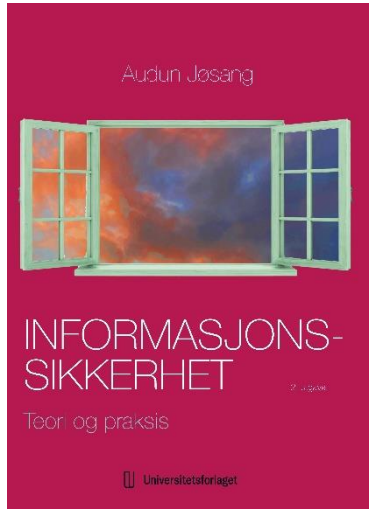
Kapittel 15:
Lover og regelverk for informasjonssikkerhet

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Oversikt

a. Begreper om lover og regelverk
b. Nasjonale lover
c. Regelverk fra EU

Forvaltningen og begrepet «myndighet»

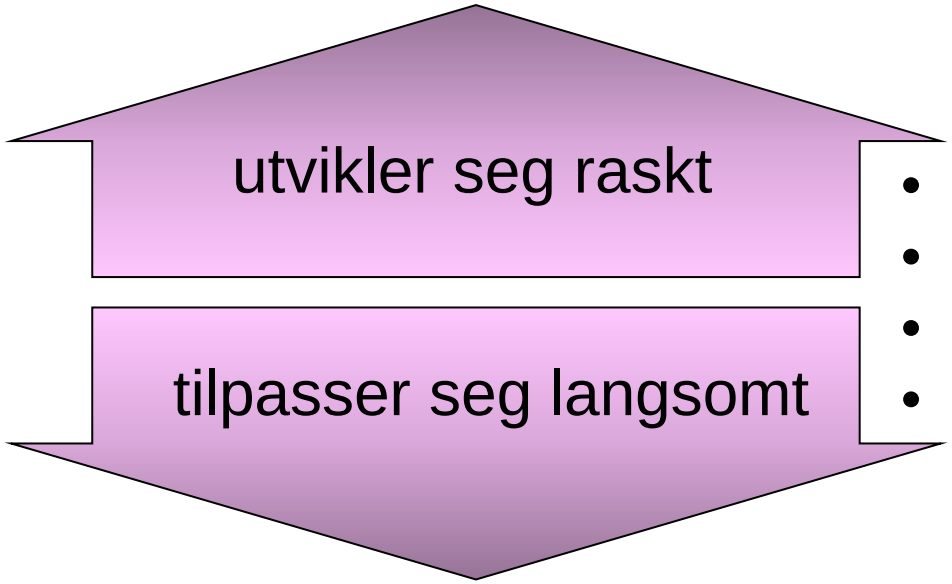
Myndighet er et rettslig begrep

- Det angir evnen til å treffe beslutning med bindende virkning for adressaten (vedtak)
- Et annet ord for myndighet er kompetanse
  - I juridisk fagterminologi brukes ikke kompetanse om kyndighet, slik vi forstår dette ordet i dagligtale
  - Kompetanse brukes om beslutningsevne

Ansvar

- Toppledelsen og eiere er overordnet ansvarlig (regnskapelig) (eng. accountable) for at drift av virksomheten skjer i samsvar med regelverk.
- Ved brudd på etterlevelse av gjeldende regelverk kan virksomheten straffes med overtredelsesgebyrer, som er en virksomhetsstraff. Alternativt, eller i tillegg, kan individer straffes med bøter eller fengsel, som er en personlig straff.
- En ansatt som klikket på en skadelig lenke i en phishing-e-post er ikke overordnet ansvarlig (regnskapelig) om det fører til et sikkerhetsbrudd med betydelig tap.
- Selv om alle i virksomheten har operativt ansvar (eng. responsibility) for informasjonssikkerhet, ligger det overordnede ansvaret (eng. accountability) alltid hos toppledelsen.
- Tvetydigheten av begrepet ansvarlig er ofte en kilde til forvirring, som kan være alvorlig hvis det medfører utvisking og pulverising av det overordnede ansvaret.

Endringstakt



- Teknologi
- Brukere
- Virksomheter
- Lovgivning

- Det er ønskelig med stabil og langsiktig regulering, som betyr at vi må forsøke å lage teknologinøytrale lover og forskrifter.
- Imidlertid kreves ofte svært god teknisk innsikt og fremsynthet for å kunne skape teknologinøytral regulering.

