Informasjonssikkerhet

FINF4012 – forelesning 11.09.2018

Jon B. Holden – jobe@holden.no

Innhold

- Overordnet om risikostyring - internkontroll
- Gjeldende regelverk med informasjonssikkerhetskrav
  - Hovedvekt på efvf, pvf
  - Dekker også andre offentligrettslige krav
- Andre risikobaserte regler i pvf

Tilstrekkelig internkontroll – også på informasjonssikkerhetsområdet

RISIKOSTYRING

Risiko

- Avvik fra mål
  - Positive og negative
- Hendelse – konsekvens (dvs. avvik fra målet) * sannsynlighet = risiko
- Risikostyring
  - Vurder risikoen
  - Er risikoen for stor?
  - Hvis ja: Vurder tiltak for å påvirke risikoen
    - Sannsynlighetsreduserende tiltak
      - Eks. Kvalitetskontroll, testing
      - Eks. Kryptering/god nøkkelhåndtering, opplæring, sjekksummer, fysisk sikkerhet, fjellhall,
    - Konsekvensreduserende tiltak
      - Eks. Beredskap, sikkerhetskopiering

Definisjoner: Risiko, informasjonssikkerhet

- ISO 27000:2016
  - 2.68 – Risk
    - effect of uncertainty on objectives
  - 2.33 – Information security
    - preservation of *confidentiality (2.12), integrity (2.40) and availability (2.9) of information*

- Vanlig avgrense til negative avvik

- Informasjonssikkerhetsrisiko – avvik mht. informasjonssikkerhetsmål
  - Bevare informasjonens
    - konfidensialitet
    - integritet
    - tilgjengelighet
  - Andre egenskaper, som autensitet, ansvarlighet, ikke-benekting og pålitelighet kan også inngå (jf. fotnote til 2.33)

Regelverk med krav til risikobasert internkontroll i forvaltningen

- Staten
  - Økonomireglementet § 4
    - Bokstav b: «sikre at fastsatte **mål og resultatkrav oppnås**, ressursbruken er **effektiv** og at virksomheten drives i samsvar med **gjeldende lover og regler**, herunder krav til god forvaltningsskikk, habilitet og etisk adferd»
    - Tredje ledd: «**Styring, oppfølging, kontroll og forvaltning** må **tilpasses** virksomhetens egenart samt **risiko** og vesentlighet.»
- Kommunen
  - Kommuneloven § 23 nr 2:
    - «Administrasjonssjefen skal sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for **betryggende kontroll**.»

Krav i pvf om risikobasert internkontroll

- Formål
  - Sikre og dokumentere etterlevelse av forordningen, jf. art 24 nr 1
  - Jf. ansvarlighetsprinsippet i art 5 nr 2
- Hva skal på plass?
  - Egnede organisatoriske og tekniske tiltak
- Hvor omfattende?
  - Tilpasset risiko, formål og omstendigheter
    - Eks. retningslinjer skal inkluderes hvis rimelig

Internkontrollbestemmelsen, art 24

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.

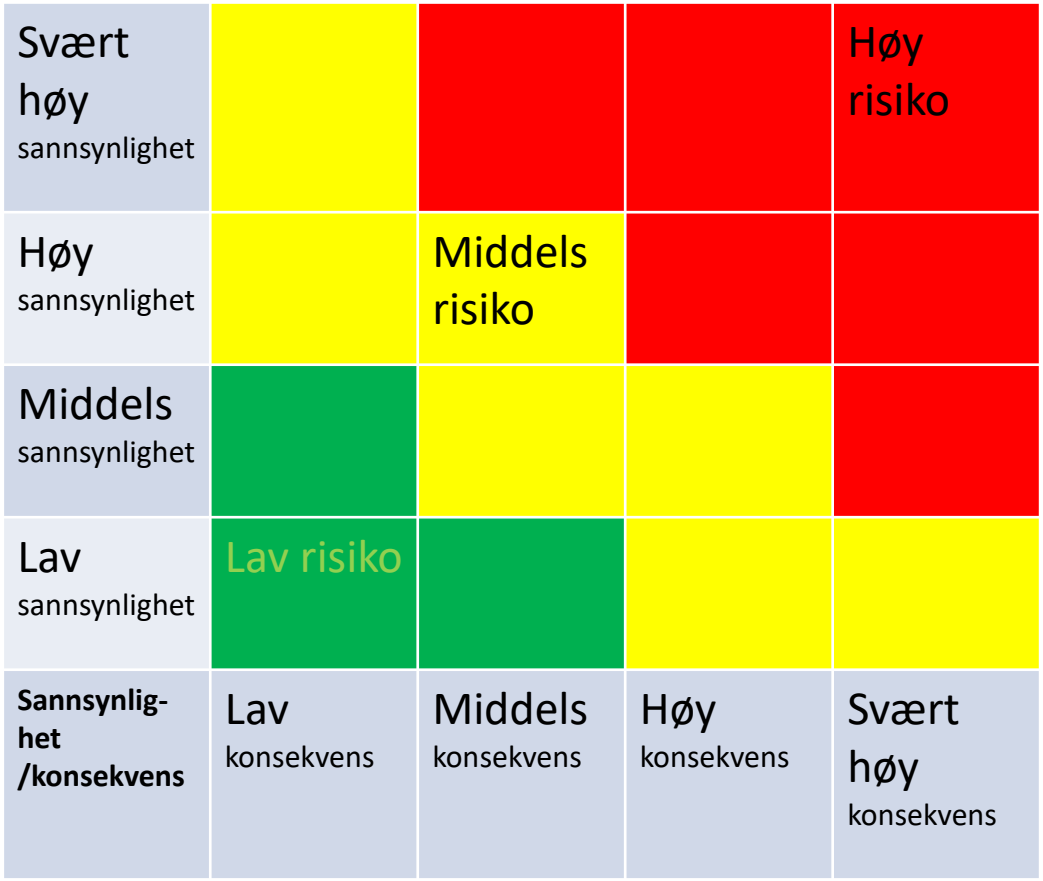
Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

