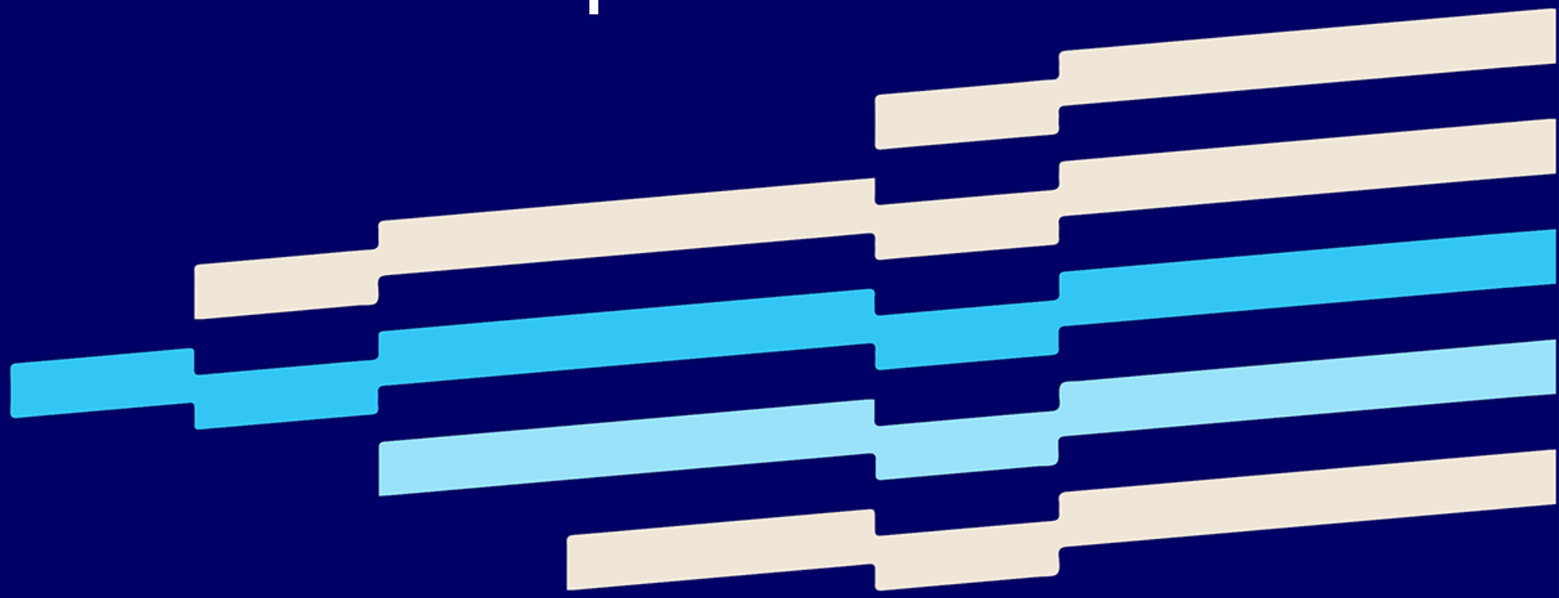
Difi
Direktoratet for
forvaltning og ikt

Risikobasert etterlevelse av pvf

—

NIFS-møte 6.11.2018

Jon Holden, Difi



Tema

- Jobbe effektivt og risikobasert
  - med infosikkerhet, pvf og annen regelverksetterlevelse
- Dvs. effektivt håndtere risiko som er *for høy*, inkl. risiko mht.
  - informasjonssikkerhetsbrudd
  - brudd på personvernlovgivningen
  - brudd på annet regelverk, etc

