Digital sårbarhet – Informasjonssikkerhet og personvern

Veronica Jarnskjold Buer

Fagdirektør Digitalisering og innebygd personvern

10.02.2021

Datatilsynet

Agenda

- Datatilsynet som ombud og tilsynsmyndighet
  - vår rolle i veiledningsarbeid innen informasjonssikkerhet
  - vår rolle med tilsyn innen informasjonssikkerhet
- Brudd på personopplysningssikkerheten

Datatilsynet skal

- føre kontroll med at personvernregelverket etterleves, og at feil og mangler ved *behandling av personopplysninger* blir rettet. Dette gjøres blant annet gjennom tilsyn og saksbehandling
- holde oss orientert om nasjonal og internasjonal utvikling når det gjelder behandling av personopplysninger
- identifisere farer for personvernet, og gi råd for hvordan farene kan unngås eller begrenses.
- være høringsinstans i saker som berører personvern
- delta i råd og utvalg
- bistå bransjeorganisasjoner med å gi råd og utarbeide atferdsnormer for å sikre personopplysninger i virksomhetene
- stimulere til opprettelse av *personvernombud* og bygge kompetanse hos ombudene
- ha en ombudsrolle overfor publikum, og gi råd og informasjon. Dette gjøres blant annet ved hjelp av våre nettsider, blogg og veiledere, veiledningstelefon, foredrag, veiledningsmøter.
- få viktige saker på dagsorden i media og bidra til samfunnsdebatt om personvern

Datatilsynets tilsynsvirksomhet relatert til informasjonssikkerhet

Personopplysningssikkerhet omfatter …

- Ansvarlighet (art 5(2)) og styringssystem for personvern og informasjonssikkerhet (art. 24 og 30)
- Informasjonssikkerhet (artikkel 32)
- Brudd på personopplysningssikkerhet (art. 33 og 34)
  - Avviksmelding
  - Informasjon til den registrerte
- Innebygd personvern (art.33 og 34)
- DPIA (art. 35)

Ansvarlighetsprinsippet (art. 5(2))

Nøkkelen er ansvarlighet
Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes.

- Ikke forhåndskontroll – melde- og konsesjonsplikt er «2017/2018»
- Flere og tydeligere rettigheter og plikter
- Risikobaserte tilnærming (informasjonssikkerhet, tiltak, DPbDD, DPIA)
- Forhåndsdrøftelse
- Revisjoner og egenkontroll
- Strengere sanksjoner

Source: LinkedIn

Ansvar en del av styringssystemet i virksomheten – art 24

Styringssystem for personvern og informasjonssikkerhet skal inneholde føringer for hvordan virksomheten skal utøve sine arbeidsoppgaver relatert til dette. Dersom virksomheten har et kvalitetsstyringssystem (for eksempel basert på ISO9001) forventer vi å finne føringer for personvern og informasjonssikkerhet her.

Stikkord er

- **Forholdsmessighet**
- **Risikovurdering** for rettigheter og friheter basert på Art, omfang, formål og sammenheng
- **Egnede, planlagte og systematiske tiltak** (tekniske og organisatoriske)
- Etablere og ta i bruk **nødvendige retningslinjer** for vern av personopplysninger
- **Kontinuerlig** prosess
- Sikre og **dokumentere (garantier for)** etterlevelse

