GDPR og informasjonssikkerhet

Sikkerhetssymposiet 2019

Jan Sandtrø

Oversikt

- Informasjonssikkerhet
- Hva kreves etter personvernforordningen (GDPR)?
- Hvilken veiledning gir Datatilsynet?
- Hva kreves *egentlig*?
- Hvordan forholde seg til kravene (på en praktisk måte)?

§

Plikt for behandlingsansvarlig og databehandler

Artikkel 24. Den behandlingsansvarliges ansvar

Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

Artikkel 28. Databehandler

Dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.

+ Artikkel 32. Sikkerhet ved behandlingen

Kravene til informasjonssikkerhet i GDPR

Artikkel 32: Behandlingsansvarlig og databehandler skal …

*«… gjennomføre **egnede tekniske** og **organisatoriske tiltak** for å **sikre** og **påvise** at behandlingen utføres **i samsvar med denne forordning**.»*

- Tekniske og organisatoriske tiltak
- Egnede tiltak (egnet sikkerhetsnivå)
- Sikre
  - Sikre konfidensialitet, tilgjengelighet og integritet
  - Sikre etterlevelse
- Påvise = Dokumentasjon

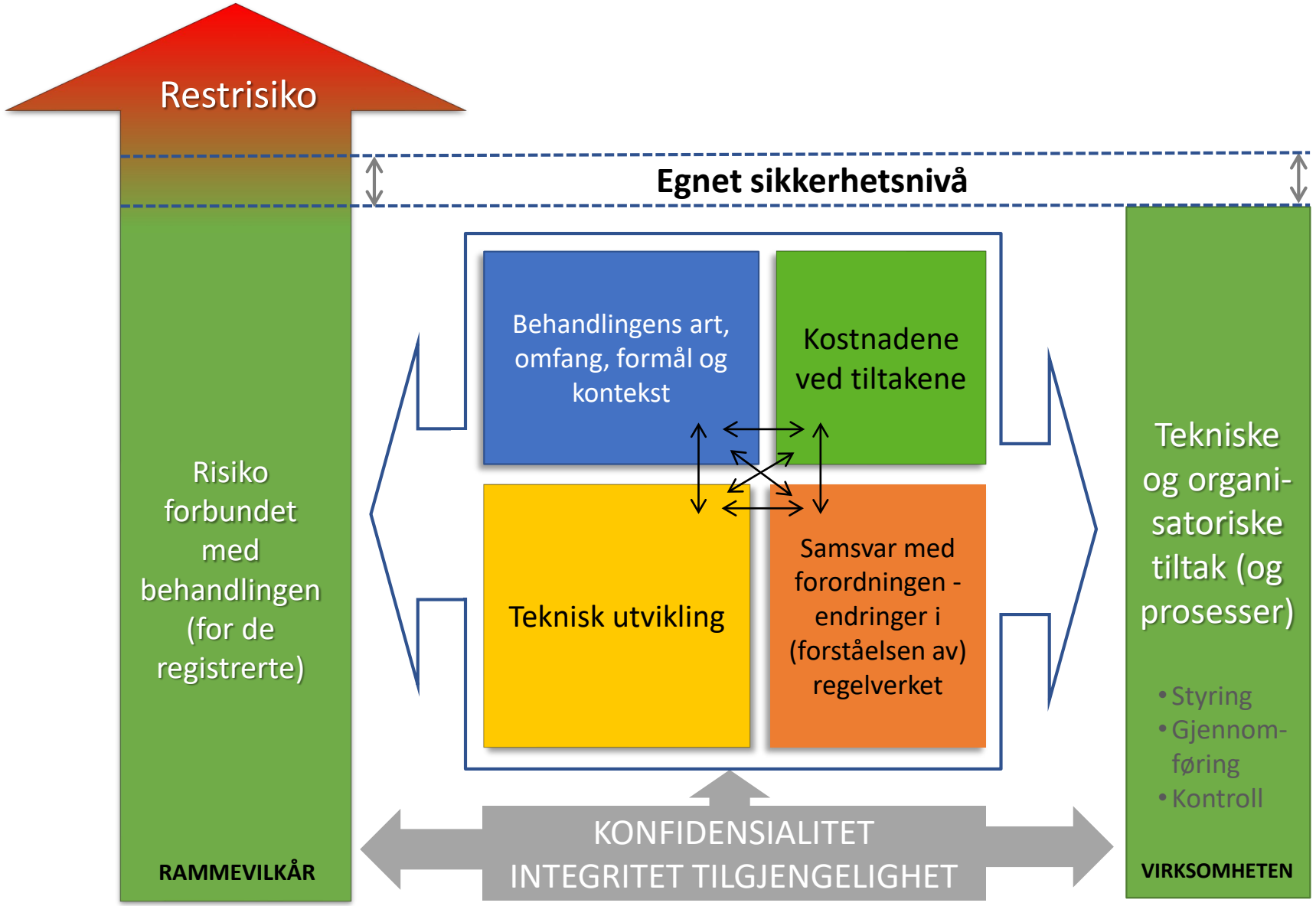
Egnet sikkerhetsnivå

- Vurderingen av «egnet sikkerhetsnivå» - vurderingstema (artikkel 32 nr. 1):
  - behandlingens art, omfang, formål og sammenhengen den utføres i
  - risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.
- Skal særlig tas hensyn til (artikkel 32 nr. 2):
  - Risikoene forbundet med behandlingen,
  - særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av (INTEGRITET) eller
  - tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet (KONFIDENSIALITET).
- Andre faktorer:
  - Godkjente atferdsnormer (artikkel 40)
  - Godkjent sertifiseringsmekanisme (artikkel 42)
- Hva er «riktig» nivå?
  - ISO 27001/27002, ISO 27701, ISAE 3000NIS-direktivet, hva «alle» gjør?
  - Riktig i «bakspeilet»?

Tekniske og organisatoriske tiltak

- Relative krav (forholdsmessighet) - ta hensyn til:
  - den tekniske utviklingen («the state of the art»)
  - gjennomføringskostnadene
  - behandlingens art, omfang, formål og sammenhengen den utføres i
  - risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.
- Eksemplifisering i bestemmelsen:
  - pseudonymisering og kryptering av personopplysninger,
  - evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
  - evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
  - en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Vurdering informasjonssikkerhet



Oppsummering

- Få krav i regelverket
- Hva er «egnet sikkerhetsnivå?
  - Må vurderes for *den konkrete* behandlingen
  - Nå? Når vurdere igjen? Endringer i behandlingen, (forståelse av) regelverk eller teknologi som nødvendiggjør ny vurdering?
  - Krav for behandlingsansvarlig og for databehandler
  - Må vurderes og besluttes, og akseptere «restrisiko»
  - Planlegge tiltakene for å nå nivået
- Vil man noen gang være «innenfor»? Eller vil alt vurderes i «bakspeilet» etter et brudd?
- Det viktigste:
  - Gjøre vurderinger og tiltak, og
  - kunne påvise (dokumentere) vurderingene og tiltakene
  - (og kontrollere at tiltak gjennomføres og etterleves)

Takk for meg

Jan Sandtrø

Advokat MNA

+47 99731934

Jan@Sandtro.no

www.sandtro.no

linkedin.com/in/sandtro

twitter.com/JanSandtro