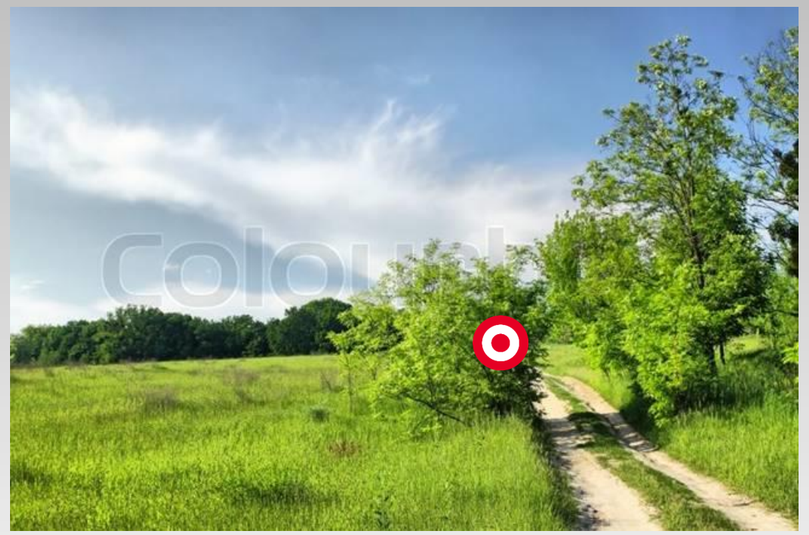
Risiko

- Definisjoner
  - Risiko – effekt av usikkerhet på måloppnåelse
    - ISO 27000:2016 - 2.68

- Overordnet: Risiko for sviktende måloppnåelse
  - Mht. hovedoppdraget – pasientsikkerhet, innbyggertjenester
  - Mht. regelverksetterlevelse, inkl. personvern, infosikkerhet
- Delbegreper:
  - Informasjonssikkerhetsrisiko – skyldes informasjonssikkerhetsbrudd: brudd på k, i eller t
    - Jf. ISO 27000:2016 pkt 2.33
  - Personvernrisiko – rammer personers friheter eller rettigheter
    - Primært personvern, men også andre rettigheter

Usikre omgivelser

- Hvor skal vi prioritere innsatsen?
- Vurdere uønskede hendelsers risiko (konsekvens og tilhørende sannsynlighet), ev. tiltak
- Mht.
  - Infosikkerhetsbrudd
  - Brudd på personvernbestemmelser
  - etc



Personvernforordningens internkontrollkrav

- **Krav om internkontroll og dokumentasjon**
  - Artikkel 24
  - Danner basis for arbeidet
  - Krever **risikobasert tilnærming**
    - Vurdere risiko for sviktende etterlevelse
    - Iverksette **egnede** tiltak
      - **Retningslinjer** er ett virkemiddel, blant flere
      - **Dokumentasjon** er ett virkemiddel.
        - Merk: skal også ivareta Datatilsynets behov

Artikkel 24.Den behandlingsansvarliges ansvar

1. 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.

2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller godkjente sertifiseringsmekanismer som nevnt i artikkel 42 kan brukes som en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes.

Difi

Pvf artikkel 24 (internkontroll)

- 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 og databehandleren 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.

Pvf artikkel 32 (infosikkerhet)

- Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og **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 oppnå et sikkerhetsnivå** som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet, ...

Sammenheng internkontroll infosikkerhet og personvern

- **Risiko** for sviktende måloppnåelse er hovedfokus – efvf § 15, (hensyntas indirekte for pvf)
- **Risiko** for personers rettigheter og friheter er hovedfokus – pvf, (inkludert blant målene i efvf)
  - mht. sikkerhetsbrudd (k, i, t) – art 32
  - mht. brudd på forordningens krav – art 24
- **Egnede** organisatoriske og tekniske tiltak skal iverksettes
  - Behandlingens art, omfang, formål og sammenheng er relevant for å finne egnede tiltak (jf. risiko for måloppnåelsen)
    - Dessuten gjennomføringskostnader og «den tekniske utvikling» – mht. pvf art 32

Difi

Pvf art 24 (internkontrollkravet) - oppsummert

- **Egnede** tekniske og organisatoriske tiltak…
- basert på
  - **risiko** for personers rettigheter og plikter, og
    - «…risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter…»
  - **egenskaper** ved behandlingen
    - «Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i…»

Personvernrisiko – hva er det?