Hierarki av regelverk

Etterlevelse

- Etterlevelse av ulike typer regelverk:
  - Lover og forskrifter
  - Vedtak fra myndighet
  - Kontrakter og avtaler
  - Normer og god forretningsskikk
  - Virksomhetens egen policy og interne regler
- Virksomhetens risikostyring omfatter som regel en type risiko som kalles etterlevelsesrisiko
  - Det har en kostnad å sørge for etterlevelse av ulike regelverk
  - Mangel på etterlevelse kan f.eks. medføre straff, bøter, og sanksjoner som regnes som et tap
  - Virksomheten må vurdere kostnad ved etterlevelse mot risiko for tap ved mangel på etterlevelse

Rapportering til styret om alvorlige sikkerhetshendelser

- «Den daglige ledelse omfatter ikke saker som etter selskapets forhold er av uvanlig art eller stor betydning.»
  - Aksjeloven § 6-14 nr. 2
  - Allmennaksjeloven § 6-14 nr. 2

  https://lovdata.no/dokument/NL/lov/1997-06-13-44/KAPITTEL_6-2#KAPITTEL_6-2
- Mørketallsundersøkelsen 2022 om følger av informasjonssikkerhetshendelser – siste/mest alvorlige hendelse (550 respondenter):
  - Rapportering av sikkerhetshendelser til styret: 43 prosent

  https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2022-web-sider.pdf

Internkontroll

- «…, egenkontroll, system for at enkeltbedrifter og virksomheter skal planlegge og organisere et kontroll- og dokumentasjonssystem for å sikre oppfyllelse av krav fastsatt i lover og forskrifter.» (Store norske leksikon)
- Krav om internkontroll på en rekke områder.
- «Internkontroll» er i stor grad samsvarende med begrepet styringssystem (ledelsessystem)

eForvaltningsforskriften
(hjemlet i forvaltningsloven)

- § 15 *Internkontroll på informasjonssikkerhetsområdet*
  - Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
  - 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.

Sikkerhetslovens formål

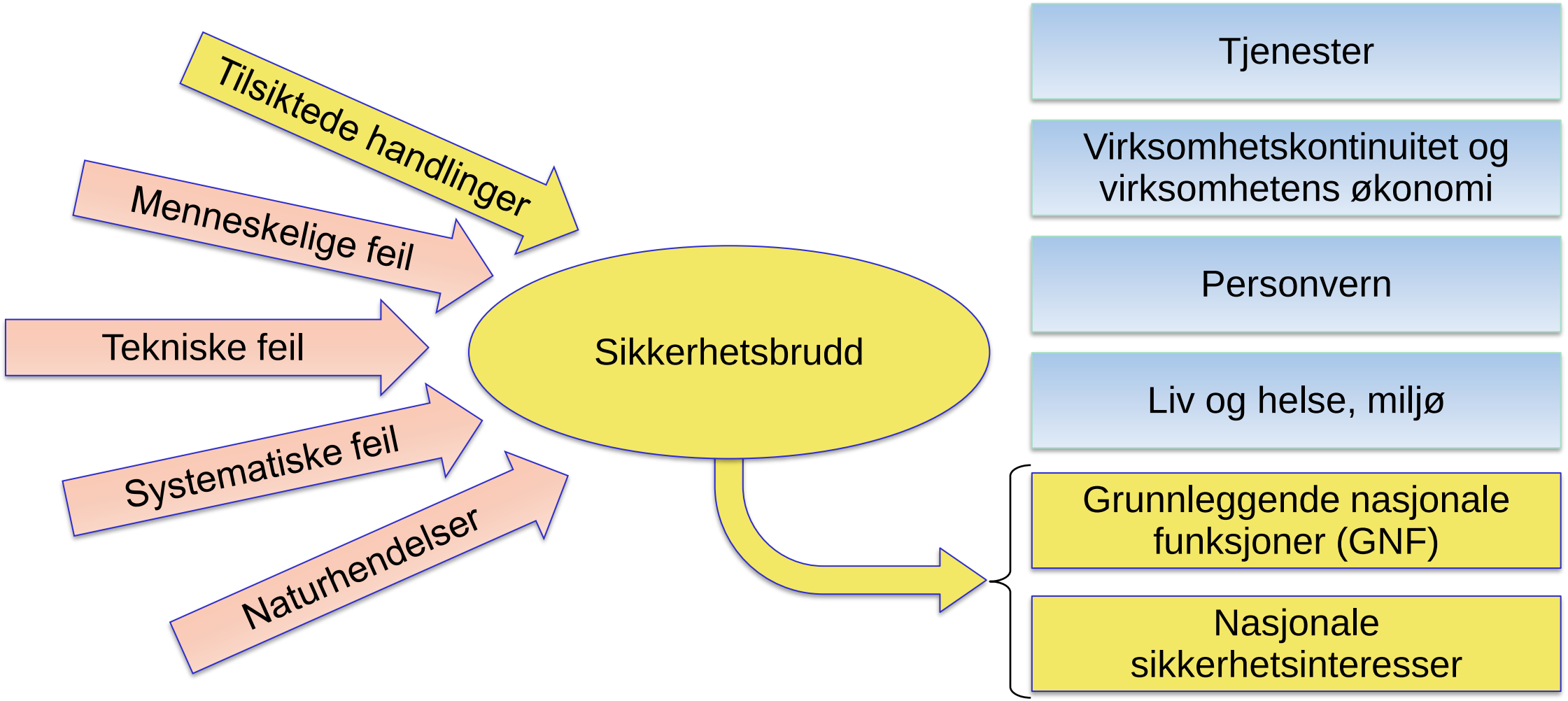
§ 1-1 formål:

