Felles anbefalinger og personopplysningsvern

Eirik Gulbrandsen | Spesialrådgiver seksjon Teknologi, Sikkerhet og Tilsyn

Datatilsynet

Hva er de viktigste forutsetninger for å lykkes?

Forståelse av digital risiko og konsekvenser

Tilstrekkelig prioritet og ressurser

Hva er den viktigste faktoren for tilstrekkelig prioritering og ressurser?

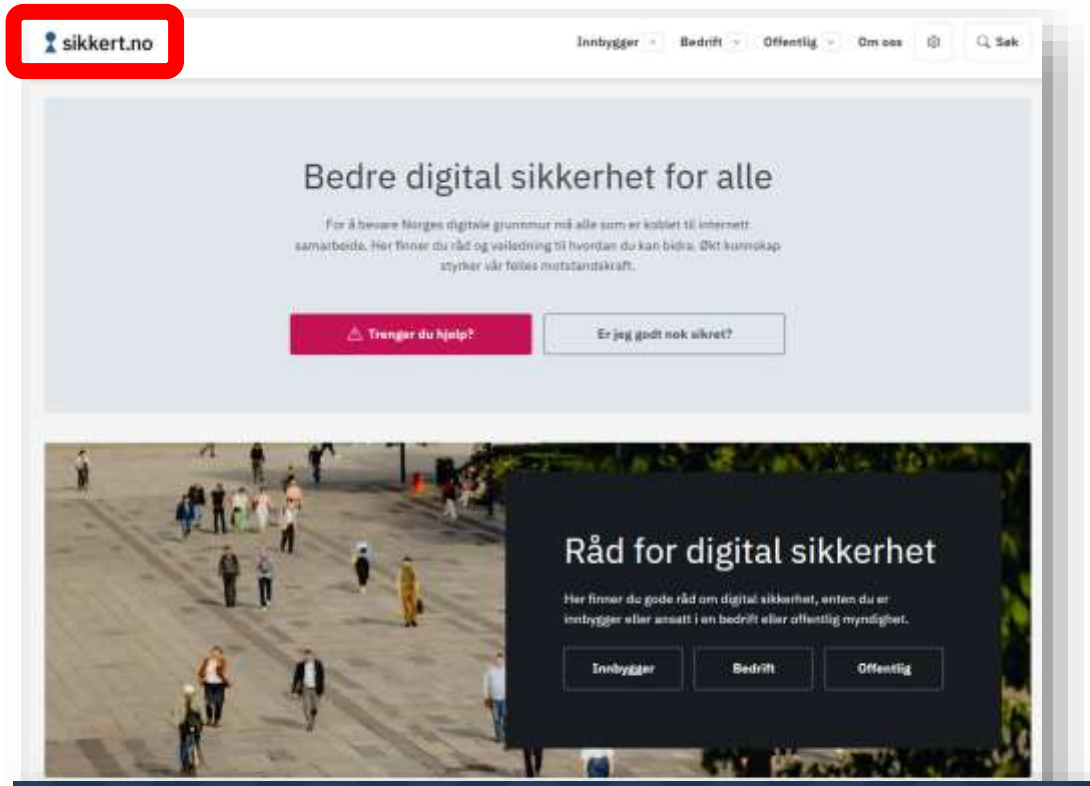
De som styrer økonomien = ledelsen

Hva er verktøyet for å sikre at ledelsen jobber systematisk med sikkerhet?

Bøter og sanksjoner

GLEM ~~lederforankring~~ – etabler lederansvar!

- velfungerende styringssystemer er en forutsetning
- etablere styringssystemer med indikatorer som betyr noe for de som styrer
- skap bestillerkompetanse!


sikkert.no
Innbygger
Bedrift
Offentlig
Om oss
Søk
Bedre digital sikkerhet for alle
For å bevare Norges digitale grunnmur må alle som er koblet til internett samarbeide. Her finner du råd og veiledning til hvordan du kan bidra. Økt kunnskap styrker vår felles motstandskraft.
Trenger du hjelp?
Er jeg godt nok sikret?
Råd for digital sikkerhet
Her finner du gode råd om digital sikkerhet, enten du er innbygger eller ansatt i en bedrift eller offentlig myndighet.
Innbygger
Bedrift
Offentlig


Flerfaktorautentisering må settes opp riktig
Vi anbefaler virksomheter å gå over til passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering.
Se hvordan du og din virksomhet kan beskytte dere (nsm.no)