- **Risiko** ifbm. tilsiktet/lovlig behandling for brudd på
  - **Personvernprinsippene** jf. art 5
    - Lovlighet/rettferdighet/åpenhet
    - Formålsbegrensning
    - Adekvate/relevante/begrenset
    - Riktighet
    - Lagringsbegrensning
    - Integritet/fortrolighet
  - Brudd på **personopplysningsplikter**
    - Rettslig grunnlag (art 6-11)
    - Informasjonsplikter (art 12-14) / Innsynsrett (art 15) / Retting, sletting, flytting (art 16-20) / Protest, profilering/automatisering (art 21-22)
    - Innebygd personvern, standardinnstillinger (art 25) / Protokoll (art 30) /Informasjonssikkerhet, varsling av brudd (art 32-34) / Personvernkonsekvensvurderinger, drøfting (art 35-36) / Personvernombud (art 37-39)
    - Behandling i utlandet – tilstrekkelige garantier (44-49)
- Risiko ifbm. utilsiktet/ulovlig behandling – **informasjonssikkerhetsrisiko**, art 32

Difi

Momenter som trekker mot høy personvernrisiko

- Veiledning til dpia-vurderinger, jf pvf art 35
  WP248 rev.01 (okt 2017). Gruppen viser også til pvf art 35 og fortalen 71, 75, 89, 91.
  Datatilsynets veileder
  - Evaluering og skåring
  - Automatisering av beslutninger & hindre rettigheter/muligheter
  - Overvåking av område
  - Opplysningenes art, inkl. særlige kategorier og andre intime opplysninger
  - Storskalabehandling
  - Sårbare registrerte, ujevn makt, vanskelig ivareta sine behov
  - Ny teknologi, med ukjente risikoer, eks. noen IoT-er
- Se også veiledning til varsling iht. pvf art 33-34, WP250

Difi

Hva betyr det i praksis?

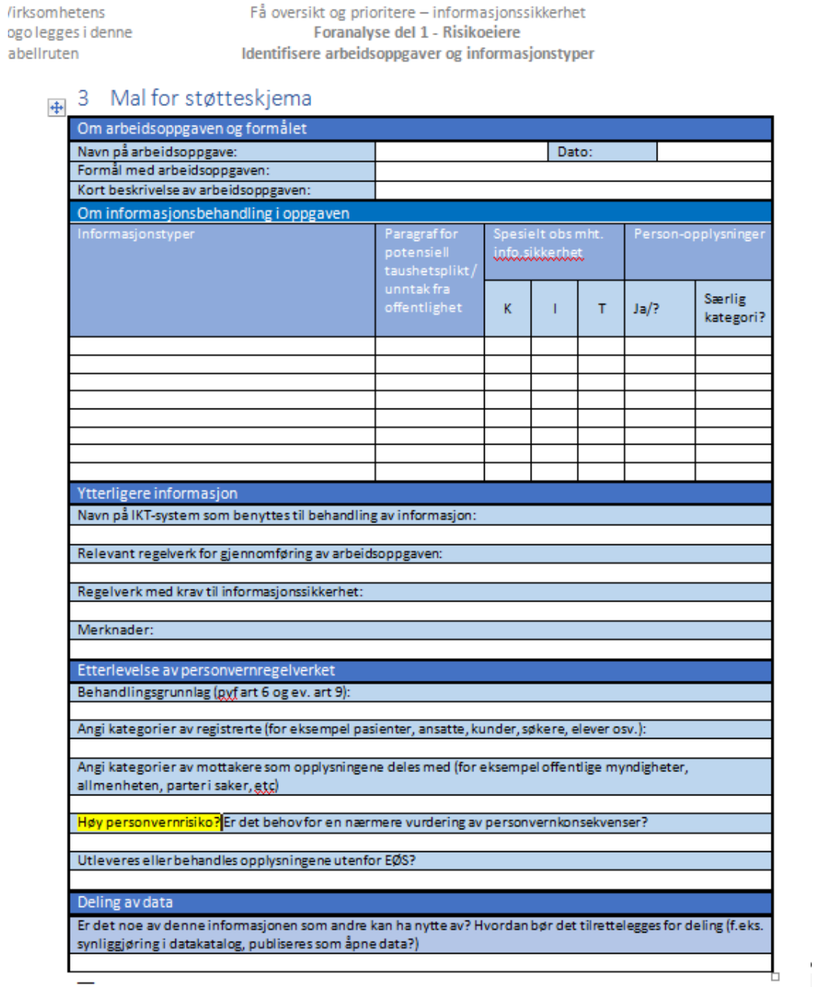
- Prioriter tiltak for å få ned høy personvernrisiko
  - Veiledning til pvf art 35 om personvernkonsekvensvurdering er til hjelp
    - Informasjonssikkerhetsrisiko er ett relevant moment
    - Sentralt poeng: **hva mener de registrerte**?

