Krav til informasjonssikkerhet

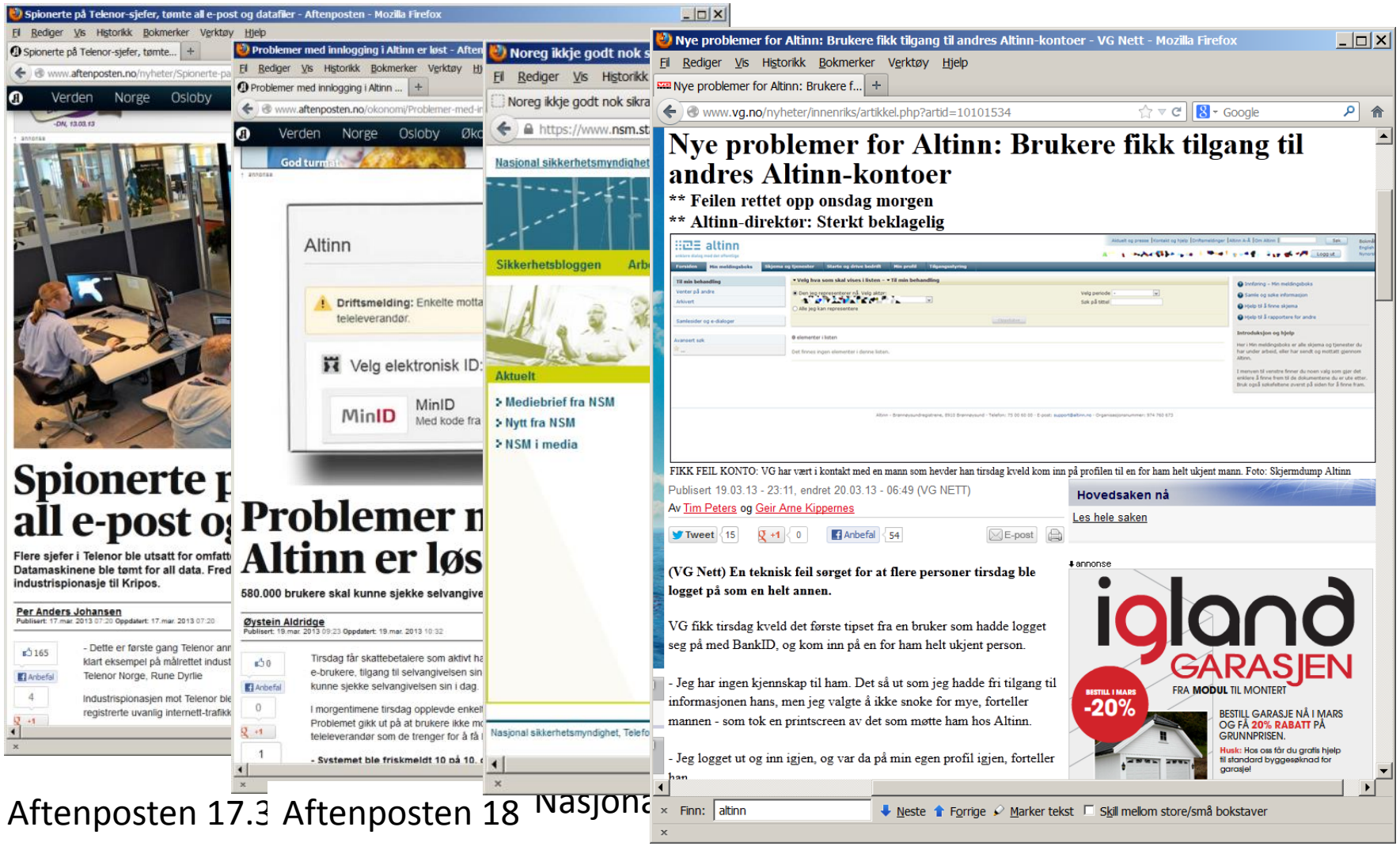
DRI1010 – forelesning 25.03.2015

Jon B. Holden – jobe@holden.no

Dagens tema: Informasjonssikkerhet og eforvaltningsforskriften

- Hva er informasjonssikkerhet?
- Krav til informasjonssikkerhet og internkontroll etter pol
- Eforvaltningsforskriften

Informasjonssikkerhet i media



Aftenposten 17.3 Aftenposten 18 Nasjona

VG 20.3.2013

Informasjonssikkerhet i media

Sikkerhet - hva skal beskyttes?

