes
- Oppgavene omfatter å gi råd, overvåke etterlevelse og være kontaktpunkt

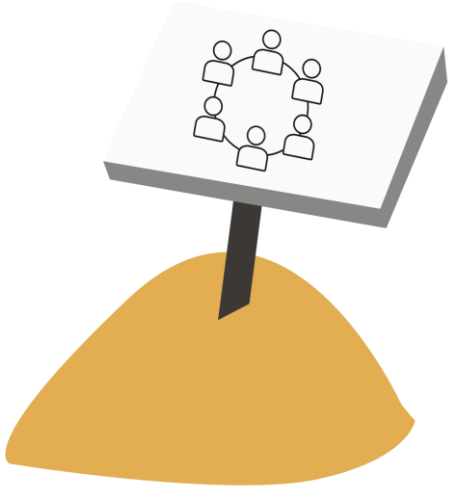


Reglene gjelder også virksomheter utenfor Europa

- Alle som tilbyr varer eller tjenester til EU- eller EØS-borgere
- De som kartlegger EU- eller EØS-borgeres adferd på nett
- Virksomheter skal kunne forholde seg til en personvernmyndighet
- Den registrerte skal kunne klage i eget land
- Personvernmyndigheter skal samarbeide

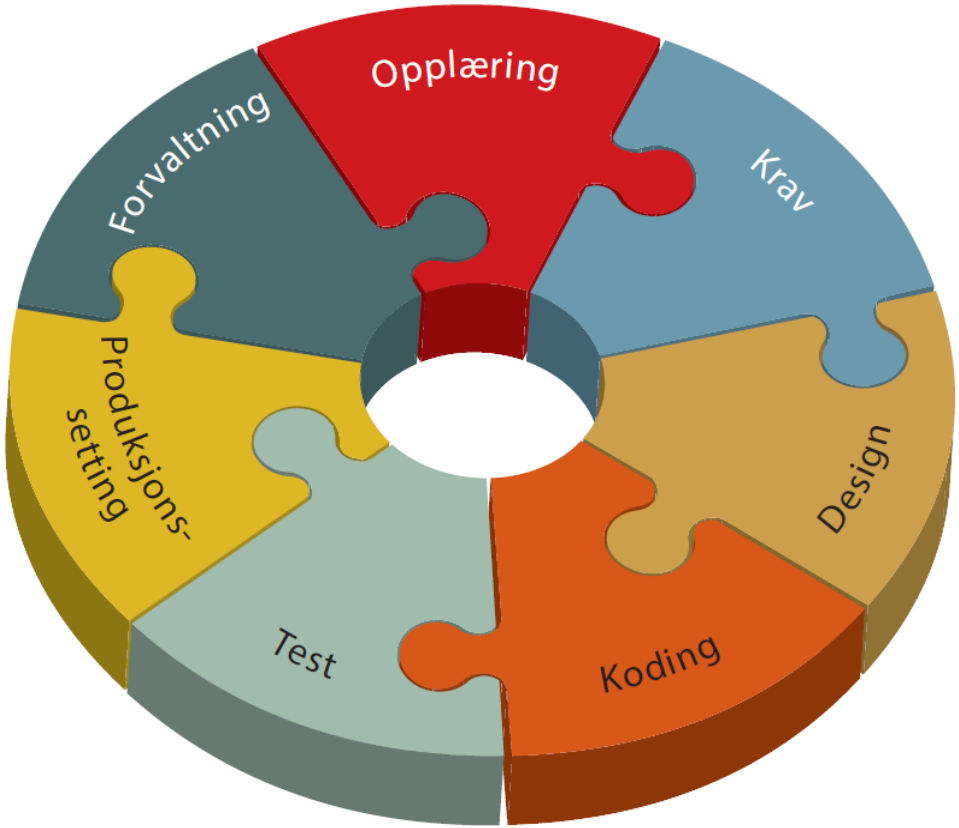
Alle bør samarbeide i egne nettverk og følge atferdsnormer

- Sektorvis utforming av retningslinjer
- Sikrer at de viktigste rutinene er på plass
- Flere fordeler ved å følge disse
- Datatilsynet skal godkjenne atferdsnormer



Programvareutvikling med innebygd personvern og personvern som standardinnstilling