Loven skal bidra til

a. å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
b. å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
c. at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Begrepet «sikkerhetstruende virksomhet» er definert som «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser» i § 1-5.4. Med andre ord fokuserer sikkerhetsloven **ikke** på å forebygge brudd på sikkerhet som følge av tekniske feil, menneskelige feil og naturhendelser

Fokus for sikkerhetsloven



Virksomhetssikkerhetsforskriften
Hjemlet i sikkerhetsloven

- **Kapittel 2** – Sikkerhetsstyring
  - **§ 3** Styringssystem for sikkerhet
  - **§ 4** Styringsdokument for det forebyggende sikkerhetsarbeidet
  - **§ 5** Sikkerhetsmål
  - **§ 6** Roller i og ansvar for det forebyggende sikkerhetsarbeidet
  - **§ 7** Ressurser og kompetanse
  - **§ 8** Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon
  - **§ 9** Evaluering og øvelser
  - **§ 10** Gjennomgang av det forebyggende sikkerhetsarbeidet av virksomhetens leder
  - **§ 11** Dokumentasjon av styringssystemet for sikkerhet

Virksomhetssikkerhetsforskriften

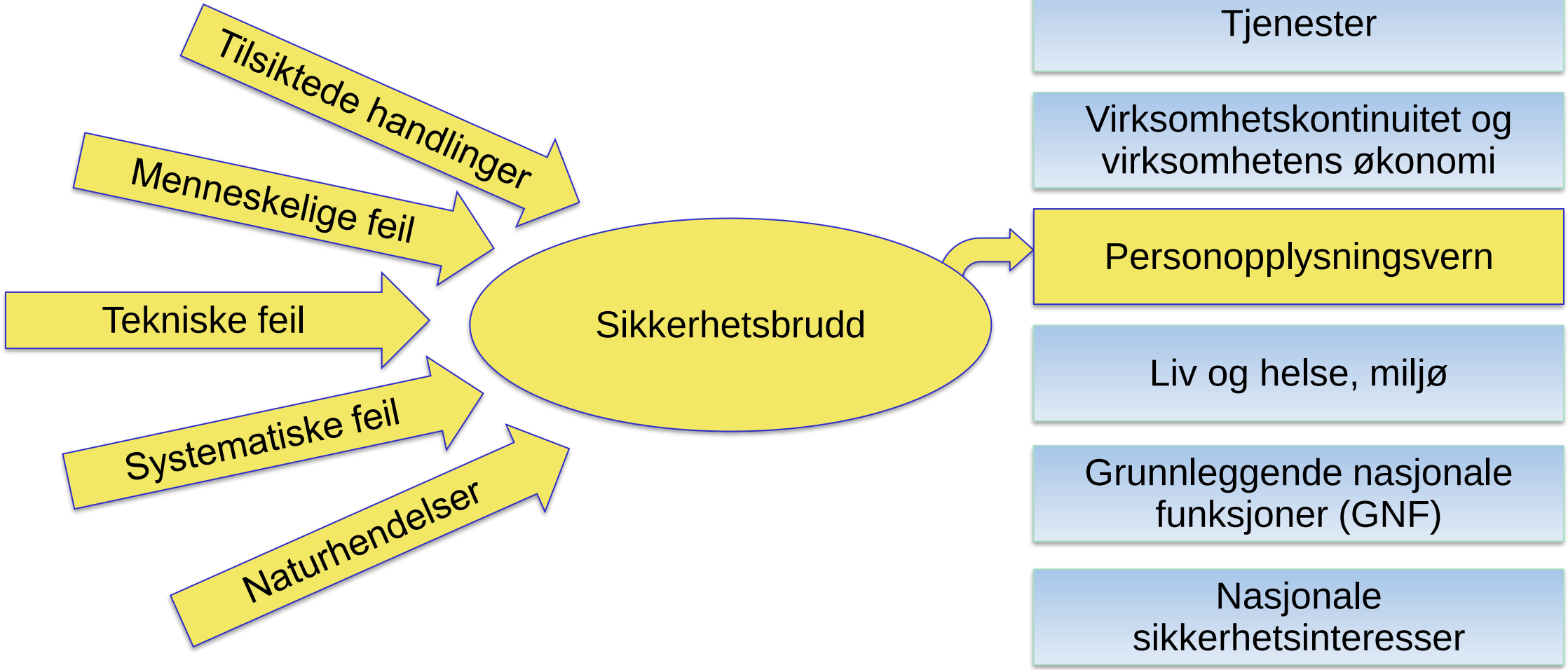
Påbyggingstiltak

- Virksomhetssikkerhetsforskriften § 14
  - «En virksomhet skal planlegge påbyggingstiltak som kan iverksettes dersom økt risiko medfører at det ikke er tilstrekkelig med grunnsikringstiltakene. Påbyggingstiltakene skal kunne iverksettes i løpet av kort tid, og de skal kunne avvikles dersom risikoen reduseres i tilstrekkelig grad» (3. ledd)
  - «Dersom den økte risikoen vedvarer, skal virksomheten vurdere om påbyggingstiltakene skal bli en del av grunnsikringen. I slike tilfeller skal virksomheten planlegge nye påbyggingstiltak» (4. ledd)
- NB! Risikopolitikk kan gi føringer for vurderingen om påbyggingstiltak skal bli en del av grunnsikringen.

