



# Status quo i endring...



«Den sikkerhetspolitiske situasjonen er i kraftig **endring**. Det innebærer nye og **sammensatte** trusler som krever **nye** sikkerhetstiltak og kunnskapsutvikling.»

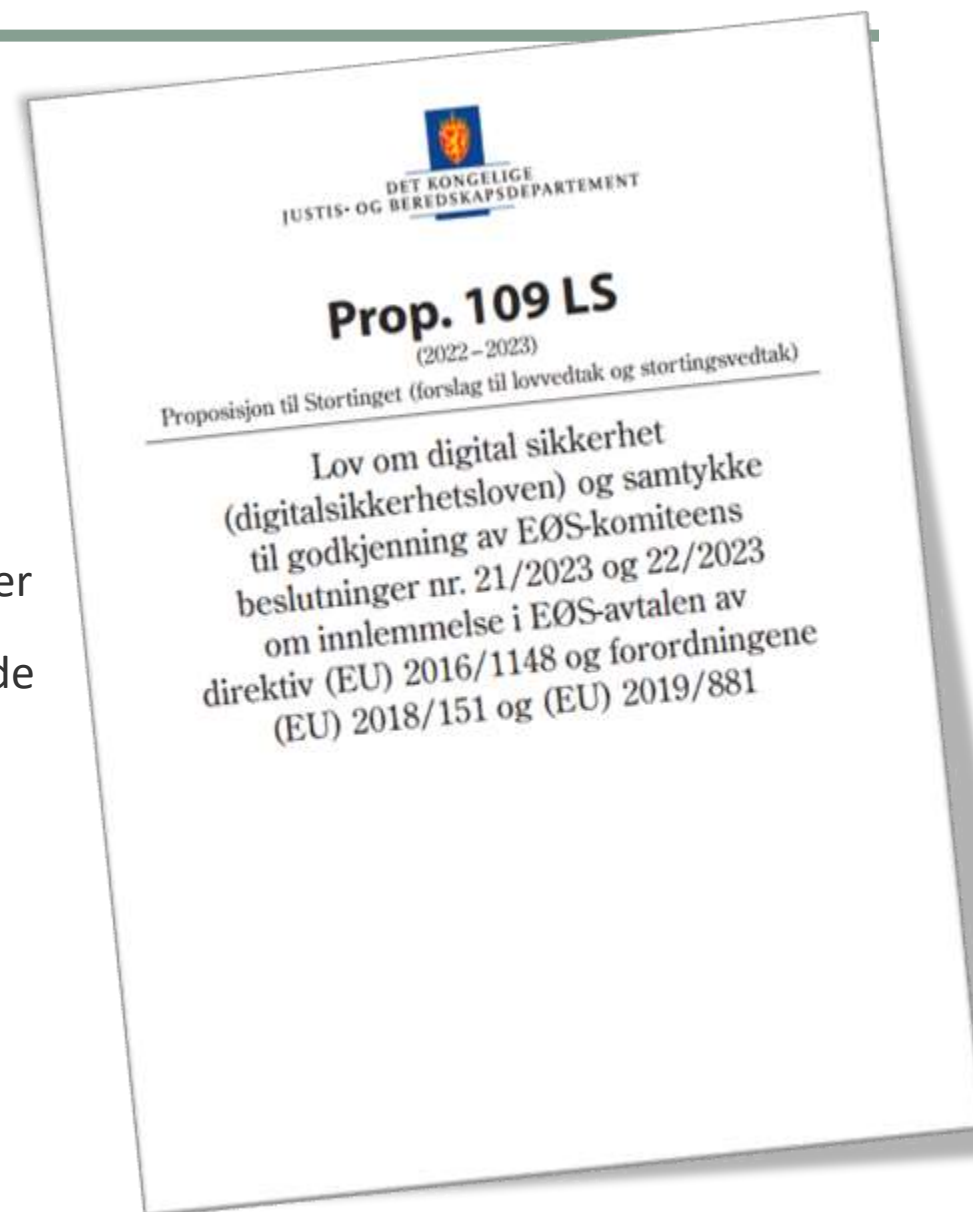


– Vi lever i en ny tid. Vår nye hverdag er ikke lenger «dyp fred». Nye trusler nå og i årene fremover krever at vi tar grep. Faren er at **trusselaktørenes bruk av teknologi kan utvikle seg raskere enn de åpne demokratiens evne til å beskytte seg**. Vi trenger en trusselbasert «føre var»-tilnærming for å hindre at fiendtlige aktører får fotfeste i Norge, sier Sofie Nystrøm, direktør i Nasjonal sikkerhetsmyndighet (NSM).