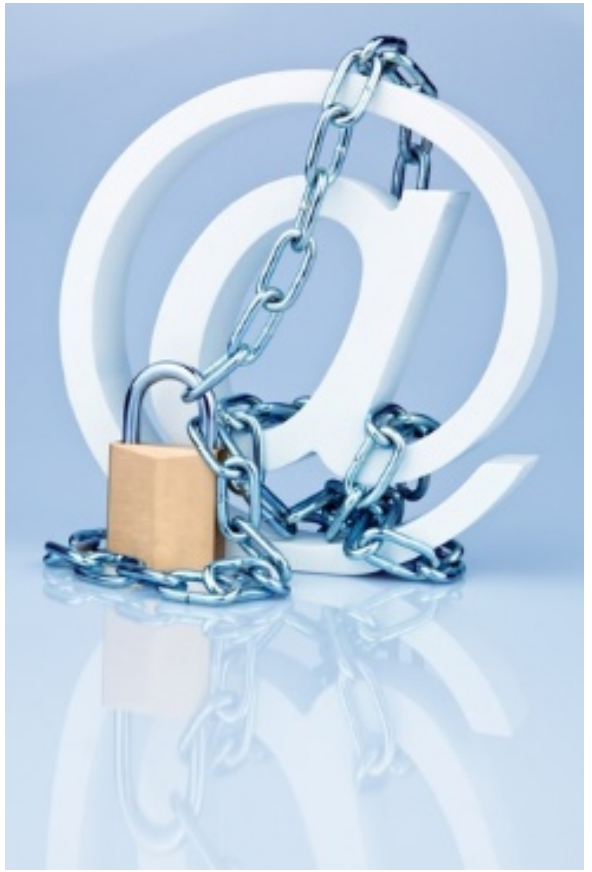
Protokoll over behandlingsaktiviteter – art. 30

- Kontaktinformasjon til behandlingsansvarlig
- Formål
- Kategorier av registrerte og personopplysninger
- Kategorier av mottakere
- Evt. overføringer til tredjeland eller internasjonale organisasjoner, og dokumentasjon på tilstrekkelig beskyttelse
- Slettefrister
- Sikkerhetstiltak

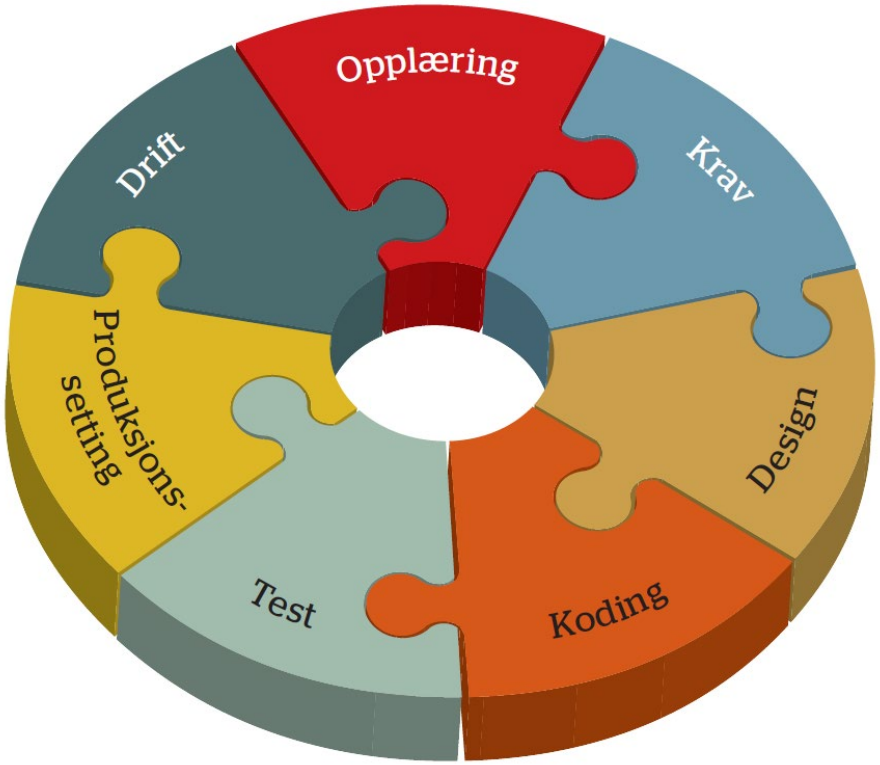
Databehandlere skal ha tilsvarende oversikt over det de gjør på vegne av ulike behandlingsansvarlige