Personopplysningslovens formål

- Personopplysningsloven (GDPR) gir bestemmelser for at behandling av personopplysninger skal skje uten uforholdsmessig stor risiko for våre «personvernrettigheter og friheter». (GDPR art. 35)
- Begrepet «rettigheter og friheter» betyr først og fremst rettighetene som beskrives i GDPR art. 12–22, men også rettigheter nedfelt i Grunnloven, i FNs menneskerettigheter og i Den europeiske menneskerettighetskonvensjonen, som blant annet beskriver retten til privatliv, kommunikasjonsvern, ytringsfrihet, religionsfrihet, retten til å organisere seg, og frihet fra diskriminering.
- Personopplysningsloven sier intet om kilder til brudd på personopplysningsvern, dermed dekker den alle typer kilder.
- Se kapittel 10 om personvern.

Fokus for personopplysningsloven (GDPR)



Nasjonale regelverk

- Det fins mange lover og forskrifter med bestemmelser som er direkte rettet mot informasjonssikkerhet
  - I tillegg fins lover og forskrifter som regulerer saksbehandling, taushetsplikt, innsynsrett og lignende forhold som kan påvirke informasjonssikkerhet.
  - Listen over regelverk på de to neste sidene er ikke uttømmende.
  - Regelverkene fins på: https://lovdata.no/

Nasjonale regelverk (1)

- Offentleglova
- Arkivlova
- Forvaltningsloven
- eForvaltningsforskriften
- Plan- og bygningsloven (kapittel 20)
- Sikkerhetsloven
- Beskyttelsesinstruksen (kun stat)
- Personopplysningsloven (Personvernforordningen)
- Ekomloven

Nasjonale regelverk (2)

- Kraftberedskapsforskriften (kapitlene 5, 6 og 7)
- Helseregisterloven (§§ 21 og 22)
- Lov om elektroniske tillitstjenester
- Verdipapirhandelloven (§ 14-7 (7))
- Forskrift om risikostyring og internkontroll (finans)
- Kassasystemlova og kassasystemforskrifta
- Straffeloven
- Tvisteloven (Realbevis er bl.a. *elektronisk lagret materiale*)

«Normen»