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** … kan brukes som en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes.

I praksis

- Risikovurdering - fare for (negative) **avvik fra mål**
  - Virksomhetens mål
  - Lovpålagte plikter (andres rettigheter)
  - Sikkerhetsbrudd
- Vurdere om risiko må håndteres, og i så fall hvordan



Risikostyring i infosikkerhetsregelverkene

- Eforvaltningsforskriften
  - § 15 - omfang og innretning «tilpasset risiko»
- Personvernforordningen
  - Art 32 - «egnet sikkerhetsnivå», art 24 om internkontroll / krav til innebygd personvern art 25 - «egnede … tiltak», krav til utredning av personvernkonsekvenser art 35 – vurdere risiko mv
- Sikkerhetsloven
  - Forskrift om sikkerhetsadministrasjon, kapittel 4, §§ 4-1, 4-2
    - fjerne «overflødige» tiltak, avdekke «behov ut over» minimumskravene

RETTSLIGE KRAV TIL INFORMASJONSSIKKERHET

Regelverk med krav til informasjonssikkerhet

- Generelle regelverk – K, I, T
  - Eforvaltningsforskriften § 15
    - og §§ 5, 8, kap 4-6
  - Personvernforordningen art 5, 32-34 – personopplysninger
- Spesielle
  - Konfidensialitet
    - Taushetspliktsregler – fvl §§ 13-13f
    - Sikkerhetsloven – rikets sikkerhet m.v
    - Beskyttelsesinstruksen – andre særlige konfidensialitetsbehov
  - Tilgjengelighet/integritet
    - Arkivloven
    - Sikkerhetsloven – skjermingsverdige objekter
  - + særlover

Forvaltningsloven

- Regler om taushetsplikt
  - Fvl § 13 – hovedregel – ”hindre”
  - Fvl § 13c – ”betryggende” oppbevaring
- Forskriftshjemmel om e-kom og e-saksbehandling, jf. § 15a

Eforvaltningsforskriften

- Opprinnelig fra 2002
- Viktige endringer 2014 – digitalt førstevalg
- Hjemlet i forvaltningsloven § 15a (og esignl)
- Formål, § 1:
  - **sikker og effektiv bruk** av elektronisk kommunikasjon med og i forvaltningen
  - **forutsigbarhet**, fleksibilitet, samordning av løsninger
  - enhver på en **enkel måte** kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige

Efvf § 15

- § 15. *Internkontroll på informasjonssikkerhetsområdet (utdrag: annet og tredje ledd)*
  - Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på **anerkjente standarder** for styringssystem for informasjonssikkerhet. Internkontrollen **bør** være en **integrert del** av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi **anbefalinger** på området.
  - Omfang og innretning på internkontrollen skal være **tilpasset risiko**.
- Veiledning: internkontroll.infosikkerhet.difi.no

Difis anbefaling mht. internkontroll

- Basere seg på ISO/IEC 27001:2013 ved etablering av internkontrollen
- Bruke veiledningen på int[illegible]rhet.difi.no

Øvrige bestemmelser i efvf

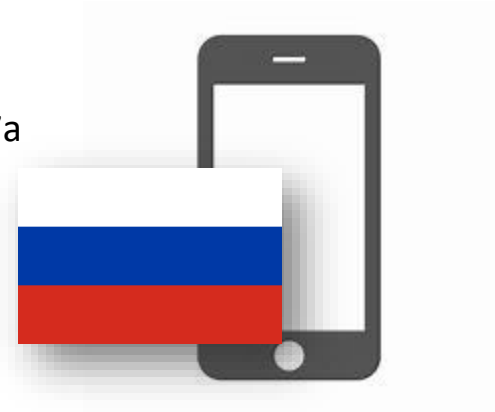
- §§ 5 og 8 – forebygge uberettiget innsyn
- § 17 og 20 – opplæring av og krav til ansatte
- Kap 4-6 – sertifikater, signaturer, private nøkler m.v.
  - §28 om konvertering av avanserte signaturer
    - Merk: Lov om tillitstjenester (gjennomfører eIDAS-forordningen) vedtatt juni 2018 – supplerer denne (plikt til å akseptere noen signaturformater m.v., hvis det kreves avanserte signaturer)