# 2023: Norge får sin første lov om digital sikkerhet



- Prop. 109 LS → 5. mai 2023
- Basert på NIS (**NIS1**)
  - Network and Information Security Directive
    - Vedtatt i EU-parlamentet 6. juli 2016 → 9. mai 2018
    - GDPR Regulation: 14. april 2016 → 25. mai 2018
- Utvalgte virksomheter vil nå bli forpliktet til å overholde digitale sikkerhetskrav og å **varsle** om alvorlige digitale hendelser.
- Det vil i første omgang gjelde for tilbydere av **samfunnsviktige** tjenester innen energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur, samt tilbydere av de digitale tjenestene digitale markedsplasser, skytjeneste, og digitale søkemotorer.
- Loven vil bli **utviklet** over tid for å gjøre norske virksomheter mer ansvarlige og sikre gjennomføring av nasjonale råd og anbefalinger.
  - IKKE implementert i Norge (før i 2023) – NSM utpekt som myndighet
  - Ingen konkrete rammer for sanksjoner (lokalt)
  - **Krav implementering av NIS1 for å implementere NIS2...**





Begge er ment å sikre våre grunnleggende (digitale) rettigheter og friheter

...og begge opererer med sanksjoner i form i form av gebyr og bøter...

- **GDPR: 20 millioner Euro eller 4% av global omsetning**
- **NIS2: 10 millioner Euro eller 2% av global omsetning**
  - Vedtatt 16. januar 2023 → 21 måneder egen lovgivning (17. oktober 2024)
- GDPR overtredelsesgebyr 2022 (i millioner €):
  - Meta (€ 405), Meta (€ 265), Clearview (€ 20), Clearview (€ 20), Clearview (€ 20), Meta Meta (€ 17), Google (€ 10)...
  - 2023? Grindr (€ 6)



# Personvern forutsetter «Sikkerhet ved behandlingen» = KIT(R)



Art 32.1(b) - Evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene



Ikke bare «et godt råd»,  
men norsk lov...

...hva betyr det i  
praksis?

# Noen utvalgte hendelser 2019-2021...



- Hydro (2019)
- Stortinget (2020)
- Østre Toten (2021)



af  Datatilsynet

## Dramaet er ikke over: Denne informasjonen kan være på avveie



# Når en virksomhet har hatt et datainnbrudd, har den ikke da allerede fått sin straff?



- Andre myndigheter fokuserer på angrepet og trusselaktøren (Politiet, NSM, NKOM, CERTs...)
  - Datatilsynet kan ha en rådgivende rolle hvis personopplysninger er involvert
- Datatilsynets oppgave er å se på den som er ansvarlig for personopplysningene
- **Datatilsynets fokus er borgernes perspektiv**
  - Hvordan har virksomheten som forvalter våre personopplysninger ivaretatt sitt ansvar og forpliktelser?
- Få gebyrsaker, men alvorlige
- 2200 avvikssaker i 2021, 9 overtredelsesgebyr (0,5%)
  - Gebyrsakene kjennetegnes av svakheter med sikkerheten i den virksomheten som forvalter mine og dine personopplysninger når sikkerhetshendelsen inntraff, uansett angriper eller årsak til hendelsen

## DEBATT Bøter etter datainnbrudd

### Når en virksomhet har hatt et datainnbrudd, har den ikke da allerede fått sin straff?

Derfor straffer Datatilsynet virksomheter som har blitt hacket.