Sterk autentisering

PASSORD ER DØDT

PASSORD ER IKKE LENGER TILSTREKKELIG

- Svak autentisering er primær angrepsvektor i mange avviksmeldinger
- Mange 2-faktor / multifaktorløsninger er ikke gode nok og blir omgått
- *«vi har slått på MS365 MFA og skjønner ikke hvordan angriper kom seg inn»*

- Mest hackede 2-faktor? Microsofts «legacy» 2-faktor (som de fleste benytter)
- Microsoft «tvinger» nå overgang til Passkeys = Tilgangsnøkler = Fido2/Webauth

=

«Phishingresistent autentisering»

nsm.no/regelverk-og-hjelp/rapporter/flerfaktorautentisering

Sterk autentisering

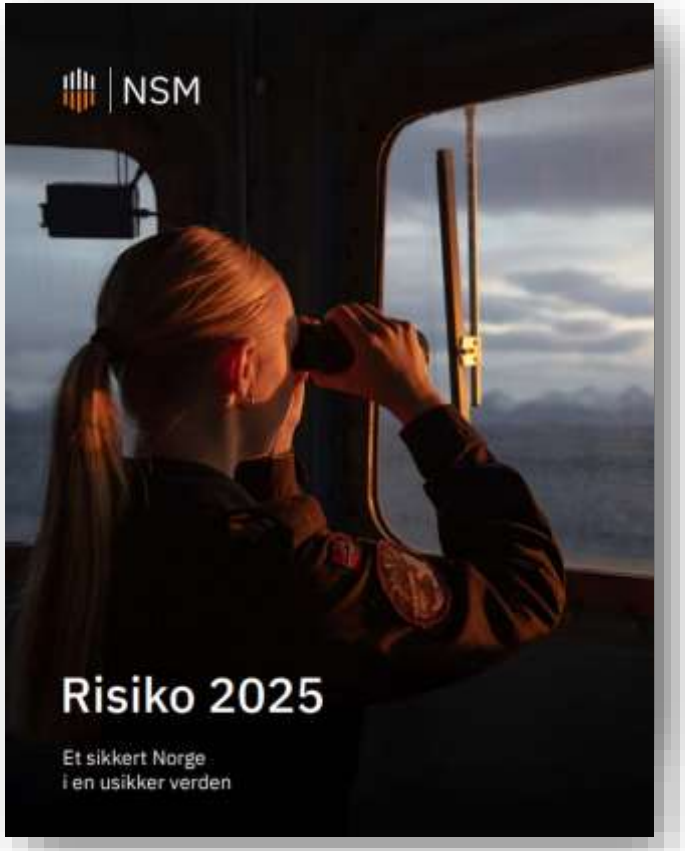
«LEGACY» MFA LIGGER PÅ DØDSLEIET

IKKE ALL MFA ER LENGER TILSTREKKELIG

Digitalsikkerhetsforskriften § 10. Teknologiske sikkerhetstiltak

Teknologiske sikkerhetstiltak skal minst omfatte

a. sterk autentisering for adgang til nettverk og informasjonssystemer



Overgang til phishingresistent autentisering

NSM anbefaler virksomheter å gå over til passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering. I 2024 har NSM og sektorvise responsmiljøer registrert en rekke phishingkampanjer der målet var økonomisk vinning, ofte via fakturasvindel. Kampanjene lar seg gjennomføre fordi virksomheter ikke påkrever phishingresistent autentisering.

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Bedre digital sikkerhet for alle

For å bevare Norges digitale grunnmur må alle som er koblet til internett samarbeide. Her finner du råd og veiledning til hvordan du kan bidra. Økt kunnskap styrker vår felles motstandskraft.

Trenger du hjelp? | Er jeg godt nok sikret?

Råd for digital sikkerhet

Her finner du gode råd om digital sikkerhet, enten du er innbygger eller ansatt i en bedrift eller offentlig myndighet.

Innbygger | Bedrift | Offentlig

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Styring av informasjonssikkerhet og personopplysningsvern

Hjem › Offentlig › Styring av informasjonssikkerhet og personopplysningsvern

Offentlig

Introduksjon

Offentlige virksomheter og deres ledere har ansvar for å styre risiko for sine oppgaver og tjenester. Å styre informasjonssikkerhet og personopplysningsvern er en del av dette, og bør være integrert i virksomhetsstyringen.