- Ytterligere lesing
  - Se veileder til eforvaltningsforskriften
    - Særlig kommentert forskrift

ANDRE OFFENTLIGRETTSLIGE REGELVERK OM INFOSIKKERHET

Sikkerhetsloven 1998

- Lov om **forebyggende sikkerhetstjeneste**
  - Definisjon: Aktivitet for å «fjerne eller redusere risiko [pga] **sikkerhetstruende virksomhet**», jf. § 3 nr 1
  - Sikkerhetstruende virksomhet: forberedelse/forsøk/gjennomføring/medvirkning mht. **spionasje, sabotasje eller terrorhandlinger,** jf. § 3 nr 2
  - Overordnet formål: ”motvirke trusler mot rikets selvstendighet og sikkerhet og andre **vitale nasjonale sikkerhetsinteresser**…”, jf. § 1
- Gjelder
  - Forvaltningen, ev. andre etter Kongens beslutning, § 2
- Sikkerhetsgradering av dokumenter for å ivareta konfidensialitetsbehov, § 11
  - 4 nivåer: STRENGT HEMMELIG/HEMMELIG/KONFIDENSIELT/BEGRENSET
  - Varighet 30 år
  - Håndteringskrav
    - Informasjonssikkerhetsforskrift: Godkjent IT-system, kryptokrav m.v.
    - Sikkerhetsadministrasjonsforskrift
    - taushetsplikt og streng need-to-know, § 12
    - NSM-godkjenning av informasjonssystemer, § 13, m.v.
    - Klarering/autorisasjon av personell
- Klassifisering av objekter for å ivareta integritets-/tilgjengelighetsbehov, § 17a
  - 3 nivåer: MEGET KRITISK/KRITISK/VIKTIG
    - Objektsikkerhetsforskriften



Ny sikkerhetslov 2018

- Lov 24/2018
  - Ikke i kraft
    - Noe videre virkeområde, nytt tilsynsregime m.v.
  - Formål
    - Vern mot sikkerhetstruende virksomhet – **tilsiktede** handlinger som kan skade **nasjonale sikkerhetsinteresser**, §§ 1-1 jf. 1-5 nr 4 og nr 1
    - «Nasjonale sikkerhetsinteresser: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser»
  - Sikring av informasjon og objekter
    - **K: skjermingsverdig informasjon** iht. kapittel 5
      - 4 graderingsnivåer opp til strengt hemmelig
      - Taushetsplikt, jf. § 5-4
    - **I/T: skjermingsverdig objekt** og infrastruktur iht. kap 7
      - 3 klassifiseringsgrader opp til meget kritisk

Beskyttelsesinstruksen

- Hjemmel: Kongens instruksjonsmyndighet, jf. Grl. § 3
  - Gjelder statsforvaltningen
- Grunnkrav
  - Særlig høyt behov for konfidensialitet, og som ikke dekkes av sikkerhetsloven, jf. § 4
    - **«Strengt fortrolig»** benyttes dersom det vil kunne **forårsake betydelig skade for** offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.
    - **«Fortrolig»** benyttes dersom det vil kunne **skade** [samme]
  - **Dokumentet må kunne unntas fra offentlighet etter offentleglova, jf. § 3**
- Graderingen må være påkrevd, ikke ”for sikkerhets skyld”, § 5 nr 2
- I utgpkt: 30 års varighet, § 5 nr 3
- Håndteringskrav
  - Streng tilgangsstyring (tjenestelig behov), § 7
  - Oppbevares forsvarlig sikret, § 9
  - Forsendeskrav: strengt fortrolig sendes i dobbelt konvolutt eller kurér, § 10
  - Elektronisk håndtering som etter sikkerhetslovens regler for BEGRENSET, ”så langt det passer”, § 12, inkl. informasjonssikkerhetsforskriften

Arkivforskriften

- Krav til sikkerhetskopiering, § 2-10 annet ledd
  - Kvar dag skal det takast tryggingskopi av databasen på elektronisk lagringsmedium. Tryggingskopiane skal lagrast på einingar som er fysisk åtskilde frå dei einingane der databasen ligg.
- Krav til godkjente lagringsmedier, § 2-11
  - Til arkivmateriale som etter gjeldande føresegner skal takast vare på for ettertida, skal det nyttast godkjent lagringsmedium, jf. §§ 2-12 - 2-15. Materiale på elektronisk medium må kopierast eller konverterast til nye lagringseiningar i den grad det er nødvendig for å ta vare på og ha tilgang til dokumentinnhaldet
- Krav til fysisk miljø, § 4-1 annet ledd
  - Arkivlokala hos offentlege organ skal gi arkivmaterialet vern mot vatn og fukt, mot brann og skadeleg varme, mot skadeleg påverknad frå klima og miljø og mot skadeverk, innbrot og ulovleg tilgjenge.