- «Normen» er kortformen av *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten*
  - Normen er en bransjenorm som er utarbeidet og som forvaltes av organisasjoner og virksomheter i helsesektoren
- Normen stiller krav som er mer detaljert og som supplerer gjeldende lover og regelverk.
- Normen er en privatrettslig avtale for aktører i helsesektoren
  - Selvreguleringsmekanisme (soft regulation) for helsesektoren

https://www.ehelse.no/normen

Regelverk fra EU

- EU har et omfattende regelverk bestående hovedsaklig av direktiver (eng. directives) og forordninger (eng. acts, regulations).
- Et EU-direktiv skal implementeres i nasjonale lover med omtrent samme innhold.
- Hvis Norge tar inn et nytt direktiv, kan det hende at Norge allerede har lover som dekker direktivet helt eller delvis.
- En EU-forordning skal som hovedregel implementeres som nasjonal lov nøyaktig slik den er artikulert av Europakommisjonen, bare oversatt til det nasjonale språk.
- EØS-landene bestemmer sammen om et EU-direktiv eller en EU-forordning skal gjelde i EØS-landene, som dermed betyr at det blir tatt inn i selve EØS-avtalen.
- Her gjelder prinsippet om alle eller ingen, det vil si at Norge ikke kan bestemme alene om vi skal eller ikke skal ta inn et EU-direktiv eller en EU-forordning.

NIS2-direktivet (Network and Information Security nr. 2)

- NIS2-direktivet gjelder fra 2023, og erstatter det tidligere NIS-direktivet fra 2016. Da Norge og EØS-landene allerede har innlemmet det forrige NIS-direktivet, betyr det at Norge også vil innlemme NIS2, som vil skje gjennom en ny lov kalt «lov om digital sikkerhet». Elementer i NIS2 er blant annet:
  - skape samarbeid om en europeisk infrastruktur for håndtering av cyberkrise gjennom EU-CyCLONe (European Cyber Crises Liaison Organisation Network)
  - harmonisere sikkerhetskrav og rapporteringsplikter
  - sørge for at medlemslandenes cybersikkerhetsstrategier dekker sikkerhet i leveransekjeder, sårbarhetshåndtering, sikkerhet i kjernenettet og generell digital sikkerhetskultur og cyberhygiene
- Lov om digital sikkerhet (NIS2-direktivet) er en parallell til sikkerhetsloven, som skal gjelde for alle virksomheter, ikke bare «grunnleggende nasjonale funksjoner»

Andre regelverk fra EU

- GDPR (General Data Protection, Regulation), 2018 (se kapittel 10)
- eIDAS-forordningen (electronic IDentification And trust Services), 2014
- eIDAS heter på norsk lov om elektroniske tillitstjenester. Forordningen er per 2023 under revisjon. eIDAS er beskrevet i avsnitt 8.7.
- PSD2 (betalingstjenestedirektivet), 2019
  - PSD2 (Payment Services Directive nr. 2) regulerer betalingstjenester i EUs indre marked, og er implementert bl.a. i finansforetaksloven og forskrift om betalingstjenester. Et viktig aspekt er at direktivet åpner for at bankkunder kan benytte andre aktører enn de tradisjonelle bankene for å utføre finansielle operasjoner
- Ekomdirektivet (Directive for establishing a European Electronic Communications Code), 2021
  - Ekomdirektivet er implementert i ekomloven, som har til formål å stimulere investeringer i og utrulling av i høyhastighetsnett i hele EU, styrke det indre marked og styrke forbrukerrettigheter.

Andre regelverk fra EU

- Cybersikkerhetsforordningen (Cybersecurity Act), 2023
  - Det noe pretensiøse navnet på denne forordningen er ikke lett å tolke intuitivt. Forordningen dreier seg hovedsakelig om ENISA (European Union Agency for Cybersecurity), som gjennom forordningen får en permanent status med spesifikt mandat. ENISA ble opprettet i 2004 som European Network and Information Security Agency, men hadde ingen permanent status og var avhengig av årlig budsjettbevilgning fra Europakommisjonen. Cybersikkerhetsforordningen gir ENISA permanent status, et styrket budsjett, flere ansatte og et styrket mandat.
- Cyber Resilience Act (under arbeid)
  - Forslaget til Cyber Resilience Act fokuserer på å sette sikkerhetskrav til digitale produkter, både maskinvare og programvare. Cyber resilience kan oversettes med cybertåleevne, eller anglifisert som cyberresiliens. Denne forordningen kan knyttes sammen med sertifisering av IKT-produkter som er en del av cybersikkerhetsforordningen beskrevet over.

Slutt på presentasjon