Sikkerhet ved behandling – art. 32

- Risikobasert tilnærming
  - Bruk gjerne anerkjente sikkerhetsstandarder til hjelp
  - Teknisk utvikling og gjennomføringskostnader
  - Art, omfang, formål og sammenheng
  - Risiko for rettigheter og friheter
- Sikkerhetstiltak
  - Pseudonymisering og kryptering av personopplysninger
  - Sikre vedvarende K, I, T og **robusthet**
  - Gjenoppretting av tilgjengelighet og tilganger ved hendelser
  - Jevnlig testing, vurdering og evaluering
- Bransjenormer eller godkjent sertifiseringsordning
  - Element for å vise etterlevelse
- Tiltak for å sørge for at behandling kun skjer på instruks fra behandlingsansvarlig

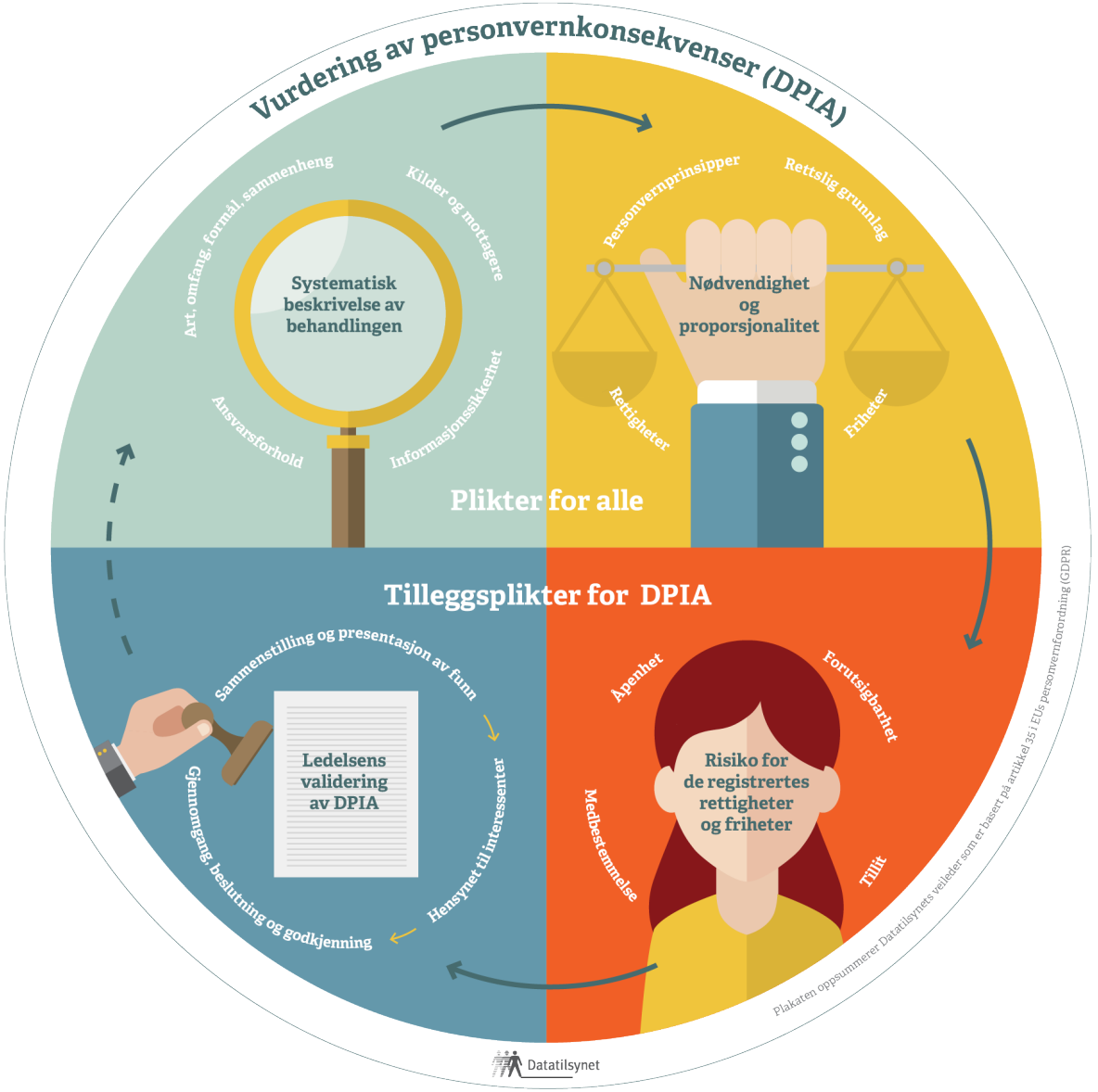


Veileder for programvareutvikling med innebygd personvern



- Obligatorisk
- Tekniske og organisatoriske tiltak.
- Ivareta **personvernprinsipper** og den **registrertes rettigheter og friheter**.
- 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 og personvern som standardinnstilling.

DPIA – en tilleggsplikt for særskilt inngripende behandlinger



Artikkel 33 & 34
…..om brudd på personopplysningssikkerheten

Hva er et brudd personopplysningssikkerheten (Art. 4(12)):

- *…. et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet*

- *Konfidensialitet-, integritet og tilgjengelighetsbrudd i personopplysninger*

Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten (Art. 33)

- Der bruddet på personopplysningssikkerheten sannsynligvis vil medføre en risiko for fysiske personers rettigheter og friheter må behandlingsansvarlig melde avvik innen 72 timer til Datatilsynet. Kan meldes trinnvis.

- Stilles krav til innholdet i avviksmeldingen.

- Databehandler melder til behandlingsansvarlig

- Samarbeid med øvrige tilsyn i EU relatert til sikkerhetsbrudd «på tvers av landegrenser» - one-stop-shop

Underretning av den registrerte om brudd på personopplysningssikkerheten (Art. 34)