PERSONVERNFORORDNINGEN

Bestemmelser om informasjonssikkerhet i PVF

- Grunnprinsipp om *integritet og konfidensialitet*, jf. art 5 nr 1 bokstav f
- Art 32-34
  - Sikkerhet ved behandlingen, art 32
  - Sikkerhetsbrudd – varslingsregler
    - Melding til tilsyn, art 33
    - Underretning til den registrerte, art 34
- Tilstøtende bestemmelser
  - Art 24 – internkontroll
  - Art 25 – innebygd personvern
  - (Art 35 – personvernkonsekvensvurdering)

PVF – Grunnprinsippene
inkl. integritet og konfidensialitet

Artikkel 5.Prinsipper for behandling av personopplysninger

1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («**lovlighet, rettferdighet og åpenhet**»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål … («**formålsbegrensning**»),

c) være adekvate, relevante og begrenset til … («**dataminimering**»),

d) være korrekte og om nødvendig oppdaterte; … («**riktighet**»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder … («**lagringsbegrensning**»),

f) behandles på en måte som sikrer **tilstrekkelig sikkerhet** for personopplysningene, herunder vern mot **uautorisert eller ulovlig behandling** og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («**integritet og konfidensialitet**»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («**ansvar**»).

Forordningens krav til informasjonssikkerhet, art 32 nr 1

- Hva skal sikres?
  - konfidensialitet, integritet, tilgjengelighet
- Hvem skal sikre?
  - Den behandlingsansvarlige og databehandleren
- Hvor sikkert?
  - Egnet sikkerhetsnivå,
  - Tilpasset risiko, kostnader og forholdene for øvrig

Artikkel 32 nr 1
Sikkerhet ved behandlingen

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 og databehandleren 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 …

Infosikkerhetstiltak, jf. art 32 - eksempler

[1. Passende tekniske og organisatoriske tiltak, herunder bl.a. alt ettersom hva som er egnet:]

a) **pseudonymisering og kryptering** av personopplysninger,

b) evne til å sikre vedvarende **konfidensialitet, integritet, tilgjengelighet og robusthet** i behandlingssystemene og -tjenestene,

c) evne til å **gjenopprette** tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d) en prosess for regelmessig **testing**, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge **av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til** personopplysninger som er overført, lagret eller på annen måte behandlet.

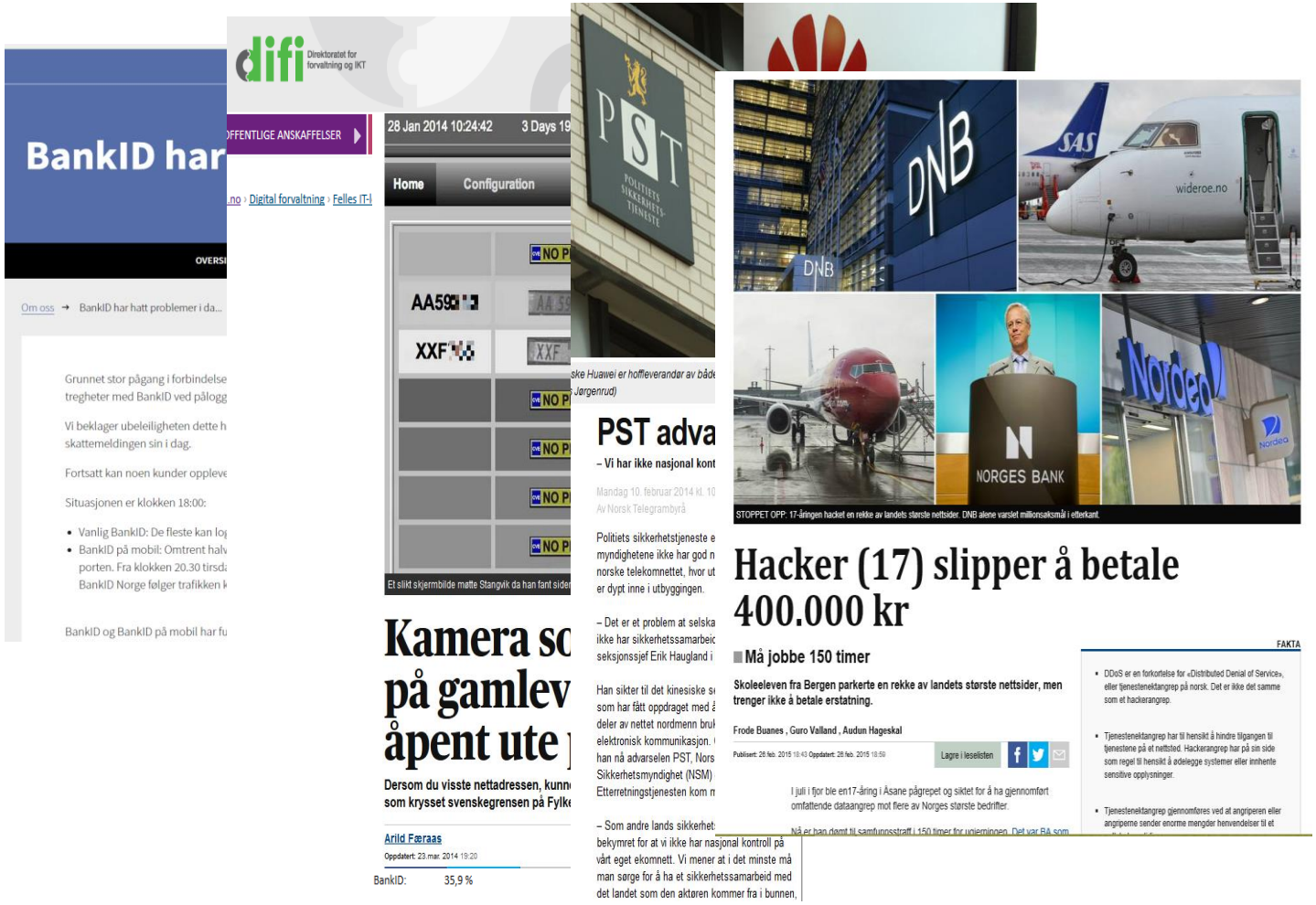
3**. Overholdelse av godkjente atferdsnormer** som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en **faktor for å påvise** at kravene i nr. 1 i denne artikkel er oppfylt.