- Informasjonssikkerhet (def. ISO 27001, 3.4)
  - Bevare konfidensialitet, integritet og tilgjengelighet. Dessuten kan andre egenskaper, som autensitet, ansvarlighet, uavviselighet og pålitelighet, omfattes.
- Konfidensialitet
  - Vern mot uautorisert innsyn
- Integritet
  - Vern mot uautorisert endring/tap
- Tilgjengelighet
  - Tilgjengelig på behov

Direktivet

- Behandlingssikkerhed, artikkel 17:
  - 1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de **fornødne tekniske og organisatoriske foranstaltninger** til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for **ulovlig behandling**.
  - **http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:31995L0046#texte**

Informasjonssikkerhet, pol § 13

- **§ 13.** *Informasjonssikkerhet*
- Den behandlingsansvarlige og databehandleren skal gjennom **planlagte og systematiske** tiltak sørge **for tilfredsstillende informasjonssikkerhet** med hensyn til **konfidensialitet, integritet og tilgjengelighet** ved behandling av personopplysninger.
- For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren **dokumentere** informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
- En behandlingsansvarlig som lar **andre** få tilgang til personopplysninger, **f.eks. en databehandler eller andre som utfører oppdrag** i tilknytning til informasjonssystemet, skal **påse at disse oppfyller kravene** i første og annet ledd.
- Kongen kan gi **forskrift** om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Personopplysningslovens krav

- Hva skal sikres?
  - Vern av konfidensialitet, integritet og tilgjengelighet for personopplysninger, pof § 2-1
- Hvem skal sikre?
  - Den behandlingsansvarlige og databehandleren, § 13
- Hvor sikkert?
  - Tilfredsstillende, jf. § 13 = forholdsmessig, pof § 2-1
  - Risikovurdering, jf. pof § 2-4
  - Behandlingsansvarlig avgjør nivå, ev. Datatilsynet, jf. pof § 2-2

Personopplysningslovens krav (forts.)

- Hvordan sikre?
  - Systematisk, dokumentert arbeid
    - Bl.a. sikkerhetsmål, -strategi, revisjoner (§§2-3 – 2-5), 5 års lagring §2-16 mfl
  - Organisatoriske, tekniske tiltak
    - Eks. pof §§ 2-11 – 2-13 pålegger tiltak *hvis nødvendig*
    - Følge opp databehandlere (”påse”, pol § 13 tredje ledd)

Internkontroll, pol § 14

- **§ 14.** *Internkontroll*
- Den behandlingsansvarlige skal etablere og holde vedlike **planlagte og systematiske** tiltak **som er nødvendige** for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes **kvalitet**.
- Den behandlingsansvarlige skal **dokumentere** tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
- Kongen kan gi **forskrift** med nærmere regler om internkontroll.

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
  - Helseregisterloven § 13 sjette ledd
- Backup, kryptering, forsvarlig destruksjon, vern mot avlytting/tempest, reserveløsning
- Revisjon, pof § 13
- Sikkerhetstesting (innbruddstest)