16. mars 2022

# Noen observasjoner om hendelsessvektorer



Forskjeller, men ofte karakter av ransomware → løsepengeangrep → digital utpressing

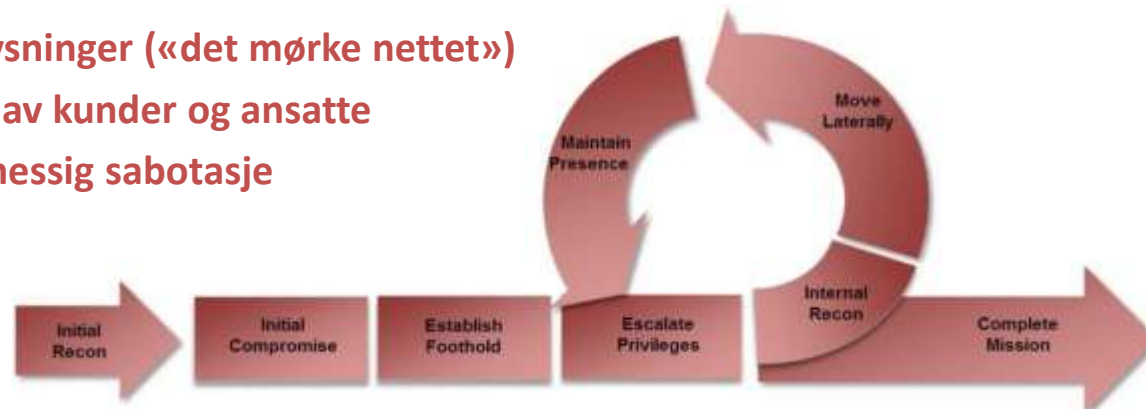
- **Typisk angrepsvektor:**

- Epost (passord uten sterk autentisering/2-faktor/MFA)
- Tilgang via:
  - Phishing (gyldig bruker klikker på lenker)
  - «Brute forcing» / Gjetting
  - Gjenbruk fra andre tjenester («Credential Stuffing»)
  - Lurer bruker til å oppgi passord på falske tjenester

Installerer malware/ransomware lokalt → kobler mot «kommandosentral» som tar over

- «Automatiske» angrep **VS** APT (Advanced Persistent Threat)-lignende angrep:

- Øyeblikkelig kryptering, sletting → kontrollerte bevegelser over tid (uthenting, sletting, kryptering)
  - Salg av opplysninger («det mørke nettet»)
  - Trakassering av kunder og ansatte
  - Forretningsmessig sabotasje



# Noen observasjoner om svakheter i systemene



- Brukerkonti kun passord / interne brukerkonto kun passord (2.6.7)
- Administratorkonti kun med passord
- Tjenester med statiske passord
- Mangler ved intern soneoppdeling (2.5)
- Manglende oversikt på utgående trafikk og interntrafikk
  - Interne tjenester kan snakke med eksterne tjenester («VG-testen»)
- Manglende logging og analyse (3.2)
  - Av «lovlig» trafikk
  - Av utgående trafikk
  - Av intern trafikk
  - Manglende (realtid) analyse av logger («brannalarm»)
    - Manglende dokumentasjon i etterkant («hva skjedde?», «kom persondata på avveie?»)
- Manglende test av sikkerhetskopier og strategi for gjenoppretting i stressituasjoner → Disaster Recovery (2.9)
- Manglende beskyttelse av sikkerhetskopier
  - Tilgangsstyring
  - «Galvanisk» skille
  - Kryptering
  - **Sletting**