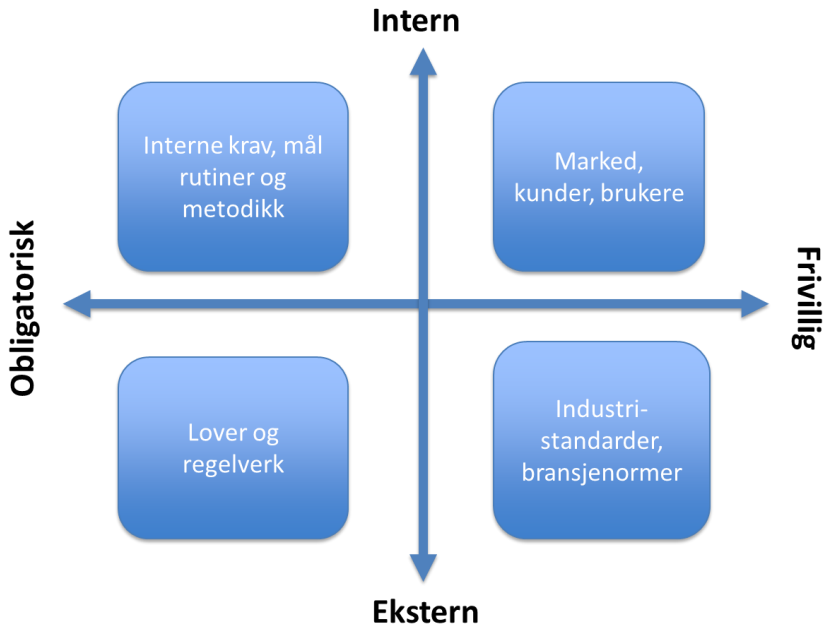
Innebygd personvern og personvern som standardinnstilling



Oppsummert:

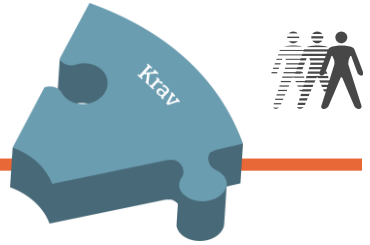
- Obligatorisk
- Tekniske og organisatoriske tiltak.
- Ivareta **personvernprinsipper** og den **registrertes rettigheter**.
- Det minst personverninngripende alternativet som standard, mht mengde, omfang, lagringstid, tilgjengelighet.
- Ha et rammeverk for programvareutvikling, og inkluder disse sju aktivitetene er i rammeverket.
- **Behandlingsansvarlige**: Krav til å benytte programvare, løsninger etc som har innebygd personvern som standardinnstilling.

Opplæring



- **Mål:** Basiskunnskap og forståelse for personvern og informasjonssikkerhet, og risiko tilknyttet dette
- **Hva skal det gis opplæring i:** Når og hvorfor personvern og informasjonssikkerhet er viktig i de ansattes daglige arbeidsoppgaver.
- **Suksesskriterier** er at virksomheten har etablert retningslinjer for personvern og informasjonssikkerhet, og at intern opplæring i disse retningslinjene er adressert.

Kravsetting

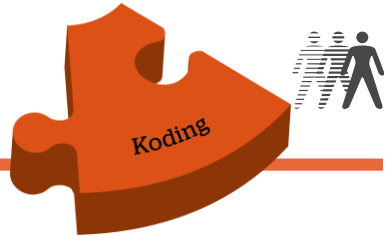


- **Sett personvern- og sikkerhetskrav**
  - Type opplysninger, hvem er eier, hvem er behandlingsansvarlig, databehandler, mottaker
  - Prinsipper skal være oppfylt og rettigheter ivaretatt
    - Nødvendig? Mengde, omfang, lagringstid, tilgjengelighet
    - Åpenhet – gi informasjon så den registrerte kan ivareta sine rettigheter
  - Informasjonssikkerhet
- **Sett toleransenivå for risiko knyttet til personvern og informasjonssikkerhet**
- **Gjennomfør vurdering av personvernkonsekvenser**
- **Gjør risikovurdering** (verdi, trussel, sårbarhet)

Design

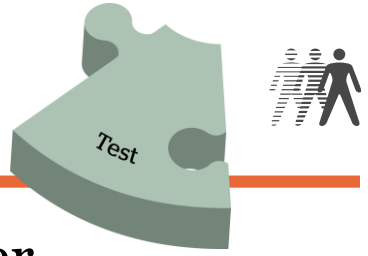
- **Dataorienterte designkrav:**
  - Minimer og begrens *«Select before you collect»,* «Gjem og skjul», Separer, Aggreger, Personvern som standard
- **Prosessorienterte designkrav:**
  - Informer, Kontroller, Håndheve, Demonstrer
- **Analyser angrepsflaten**
  - i den designede programvaren for å **redusere** muligheter til å utnytte svake punkter og sårbarheter.
- Ved **trusselmodellering**
  - analyserer man komponenter, tilgangspunkter, dataflyt og prosessflyt i programvaren.
  - hvordan noen kan misbruke programvaren ved ulike scenarioer.
  - hvordan designet kan forbedres for å unngå trusler som er identifisert.
  - Resultat er et mer herdet og robust sluttprodukt.