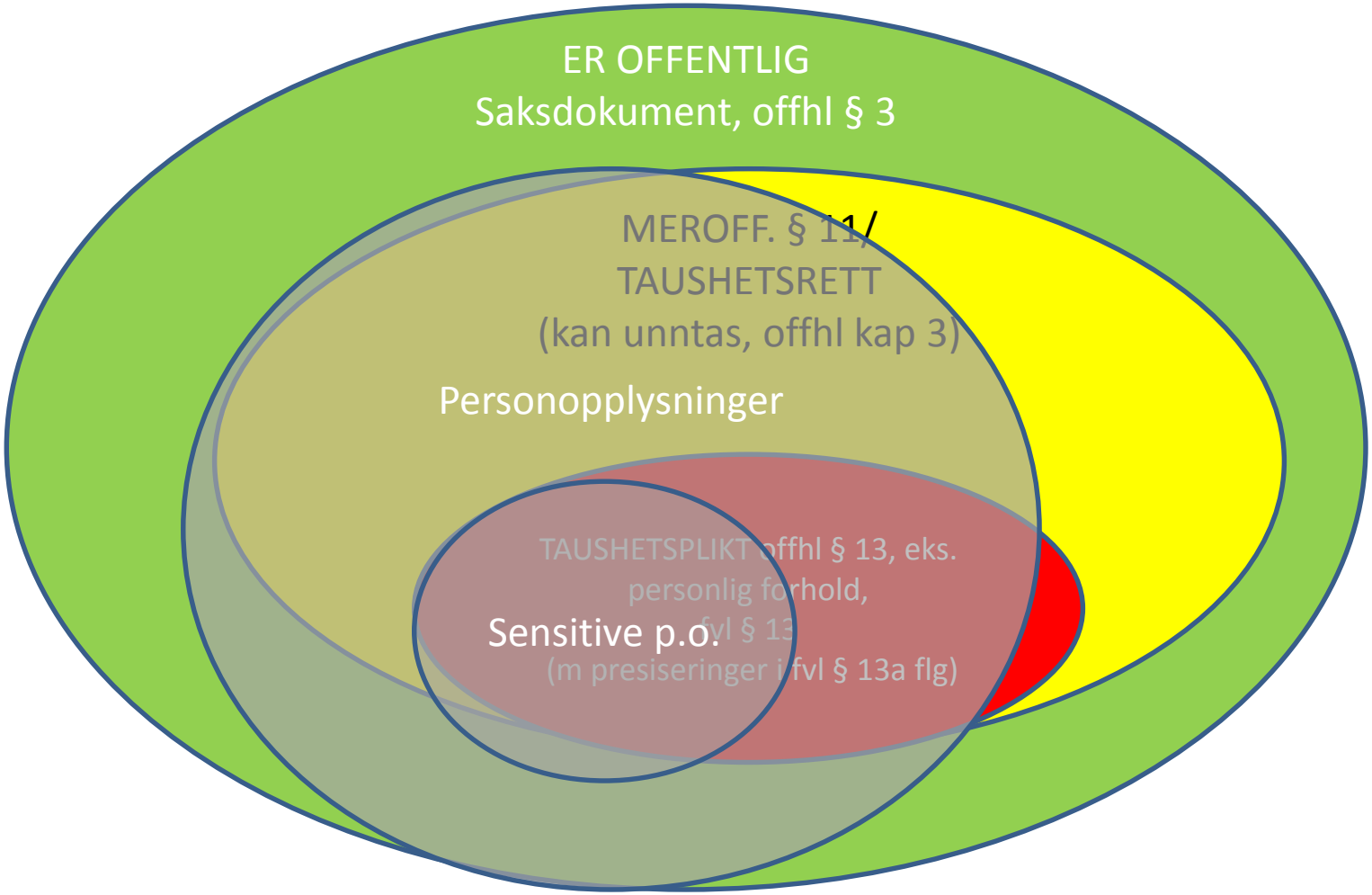
Gjennomføring av risikovurdering

- Mange metoder
- Veiledning fra Datatilsynet og Difi
  - Kartlegge opplysningstyper etc
  - Identifisere uønskede hendelser
  - Vurdere konsekvenser og sannsynligheter
  - Innplassering i risikomatrise
  - Valg av tiltak