→

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

→

Ha oversikt og prioritere (OP)

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt...

→

Vurdering av risiko (RV)

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko knyttet til informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde, og vite hvilke risikoer...

→

Håndtering av risiko

Måling, evaluering og

digitalsikkerhetsloven

Overvåking og

tjenester

Veileder i digitalsikkerhetsloven og -forskriften

NSM har utarbeidet veiledning i digitalsikkerhetsloven og -forskriften for virksomheter.

→

Slik fungerer tjenesten:

Flerfaktorautentisering må settes opp riktig

Vi anbefaler virksomheter å gå over til passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering.

Se hvordan du og din virksomhet kan beskytte dere (nsm.no)

sikkert.no

Innbygger | Bedrift | Offentlig | Om oss | Søk

Styring av informasjonssikkerhet og personopplysningsvern ?

Hjem » Offentlig » Styring av informasjonssikkerhet og personopplysningsvern

Offentlig

Introduksjon

Offentlige virksomheter og deres ledere har ansvar for å styre risiko for sine oppgaver og tjenester. Å styre informasjonssikkerhet og personopplysningsvern er en del av dette, og bør være integrert i virksomhetsstyringen.

→

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

→

Ha oversikt og prioritere (OP)

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt...

→

Vurdering av risiko (RV)

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko knyttet til informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde, og vite hvilke risikoer...

→

Håndtering av risiko

Måling, evaluering og

Overvåking og

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

Dette skal gjøres ved å lage en plan for styringsaktiviteter som gjennomføres systematisk i hele virksomheten.

Virksomhetens ledelse skal sørge for å

- etablere og følge opp styringsaktivitetene som en del av virksomhetsstyringen
- gi føringer for styringsaktivitetene og det øvrige arbeidet med informasjonssikkerhet og personopplysningsvern
- sørge for tilstrekkelig ressurser til arbeidet med informasjonssikkerhet og personopplysningsvern
- følge opp at styringsaktivitetene fungerer godt og gjøre nødvendige endringer ved behov
- følge opp at virksomhetens oppgaver og tjenester har tilstrekkelig informasjonssikkerhet og personopplysningsvern

LS-1 Gi føringer

Virksomhetsledelsen skal gi føringer for hvordan styringen av informasjonssikkerhet og personopplysningsvern skal fungere som en del av den helhetlige styringen av virksomheten. Innholdet i føringene bør være basert på virksomhetens interne og eksterne rammebetingelser. Føringene skal inneholde overordnet beskrivelse av formålet med virksomhetens informasjonsbehandling, og hvilken betydning den har for virksomhetens oppgaver og tjenester.

Virksomhetsledelsen har ansvaret for å gi føringer for

- struktur og innhold i styringsaktivitetene
- roller og myndighet i arbeidet med styring av informasjonssikkerhet og personopplysningsvern
- delegering av oppgaver for å styre informasjonssikkerhet og personopplysningsvern til ledere som er mål- og resultatansvarlige for et område (risikoeiere).

Innhold

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

Dette skal gjøres ved å lage en plan for styringsaktiviteter som gjennomføres systematisk i hele virksomheten.

Virksomhetens ledelse skal sørge for å

- etablere og følge opp styringsaktivitetene som en del av virksomhetsstyringen
- gi føringer for styringsaktivitetene og det øvrige arbeidet med informasjonssikkerhet og personopplysningsvern
- sørge for tilstrekkelig ressurser til arbeidet med informasjonssikkerhet og personopplysningsvern
- følge opp at styringsaktivitetene fungerer godt og gjøre nødvendige endringer ved behov
- følge opp at virksomhetens oppgaver og tjenester har tilstrekkelig informasjonssikkerhet og personopplysningsvern

LS-1 Gi føringer

Virksomhetsledelsen skal gi føringer for hvordan styringen av informasjonssikkerhet og personopplysningsvern skal fungere som en del av den helhetlige styringen av virksomheten. Innholdet i føringene bør være basert på virksomhetens interne og eksterne rammebetingelser.
Føringene skal inneholde overordnet beskrivelse av formålet med virksomhetens informasjonsbehandling, og hvilken betydning den har for virksomhetens oppgaver og tjenester.