Koding



- **Bruk godkjente verktøy og rammer**
  - Beskriv bruksområde, sikkerhetsfunksjonalitet, omfatter Støttekomponenter og verktøy fra tredjeparter, Verktøy må risikovurderes og analyseres for sårbarheter
- **Ugyldiggjør utrygge funksjoner og moduler**
  - Analyser funksjoner, API, tredjepartsbibliotek og moduler,Forby de som er utrygge, oppdater de som er utdaterte eller inneholder kjente sårbarheter, Bruk verktøy for kodeskanning for å sjekke koden, Deaktiver unødig sporing, logging og innsamling av personopplysninger
- **Statisk kodeanalyse og kodegjennomgang**
  - Automatiske verktøy, Manuell gjennomgang for å fange opp svakheter som kan medføre feil bruk eller lekkasje av personopplysninger, Regelmessig gjennomgang

Test



- **Test om personvern og sikkerhetskravene** er implementert og riktig implementert?
  - Er alle komponenter med?
- **Sikkerhetstesting**
  - Dynamisk testing: Test funksjonalitet i kjørende kode, brukerrettigheter og kritiske sikkerhetsfeil
  - Fuzz testing: Fremprovoser feil i programvaren, misformet data inn i programvaren, Test alle grensesnitt
  - Penetrasjonstesting/ sårbarhetsanalyse: Kjøres før produksjonssetting og jevnlig,
  - Lovlig og autorisert forsøk på å finne, utnytte og avdekke sårbarheter
- **Gjennomgang av trusselmodell og angrepsflate**
  - Verifisere at angrepsvektorer som ble avdekket i designfasen er håndtert, at nye ikke er introdusert og ikke håndtert, Ny gjennomgang av trusselmodell og vurderingen av personvernkonsekvenser

Produksjonssetting

- **Utarbeid plan for hendelseshåndtering** for effektivt håndtere oppgaver og hendelser som kan oppstå etter produksjonssetting.
  - Hva er en hendelse, hvilken livssyklus den har (omfatter å detektere, analysere, rapportere, håndtere og normalisere), ressurser, kontaktpunkt/responssenter, kontaktinformasjon, responstid, kanaler, logger, rutiner, patching, evaluering, varsle ledelsen, den registrerte og Datatilsynet.
- **Full sikkerhetsgjennomgang av programvaren** skal baseres på tidligere gjennomganger i utviklingsløpet og inngå i de kontrollpunkter (control gates) som må gjøres før produksjonssetting.

- **Godkjenning av produksjonssetting**
  - Sikkerhetsrådgiver og personvernombud verifiserer at definerte sikkerhets- og personvernkrav er implementert og fungerer etter hensikten.
  - Virksomheten må definere hvem som har godkjenningsmyndighet.

- **Arkivering** bør gjøres av all relevant data og dokumentasjon fra hele utviklingsløpet.

Forvaltning

- **Håndtere hendelser og avvik etter planen**
  - Når akutte hendelser opptrer, er det viktig å bevare roen og å bruke tid på å analysere hendelsen.
  - Responsteamet skal vite hvem de skal kontakte når og hvem som er i stand til å bygge, teste og installere oppdateringer.
  - Responsteamet må vite hvilke prioriteringer som gjelder, samt vite nøyaktig hva de kan og skal gjøre når det virkelig er krise.
  - Øv
- **Forvaltning, drift og vedlikehold av programvaren skal følge etablerte rutiner for hvordan personvern og sikkerhet skal ivaretas over tid.**
  - Styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold.
    - Rutiner for regelmessige testing og revidering, sikkerhetsovervåkning, målinger, forbedring mm.

Vurdering av personvernkonsekvenser (DPIA) og forhåndsdrøftelse

Vurdering av personvernkonsekvenser – art. 35

Det er flere typetilfeller der det er nødvendig å utrede personvernkonsekvenser:

- systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
- behandling av sensitive personopplysninger i stort omfang
- systematisk overvåking av offentlig område i stort omfang

I tilfelle man er i tvil anbefaler vi å utføre en DPIA.

Datatilsynet **må** publisere liste over når det er påkrevd.

Datatilsynet *kan* publisere liste over når det ikke er påkrevd.

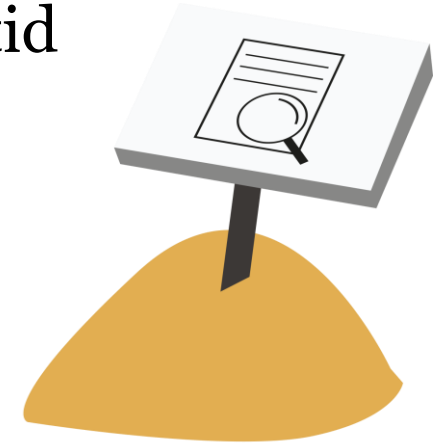
Vurdering av personvernkonsekvenser – art. 35

Vurderingen skal som minimum inneholde:

- Systematisk beskrivelse av behandlingen, formål, og evt. hvilken berettiget interesse den ivaretar.
- Vurdering av nødvendighet og forholdsmessighet, sett opp mot formålet.
- Vurdering av risikoen for rettigheter og frihet til registrerte.
- Tiltak som skal iverksettes for å redusere risikoen.

Forhåndsdrøftelser – Art. 36

- Ved høy risiko, som ikke kan begrenses, skal vi involveres i forhåndsdrøftelser
- Det stilles krav til dokumentasjon som skal sendes inn til oss
- Forordningen stiller krav til vår behandlingstid
- Datatilsynet kan veilede eller forby behandlingen



Takk for meg!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

veronica@datatilsynet.no | Twitter: @veronica_buer