4. Den behandlingsansvarlige og databehandleren **skal treffe tiltak for å sikre** at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger **bare etter instruks** fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.

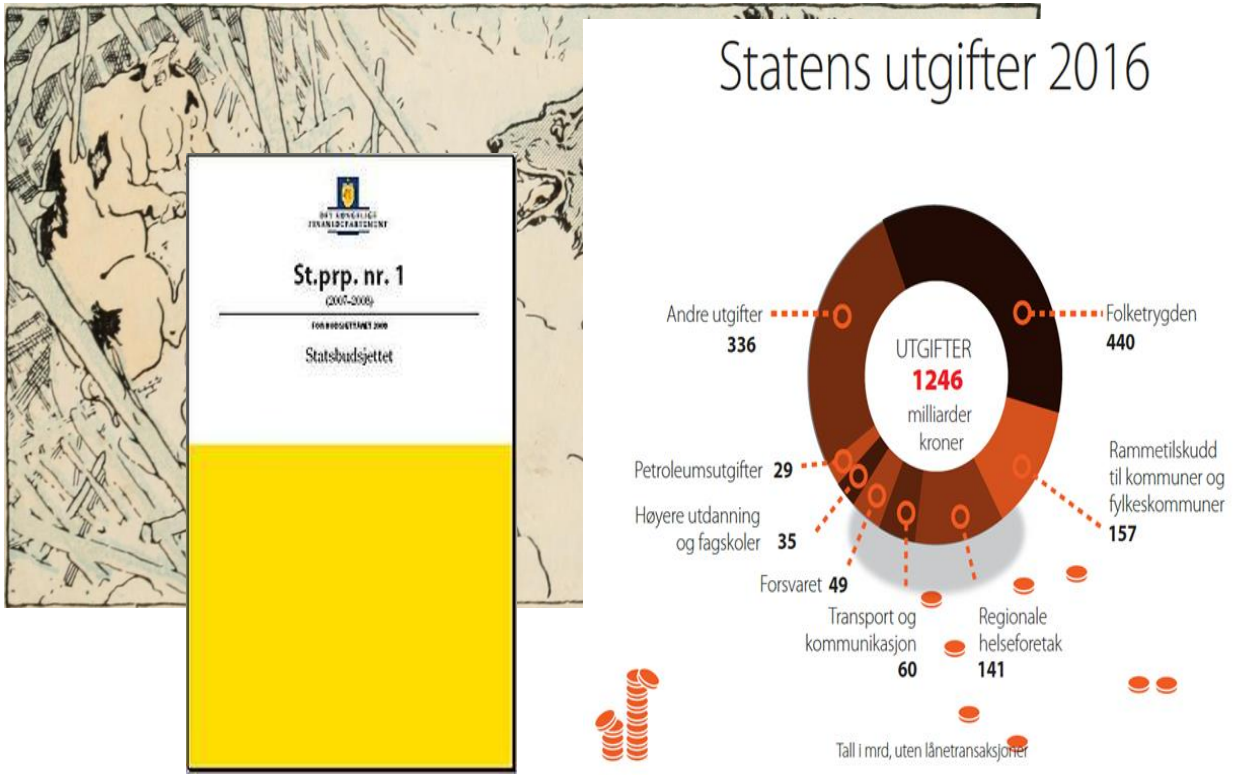
Eksempler på sikkerhetstiltak

- Krav til innlogging
  - Passord, MinID, BankID, smartkort, biometri (fingeravtrykk, ansiktsgeometri), etc
- Tilgangsstyring (need-to-know vs. need-to-hide)
- Krav til logging, gjennomgang av logger
- Backup, reserveløsninger
- Kryptering, tempest-vern, forsvarlig sletting
- Sikkerhetstesting (innbruddstest)
- Revisjon