Virksomhetsledelsen har ansvaret for å gi føringer for

- struktur og innhold i styringsaktivitetene
- roller og myndighet i arbeidet med styring av informasjonssikkerhet og personopplysningsvern
- delegering av oppgaver for å styre informasjonssikkerhet og personopplysningsvern til ledere som er mål- og resultatansvarlige for et område (risikoeiere).

Innhold

LS-1 Gi føringer

Virksomhetsledelsen ska
informasjonssikkerhet og
den helhetlige styringen a
basert på virksomhetens
Føringene skal inneholde
virksomhetens informasjo
virksomhetens oppgaver

Virksomhetsledelsen har

- struktur og innhold i styringsaktivitetene
- roller og myndighet i arbeidet med styring av informasjonssikkerhet og personopplysningsvern
- delegering av oppgaver for å styre informasjonssikkerhet og personopplysningsvern til ledere som er mål- og resultatansvarlige for et område (risikoeiere).
- hvordan risikoeiere skal forstå, vurdere og håndtere risiko, inkludert kriterier for å akseptere risiko
- hvordan risikoeiere skal sørge for innebygd personvern i op tjenester som behandler personopplysninger
- hvordan styringsaktivitetene skal gjennomføres

OP-3 Vurdere behov for risikovurderinger

Risikoeiere skal regelmessig vurdere behovet for oppdaterte eller nye risikovurderinger innen sitt ansvarsområde. Foranalysen er grunnlaget for behovsvurderingen. Vurderingen skal avdekke om det er behov for ytterligere risikovurdering og -håndtering på ansvarsområdet.

Risikoeier skal også vurdere behovet for risikovurdering eller personvernkonsekvensvurdering dersom det skjer endringer grad kan påvirke informasjonssikkerhet og personopplysning og tjenester.

RV-2 Vurdere personvernkonsekvensvurdering (DPIA)

All behandling av personopplysninger krever et formål, et behandlingsgrunnlag, en vurdering av nødvendighet og proporsjonalitet og skal i hovedsak dokumenteres i en protokoll over behandlingsaktiviteter. En slik behandlingsprotokoll kan publiseres offentlig som en del av personvernerklæringen.

Dersom det er sannsynlig at en type behandling av personopplysninger kan medføre høy risiko for fysiske personer skal risikoeier i tillegg sørge for å gjennomføre en personvernkonsekvensvurdering (DPIA) for å finne de ekstra tiltakene som må til for å redusere en høy risiko. Slike vurderinger skal omfatte alle forhold og plikter knyttet til personvern, inkludert personopplysningssikkerhet. En vurdering av personvernkonsekvenser skal minimum inneholde:

- En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen

En vurdering av personvernkonsekvenser er særlig nødvendig i følgende tilfeller (listen er ikke uttømmende):

- bruk av ny teknologi, nye måter å behandle personopplysninger på eller nye bruksområder for personopplysninger
- en systematisk og omfattende vurdering av personopplysninger basert på automatisert behandling som i betydelig grad påvirker den fysiske personen
- behandling i stor skala av særlige kategorier av personopplysninger
- en systematisk overvåking i stor skala

ME-4 Vurdere effektivitet av sikkerhets- og personverntiltak

Virksomhetsledelsen har ansvar for at det regelmessig vurderes om sikkerhets- og personverntiltakene er effektive. Hensikten er å undersøke om tiltakene er etablert, at de virker som tiltenkt, og at de har ønsket effekt på virksomhetens informasjonssikkerhet og personopplysningsvern.

Gir evne til

- å kjenne status på sikkerhets- og personverntiltak
- å ha formåls- og kostnadseffektive sikkerhets- og personverntiltak
- å vurdere om styringsaktivitetene for å vurdere og håndtere risiko fungerer godt

Artikkel 32. *Sikkerhet ved behandlingen*

1. 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,

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.