Kartlegging

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

Kartlegging - konfidensialitet

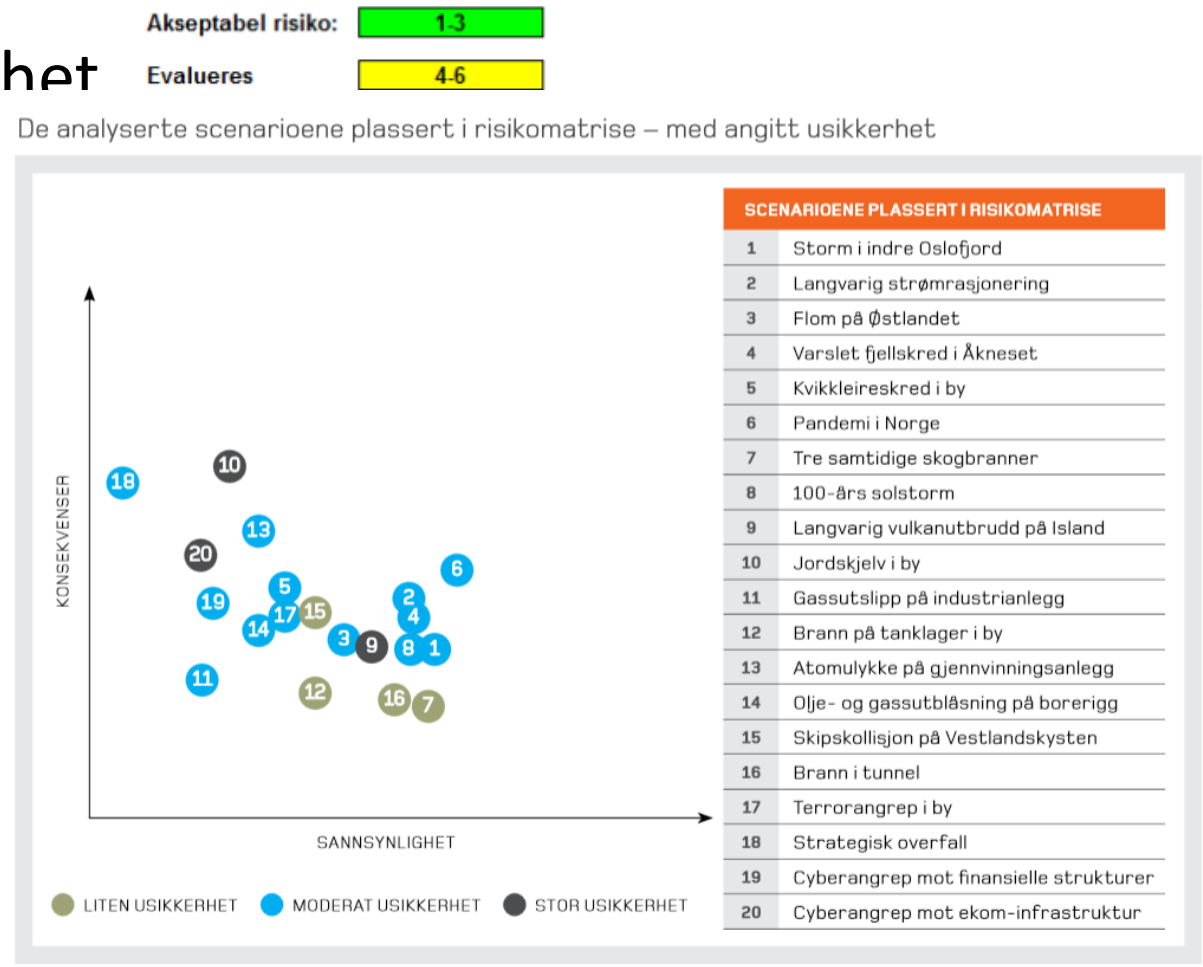


Identifisere og analysere hendelser

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

Risikomatrise

- Risiko: sannsynlighet konsekvens
- Akseptabelt risikon fastsettes
- Sannsynlighet vurd
  - Letthet, motivasjo kapasitet, frekvens
- Konsekvenser
- Eksempler: Box, Nasjonalt risikob 2012 (s17)