NSM Grunnprinsipper

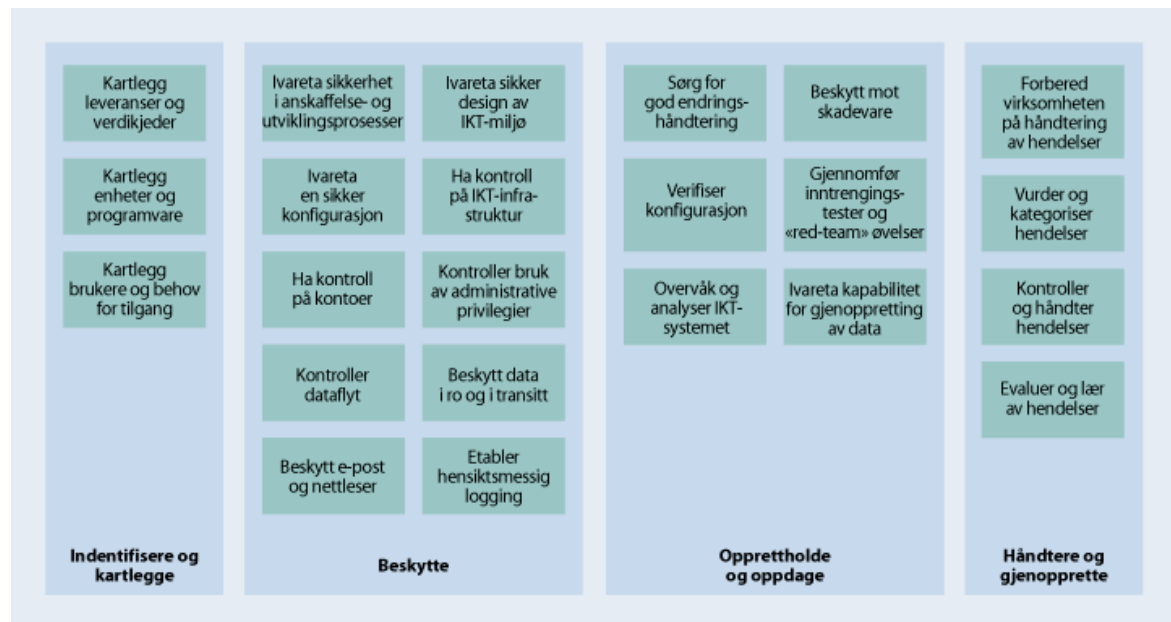
# Hvorfor er man ikke forberedt?

---



- **Ikke effektiv formidling av risiko til de som sitter på pengene → ledelsen**
  - Manglende prioriteringer og investeringer i IT-sikkerhet og personvern
- **Manglende forankring i ledelsen**
  - Informasjonssikkerhet er ikke tilstrekkelig integrert i de generelle styringssystemene
  - Personvern er ikke tilstrekkelig integrert i de generelle styringssystemene
  - Manglende prosesser for informasjonssikkerhetsstyring
  - Manglende prosesser for styring av personopplysningssikkerhet

# Kilder til veiledning for konkrete tiltak [for offentlig virksomhet]



- NSM – Grunnprinsipper versjon 2.0
  - NSM Grunnprinsipper versjon 3.0
  - NIS (Network and Information Security Directive)

Digdir – Internkontroll i praksis -  
Informasjonssikkerhet

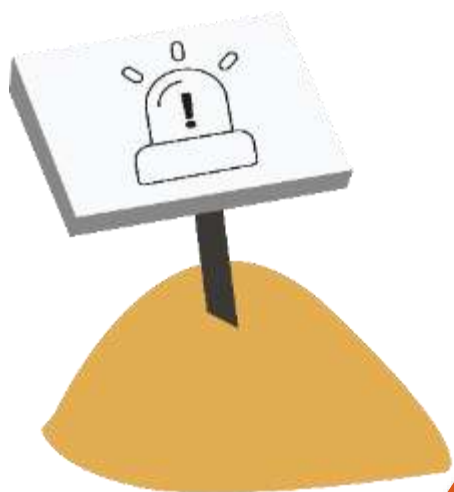


Vi «banker på». Hva nå?

---



## Når må virksomheten sende melding om avvik til Datatilsynet?



Med andre ord en lav terskel for å melde til Datatilsynet

«Ved brudd på personopplysningssikkerheten ..., med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter.»

Definisjon: «*brudd på personopplysningssikkerheten*» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig (uautorisert) spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet (art. 4 nr. 12)

Art. 33

# Hva skjer når Datatilsynet banker på døra?

---



*(Vi banker som regel på postkassa...)*

- Vurdering av initiell melding
- Det store flertallet av avvikssaker avsluttes, mens andre er mer alvorlige og krever mer oppfølging.
- Innhenting av ytterligere informasjon fra den behandlingsansvarlige
  - Aktiv dialog
- Krav om redegjørelse – pålegg om å gi Datatilsynet informasjon om brudd på personopplysningssikkerheten eller forhold som fremgår av klage, jf. personvernforordningen artikkel 58.