Praktisk øvelse – vurder K, I, T tilsiktet/utilsiktet



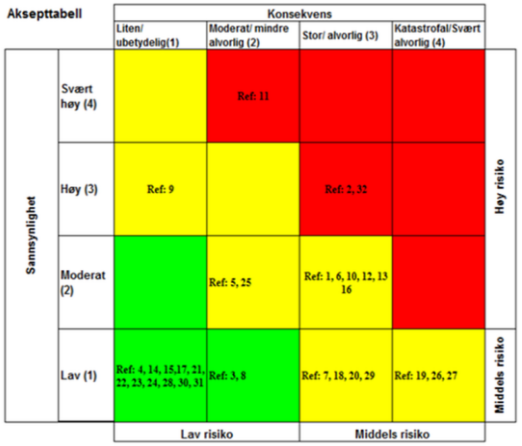
Hvor sikkert?



HVORDAN FINNE RIKTIG NIVÅ?

Risikovurdering - prioritering av tiltak

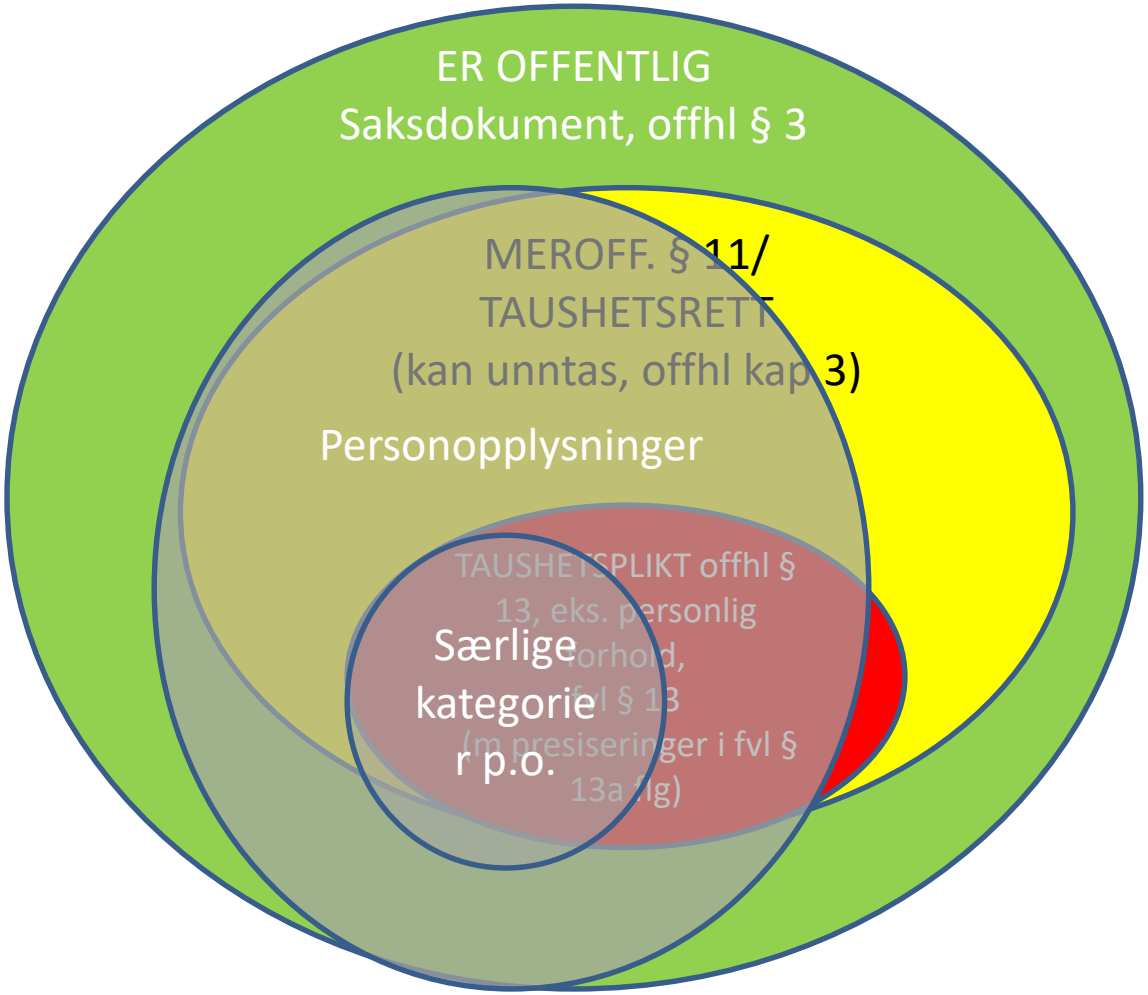
- Mange metoder
- Veiledning fra Datatilsynet og Difi
  - **Kartlegge** arbeidsprosesser, opplysningstyper
  - **Identifisere** uønskede hendelser
  - **Vurdere** konsekvenser og tilhørende sannsynligheter
  - Innplassering i **risikomatrise**
  - Valg av ev. **tiltak**