  - Behandlinger som kanskje særlig bør vurderes:
    (pga skadepotensiale, ta med sannsynlighet!)?
    - Intime opplysninger (konfidensialitetsbehov - lovlighet)
    - Beslutninger med stor betydning (integritetsbehov – riktighet)
    - Usikre beslutninger (- riktighet, formålsendring, eks. stordata)
    - Uventet bruk (åpenhet)
    - Atferdskjølende bruk (rimelighet)
- Finne egnede tiltak
  - Eks. god informasjon, involvere brukerne, sikkerhetstiltak,

Difi

Internkontrollveilederen ble revidert i sommer

- Foranalyse
  - Prosesskartlegging med tilhørende informasjonsbehandling
    - OBS mht K, I, T
    - Personopplysninger, særlige kategorier
    - Identifisere om behandlingen kan gi «høy personvernrisiko»



/irksomhetens ogo legges i denne abellruten

Få oversikt og prioritere – informasjonssikkerhet
Foranalyse del 1 - Risikoeiere
Identifisere arbeidsoppgaver og informasjonstyper

3 Mal for støtteskjema

Om arbeidsoppgaven og formålet						
Navn på arbeidsoppgave:			Dato:			
Formål med arbeidsoppgaven:						
Kort beskrivelse av arbeidsoppgaven:						
Om informasjonsbehandling i oppgaven						
Informasjonstyper	Paragraf for potensiell taushetsplikt / unntak fra offentlighet	Spesielt obs mht. info.sikkerhet			Person-opplysninger	
		K	I	T	Ja/?	Særlig kategori?
Ytterligere informasjon						
Navn på IKT-system som benyttes til behandling av informasjon:						
Relevant regelverk for gjennomføring av arbeidsoppgaven:						
Regelverk med krav til informasjonssikkerhet:						
Merknader:						
Etterlevelse av personvernregelverket						
Behandlingsgrunnlag (pvf art 6 og ev. art 9):						
Angi kategorier av registrerte (for eksempel pasienter, ansatte, kunder, søkere, elever osv.):						
Angi kategorier av mottakere som opplysningene deles med (for eksempel offentlige myndigheter, allmenheten, parter i saker, etc)						
Høy personvernrisiko? Er det behov for en nærmere vurdering av personvernkonsekvenser?						
Utleveres eller behandles opplysningene utenfor EØS?						
Deling av data						
Er det noe av denne informasjonen som andre kan ha nytte av? Hvordan bør det tilrettelegges for deling (f.eks. synliggjøring i datakatalog, publiseres som åpne data?)						

?

Difi