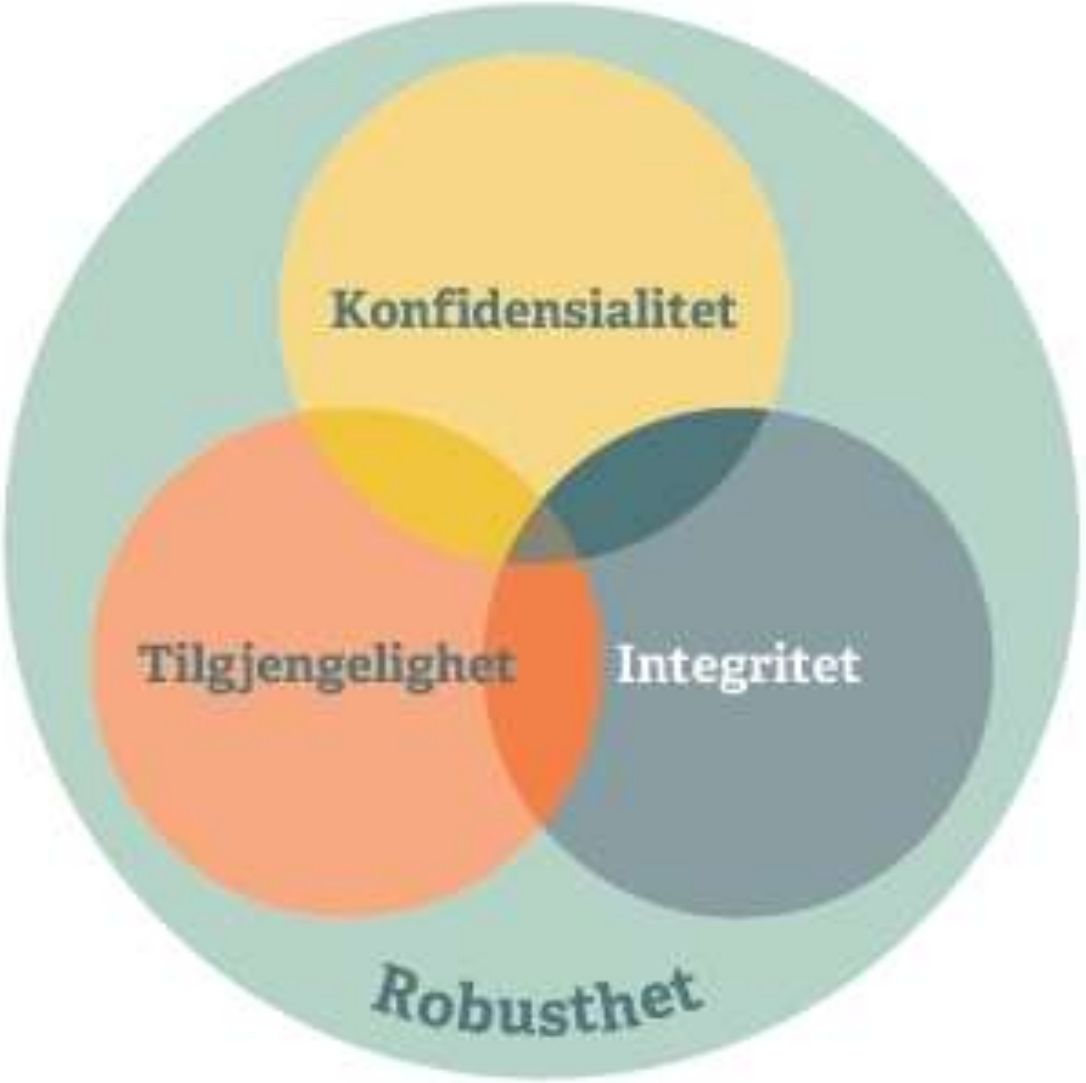
Personopplysningssikkerhet er:

- Sikring av **konfidensialitet (K)**
  - personopplysninger skal ikke bli kjent for uvedkommende

- Sikring av **integritet (I)**
  - personopplysninger ikke kunne bli endret utilsiktet eller av uvedkommende

- Sikring av **tilgjengelighet (T)**
  - personopplysninger er tilgjengelig for autoriserte ved behov

- **Robusthet**
  - tiltakene skal være effektive over tid og være motstandsdyktige overfor hendelser



Eksempler på rammeverk for konkretisering av art 32-krav

Styrende retningslinjer for autentiseringsløsninger

Jf. personvernforordningen artikkel 32.1.b:

evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og –tjenestene

Hva betyr det i praksis?

Støtteverktøy: *NSM Grunnprinsipper 2.6 Ha kontroll på identiteter og tilganger*

Rammeverk for kontrolltiltak: *ISO27002 (A.9, A.13) → ISO27001*

Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer

Jf. personvernforordningen artikkel 32.1.c:

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

Hva betyr det i praksis?