Kartlegging

- Konfidensialitet - innsynsvern
  - Uvedkommendes bruk/innsyn
  - Taushetsplikt vs. offentlighet
- Integritet - endringsvern
  - Betydning for vedtak, avgjørelser
- Tilgjengelighet - tilgangsvern
  - Tidskritisk?

Kartlegging - konfidensialitet



Identifisere og analysere hendelser

- Identifisere uønskede hendelser
  - Villede og uaktsomme handlinger, hendelige uhell og naturfenomener
- Vurdere konsekvenser for hendelsene
- Vurdere sannsynlighet for hendelsene
- = Risiko

Eksempler på hendelser

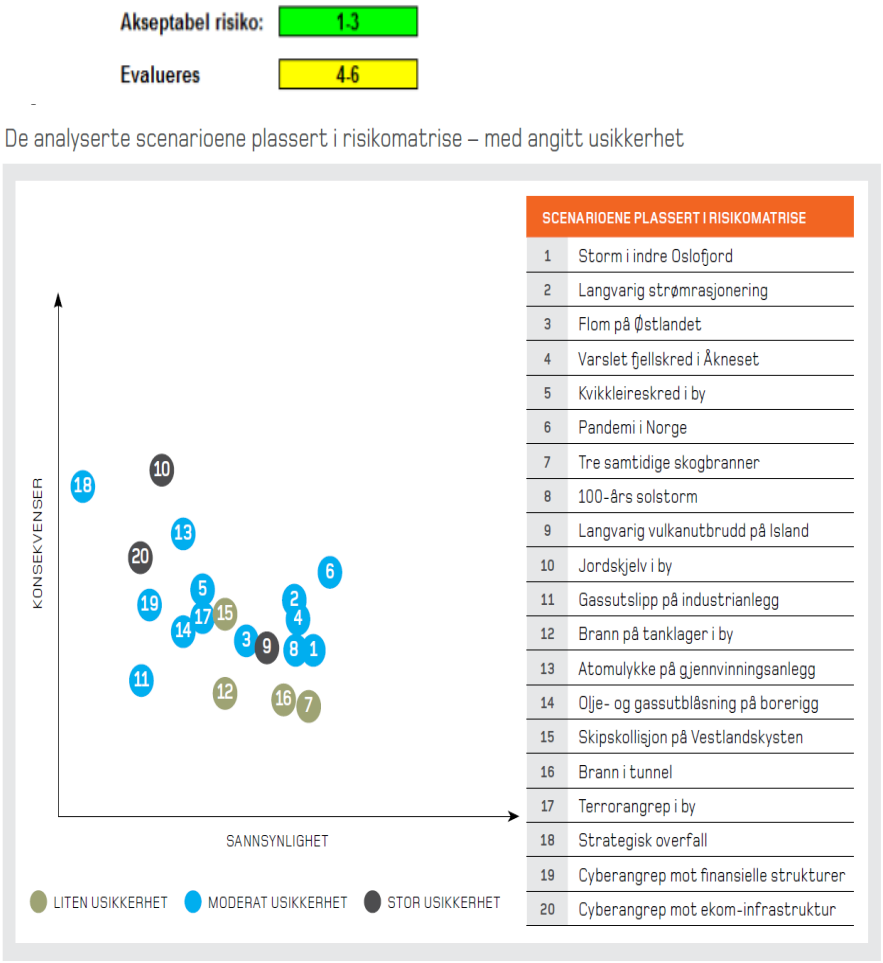
- Hacking av nettløsning – publiserer opplysningene
- Hacking av nettløsning – endrer utbetalingskonto
- Utro tjener selger opplysninger om Kongehuset til pressen
- Datahallen brenner – opplysningene mistes
- Datahallen brenner – tjenesten er utilgjengelig

Vurdering av skade og sannsynlighet

- Egne og andre erfaringer
  - Tilfeldige hendelser
  - Tilsiktede hendelser
- Trusselaktører - hvem har nytte av opplysningene?
  - Motivasjon til misbruk
  - Gevinst av misbruk
- Kan skaden heles?

Risikomatrise

- Risiko: sannsynligh konsekvens
- Akseptabelt r fastsettes
- Konsekvense
- Sannsynlighe vha.
  - Letthet, mo kapasitet, f
- Eksempler: Nasjonalt risikobilde (s205)



FIGUR 22. Nasjonalt risikobilde – samlet risikomatrise viser vurdert risiko (sannsynlighet, konsekvens og usikkerhet) knyttet til de konkrete alvorlige scenarioene som er analysert.