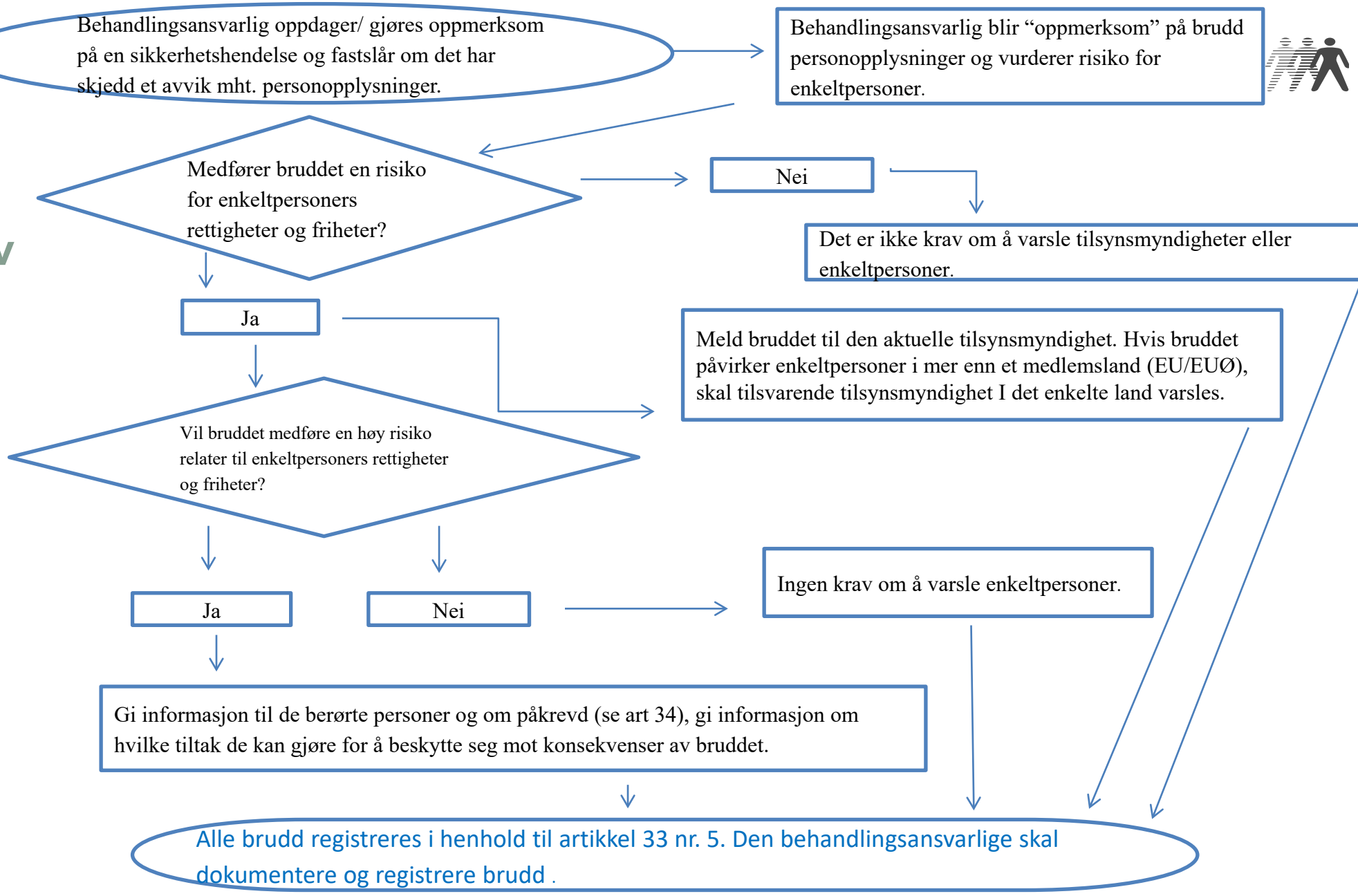
- Der bruddet på personopplysningssikkerheten sannsynligvis vil medføre en ***høy*** risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige **uten ugrunnet opphold** underrette den registrerte om bruddet.
- Krav til hvilken type informasjon som skal gis til den registrerte – hva har skjedd, hvilke tiltak har behandlingsansvarlig tatt, hva er det viktig at den registrertes foretar seg mm.
- Den registrerte skal kunne ta sine forhåndsregler

Vurdere virksomhetens brudd på informasjonssikkerhet (76)

- Risikoen bør vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko.

- Hvor sannsynlig og alvorlig risikoen for den registrertes rettigheter og friheter er, bør fastslås ut fra behandlingens art, omfang, formål og sammenhengen den utføres i.

Håndtering av brudd på person-opplysnings-sikkerheten



Konkurranse – Innebygd personvern i praksis 2020

Datatilsynet inviterer til ny konkurranse om beste programvare utviklet utfra prinsippene for innebygd personvern. Send oss programvare, tjenester, apper eller andre løsninger dere har utviklet eller holder på å utvikle som viser innebygd personvern i praksis.

I år har vi egen studentkategori, der premien er et stipend på 20 000 kr.

Hvordan delta i konkurransen?
Fyll inn søknadsskjema på nettsidene våre og send oss en nærmere beskrivelse av produktet. Les mer på datatilsynet.no

Frist for å sende inn bidrag 1. desember 2020
Vinnerne vil lanseres februar/mars 2021.

Jury:
Dag Wiese Schartum, Lillian Røstad, Maria Bartnes, Torgeir Waterhouse, Martha Eike, Veronica J. Buer

Takk for oppmerksomheten!

Datatilsynet

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

datatilsynet.no
personvernbloggen.no

@datatilsynet (Twitter)
@veronica_buer