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

Andre regelverk med krav til informasjonssikkerhet

- eforvaltningsforskriften, § 15 m.fl.
- Taushetspliktsbestemmelser
  - Forvaltningsloven §13, lignl §3-13
  - Sikkerhetsloven & informasjonssikkerhetsforskriften, objektsikkerhetsforskriften
  - Beskyttelsesinstruksen (kun statsforvaltningen)
- Internkontrollkrav
- Særregulering
  - Helseregisterloven, ikt-forskriften

Forvaltningsloven § 13 flg

- **hindre** at andre får adgang eller kjennskap… § 13
- forsvarlig oppbevaring, § 13c annet ledd
- informerte medarbeidere, § 13c første ledd

Kort om sikkerhetsloven

- Formål, jf. § 1
  - ”motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser…”
- Gradering, § 11 – STRENGT HEMMELIG/ HEMMELIG/ KONFIDENSIELT/ BEGRENSET
  - Skade hvis informasjonen kommer på avveie (ref. § 1)
- Streng need-to-know, § 12
- NSM-godkjenning av informasjonssystemer, § 13, m.v.
- Forskrifter
  - Informasjonssikkerhetsforskrift m.v. med detaljerte sikringsregler
  - Objektsikkerhetsforskriften

Kort om beskyttelsesinstruksen

- Instruks for statsforvaltningen
- Gradering (§ 2)
  - STRENGT FORTROLIG eller FORTROLIG
- Vurderingstema (§ 4)– skade/betydelig skade mht.
  - offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende
- Konsekvenser
  - Strengt need-to-know-prinsipp, § 7 – personlig ansvar
- Elektronisk behandling ”så langt det passer” ihht. deler av informasjonssikkerhetsforskriften etter sikkerhetsloven, jf. § 12

Eforvaltningsforskriften

- Opprinnelig fra 2002
- Viktige endringer 2014 – digitalt førstevalg
- Forankret 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 og informasjonssikkerhet

- Overordnet krav til **internkontroll** på informasjonssikkerhetsområdet, § 15
  - Basert på anerkjente standarder for styringssystem for informasjonssikkerhet
  - Mål og strategier, ref. pof § 2-3
  - Omfang basert på **risiko**, ref. pof § 3-1
  - Fortrinnsvis helhetlig styringssystem
- Publikums digitale kommunikasjon med forvaltningen
  - Kan skje uten bruk av sikkerhetstjenester, med mindre det kreves, § 4
    - Organet må tilby eller peke på løsninger, § 4 nr 4
  - Regulering av innkommende taushetsbelagte opplysninger fra publikum, § 5
- Efvf kap 4-6 – regulering av sertifikater og private nøkler

Digital kommunikasjon til innbyggerne

- Digitale **meldinger** til innbyggerne
  - Kan sendes, efvf § 8
  - Strengere krav til enkeltvedtak og andre viktige meldinger
    - Egnet informasjonssystem (hovedregel)
    - Varsel, gjentatt varsel
    - Logging av innsyn
  - Innbygger kan reservere seg mot å få viktige meldinger, § 9

- Digital **kontaktinformasjon** til innbyggerne
  - Kan lagres, efvf § 31
  - Opprettes med opplysninger fra ID-porten, § 38
  - Kan brukes i forvaltningen, varsling § 29

- Spørsmål?

Kort om elektronisk signatur

- Esignaturloven § 3 definerer tre typer e-signaturer
  - Nr 1: (vanlige)
  - Nr 2: Avanserte
  - Nr 3: Kvalifiserte
- Hva kreves?
  - Prosessrettslig, privatrettslig, forvaltningsrettslig utgpkt
    - Fri bevisbedømmelse, formfrihet, forsvarlig saksbehandling
  - Regelverket gir tidvis avklaring
  - Risikovurdering!
- Merk efvf § 26 nr 2 – langtidslagring
  - arkivet vil kunne bryte signaturen, må da gå god for bindingen
- Revisjon av regelverket på gang – ny forordning vedtatt 2014 (eIDAS)