Risikovurdering

- Kan få hjelp av ev. gjennomført personvernkonsekvensvurdering, jf. art 35
  - Nødvendig hvis **sannsynligvis «høy risiko»** for fysiske personers rettigheder og friheter
  - Analysen skal bl.a. inkludere
    - vurdering av risiko, art 35 nr 7 c
- Relevante momenter for risikovurderingen
  - Fortalen avsnitt 75 – relevante skader, relevante momenter
- Merk: Objektiv vurdering
  - Fortalen avsnitt 76

Fortalen 75 – risikoøkende momenter

- Behandling av personopplysninger kan føre til at det oppstår risikoer av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter som kan medføre fysisk, materiell eller ikke-materiell skade, særlig
  - når behandlingen **kan føre til** forskjellsbehandling, identitetstyveri eller -bedrageri, økonomisk tap, skade på omdømme, tap av **fortrolighet for taushetsbelagte** personopplysninger, uautorisert **oppheving av pseudonymisering** eller andre **betydelige økonomiske eller sosiale ulemper**,
  - når de registrerte kan bli **fratatt sine rettigheter og friheter** eller bli hindret i å **utøve kontroll over egne personopplysninger**,
  - når behandlingen gjelder personopplysninger om **rasemessig eller etnisk opprinnelse, politisk oppfatning, religion eller overbevisning, fagforeningsmedlemskap,** og behandling av genetiske opplysninger, helseopplysninger, seksuelle forhold eller straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak,
  - når personlige aspekter vurderes, særlig for å analysere eller forutsi aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser, for å opprette eller bruke personlige **profiler**,
  - når sårbare fysiske personers, særlig **barns**, personopplysninger behandles, eller når behandlingen omfatter en stor mengde personopplysninger og berører et stort antall registrerte

Hvilke sikkerhetstiltak? Jf art 32

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 og databehandleren 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 …

Hvis det går galt, jf. art 33-34.

- **Dokumentasjonsplikt**, jf. art 33 nr 5
- Når er det **varslingsplikt**?
  - Brudd på personopplysningssikkerheten = K-, I-, T-brudd
    - pvf art 4(12) «brudd på personopplysningssikkerheten» 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»
    - Veiledning fra artikkel 29-gruppen - WP250 rev.01 (oppdatert 6.2.2018)
- **Hvem skal varsle om hva?** jf. art 33 nr 1, nr 2, art 34 nr 1.
  - Databehandler til den behandlingsansvarlige
    - Alt
  - Den behandlingsansvarlige til tilsynsmyndigheter, art 33
    - med mindre «sannsynligvis ikke vil medføre risiko»
  - Den behandlingsansvarlig til de(n) registrerte, art 34
    - hvis det er «sannsynlig at bruddet … vil medføre … høy risiko» & ikke unntaksregler treffer
- Hvor fort?
  - Uten ugrunnet opphold.
  - Som hovedregel senest innen 72 timer til tilsynsmyndigheter..
- **Eksempler** på (potensielle) personopplysningssikkerhetsbrudd:
  - Mistet ukryptert minnepinne (2008), hacking (2013 usa), ransomware 2017, langvarig strømbrudd (2018), Skolemeldings-app (2018)

Innebygd personvern m.v., art 25

Idet det tas hensyn til

1. den tekniske utviklingen,
2. gjennomføringskostnadene,
3. behandlingens art, omfang, formål og sammenhengen den utføres i, samt
4. risikoene av varierende sannsynlighets- og alvorlighetsgrad
5. for fysiske personers rettigheter og friheter som behandlingen medfører,

skal **den behandlingsansvarlige**, både

- på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen,
- gjennomføre **egnede tekniske og organisatoriske tiltak**,
  - **f.eks. pseudonymisering**, utformet med sikte på en **effektiv gjennomføring av prinsippene** for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen

for å **oppfylle**

- **kravene i denne forordning** og verne de registrertes rettigheter.

Vurdering av personvernkonsekvenser, art 35

Artikkel 35 Vurdering av personvernkonsekvenser

1. Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en **høy risiko** for fysiske personers rettigheter og friheter, skal den **behandlingsansvarlige** før behandlingen foreta en **vurdering av hvilke konsekvenser** den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.

…

Personvernkonsekvensvurderingen kan vise behov for forhåndsdrøfting, jf. art 36. Se også fortalen 94:

” Dersom en vurdering av personvernkonsekvenser viser at behandlingen, **i fravær av** garantier, **sikkerhetstiltak** og mekanismer **for å redusere risikoen**, vil innebære en **høy risiko** for fysiske personers rettigheter og friheter, og den behandlingsansvarlige mener at risikoen ikke kan reduseres ved hjelp av rimelige midler, idet det tas hensyn til tilgjengelig teknologi og gjennomføringskostnader, **bør tilsynsmyndigheten rådspørres** før oppstart av behandlingsaktivitetene.”

SPØRSMÅL?