# Hva ser Datatilsynet etter?



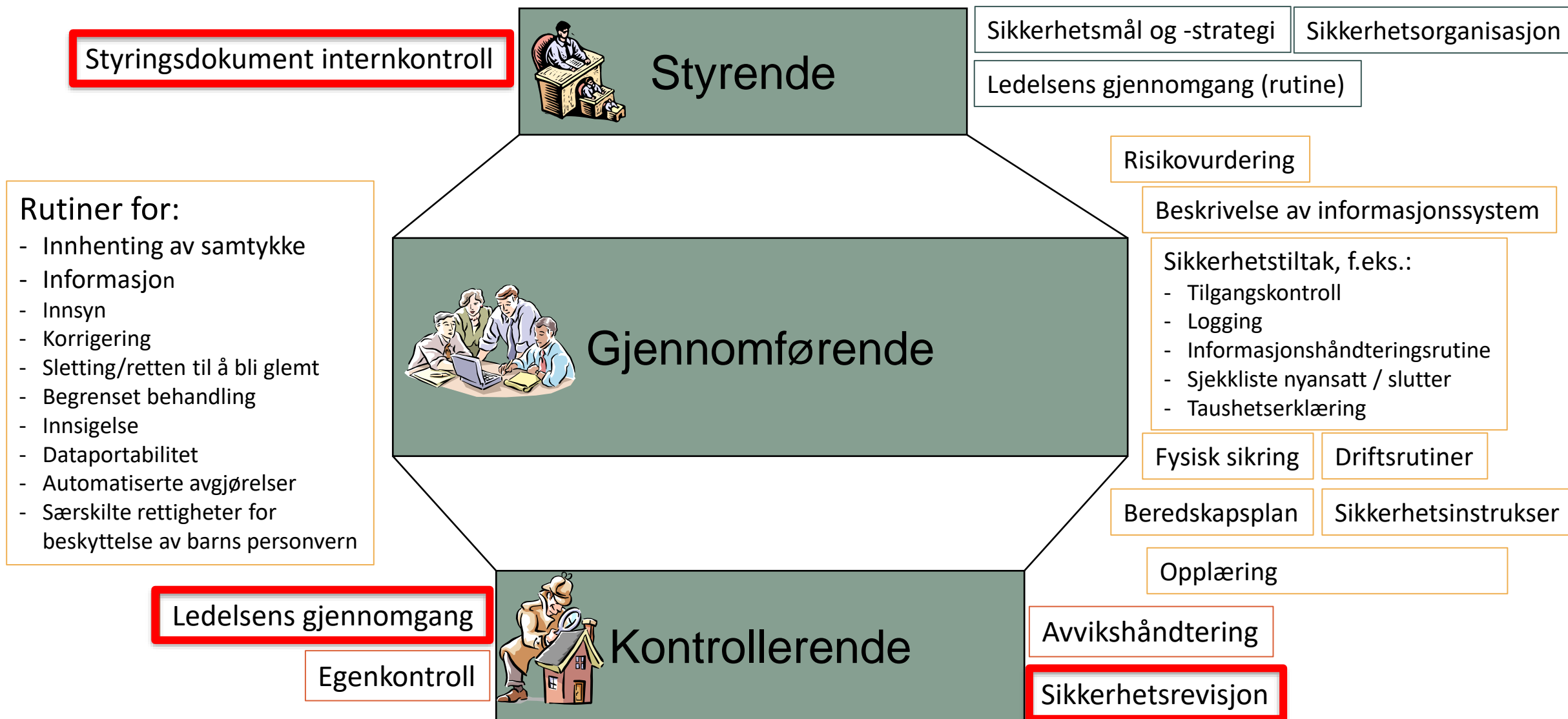
- Ansvarlighetsprinsippet, jf. artikkel 5 nr. 2. (påvise ansvar jf. 5.1.f – sikkerhet ved behandlingen)
- Har meldingen et innhold som svarer til kravene i artikkel 33? (skjema Altinn) Hvis ikke, krav om ytterligere informasjon evt. redegjørelse (pålegg om å gi Datatilsynet informasjon)
- Gikk det lang tid før hendelsen ble oppdaget og deretter meldt til Datatilsynet? (72-timer fristen)
- Konteksten personopplysningene er blitt behandlet (inkl. type virksomhet, kategorier personopplysninger og registrerte)
- Hvor alvorlige er konsekvensene for registrertes rettigheter og friheter, og er det mange berørte?
- Har man kontroll med hvilken informasjon som er berørt og hvordan den er berørt? (logging)
- Har virksomheten hatt tilsvarende brudd tidligere?
- Er det gitt tilstrekkelig informasjon til de registrerte?
- Er de igangsatte tiltakene tilstrekkelige og effektive?
- Indikerer meldingen andre brudd på personvernlovgivningen enn selve avviket? (f.eks. sletting)
- Indikerer bruddet mangler ved internkontroll og informasjonssikkerhet? \*

- \* • Er det etablert systemer for hendelseshåndtering?
- Er det dokumenterte prosesser for informasjonssikkerhetsstyring inkl personopplysningssikkerhet
- Er informasjonssikkerhetsarbeid integrert i den generelle internkontrollen/styringssystemer

→ indikasjoner på at virksomheten ikke har forstått sitt ansvar

→ indikasjoner på at virksomheten ikke har lært 15 av tidligere hendelser

# Dokumentasjon av internkontroll – dokumentstruktur



# Tilsyn i 93(!) kommuner og 5 fylkeskommuner



## 4. Krav om redegjørelse

Vi ber kommunen sende oss følgende:

- 4.1 Kommunens behandlingsprotokoll, jf. personvernforordningen artikkel 30
- 4.2 Oversikt over kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2
- 4.3 En kort beskrivelse av kommunens overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes
- 4.4 Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, jf. personvernforordningen artikkel 32
- 4.5 Kommunens eventuelle overordnede sikkerhetsstrategi
- 4.6 Oversikt over eventuelle IS-samarbeid med andre kommuner
- 4.7 Styrende retningslinjer for autentiseringsløsninger i kommunen
- 4.8 Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer, jf. personvernforordningen artikkel 32.1.c)
- 4.9 Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. personvernforordningen artikkel 32.1.d)



## Tilsyn i kommuner og fylkeskommuner

Vi har satt i gang et større tilsynsarbeid med nærmere hundre norske kommuner og fylkeskommuner sin ivaretagelse av personopplysningssikkerheten.



I den andre fasen vil Datatilsynet på bakgrunn av svarene vi mottar i brevkontrollene, gjennomføre **et antall stedlige tilsyn**.

[www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/tilsyn-i-kommuner-og-fylkeskommuner/](http://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/tilsyn-i-kommuner-og-fylkeskommuner/)

## Håndtering av personvernet ved digitale angrep

### Innhold

1. [Innledning](#)
2. [Tjenestenektangrep \(DDoS\)](#)
3. [Phishing og e-postangrep](#)
4. [Direktørsvindel](#)
5. [Utpressingsangrep](#)
6. Hva gjør dere?

## Hva gjør dere?

Hvis dere oppdager en pågående sikkerhetshendelse, er det viktig at dere prioriterer håndtering av selve hendelsen og får oversikt over situasjonen:

- [Ta i bruk planen deres for krisehåndtering](#) hvis dere har det, og opprett krisestab.
- Vurder å involvere tredjeparter for å håndtere hendelsen hvis dere ikke har kompetanse til å gjøre det selv. Se [Nasjonal sikkerhetsmyndighet sin liste over godkjente aktører \(nsm.no\)](#) og [Næringslivets Sikkerhetsråds nødplakat for digitale angrep \(nsr-org.no\)](#).
- Det finnes en rekke tilbydere av CERT-tjenester Computer Emergency



### Håndtering av avvik

Meld bruddet her ([altinn.no](http://altinn.no))

- › Meld brudd på personopplysningssikkerheten til Datatilsynet
- › Hva er et brudd på personopplysningssikkerheten?
- › Hvilke brudd skal meldes til Datatilsynet?

- › Hvem kan melde bruddet til Datatilsynet?
- › Informasjon til de berørte
- › Hvordan følge opp bruddet internt?
- › Håndtering av personvernet ved digitale angrep

# Takk for oppmerksomheten!



postkasse@datatilsynet.no  
Telefon: +47 22 39 69 00

[datatilsynet.no](https://www.datatilsynet.no)  
[personvernbloggen.no](https://www.personvernbloggen.no)