Støtteverktøy: *NSM Grunnprinsipper 2.9 Etabler evne til gjenoppretting av data*

Rammeverk for kontrolltiltak: *ISO27002 (A.13) → ISO27001*

Hvordan skal kravene til personopplysningssikkerhet forstås

- Det er risikoen for den registrerte det siktes til, og ikke risikoen for den behandlingsansvarlige eller databehandleren selv.

- Det er altså ikke virksomhetens risiko som er i fokus, men individets risiko. Mange virksomheter gjennomfører risikovurderinger ut fra virksomhetens risiko, etter forordningen kreves det her en annen vurdering.

  - **Virksomhetens risiko:** handler om økonomiske tap, bøter, tap av kunder, rykte eller driftsstans.

  - **Den registrertes risiko:** handler om konsekvenser for enkeltpersoner dersom deres opplysninger misbrukes, kommer på avveie eller blir feilbehandlet.

En vurdering etter art. 32 må alltid stille spørsmålet: "Hva kan skje med personen hvis sikkerheten svikter?" – ikke bare "Hva kan skje med virksomheten?".

Eksempler på forskjellige vurderinger

- **Datainnbrudd i en nettbutikk (K)**
  - *Virksomhetens risiko: Tap av inntekter, omdømmeskade, kostnader til å rydde opp og mulig sanksjoner.*
  - Den registrertes risiko: Identitetstyveri dersom betalingsinformasjon lekker, uautorisert bruk av e-post og passord, phishing-angrep.
- **Feil i et HR-system (I)**
  - *Virksomhetens risiko: Ineffektiv drift, feil i lønnsutbetalinger, kostnader til å korrigere data.*
  - Den registrertes risiko: At helseopplysninger, advarsler eller fagforeningstilknytning feilaktig registreres og senere brukes mot dem – kan påvirke deres karriere eller føre til diskriminering.
- **Tapt USB med kundedata (K)**
  - *Virksomhetens risiko: Brudd på interne rutiner, kostnader til å varsle myndigheter og kundene, mulig sanksjoner.*
  - Den registrertes risiko: Risiko for svindel, spam, sosial manipulering eller at sensitiv informasjon (f.eks. sykdomshistorikk) blir kjent for uvedkommende.
- **Systemnedetid i en helsetjeneste (TI)**
  - *Virksomhetens risiko: Avbrudd i drift, økonomisk tap, redusert tillit.*
  - Den registrertes risiko: Manglende tilgang til journaler eller feilbehandling fordi leger ikke får opp riktige opplysninger – kan skade pasientens helse eller liv.
- **Bruk av profilering i markedsføring (I)**
  - *Virksomhetens risiko: Feilsegmentering som gir lavere salg, feilaktige analyser, mulig sanksjoner.*
  - Den registrertes risiko: Urettferdig forskjellsbehandling (f.eks. høyere priser for enkelte grupper), tap av kontroll over egne data, inngrep i privatliv.

Hvilke brudd skal meldes til Datatilsynet?

Unntak fra meldeplikten

Når den behandlingsansvarlige opplever et brudd på personopplysningssikkerheten, må det vurderes hvilken *risiko* bruddet innebærer for de berørte personenes rettigheter og friheter.

Den behandlingsansvarlige trenger ikke melde bruddet til Datatilsynet dersom «bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter».

Den behandlingsansvarlige må være tilnærmet helt sikker på at bruddet ikke vil medføre eller har medført noen risiko for de berørte, for at unntaket skal være oppfylt.

Digitale angrep mot datasystemer hvor personopplysninger har blitt hentet ut, er endret på eller er utilgjengelige, eller at det er sannsynlig at dette har skjedd og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Tilgangsstyring **mangler, gir ikke effektiv beskyttelse, har feilet eller er blitt omgått**, slik at uvedkommende har fått tilgang til personopplysninger, har endret på eller gjort dem utilgjengelige, og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Forsendelsesfeil som inneholder beskyttelsesverdige personopplysninger og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

- Pakker, brev eller e-post sendt til feil mottaker(e)
- Forsendelser til riktig mottaker, men utilsiktede opplysninger om andre personer

Eksempler på typiske brudd som kan meldes til Datatilsynet

Digitale angrep mot datasystemer hvor personopplysninger har blitt hentet ut, er endret på eller er utilgjengelige, eller at det er sannsynlig at dette har skjedd og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Sårbarheter er oppdaget, hvor personopplysninger kan ha eller har blitt hentet ut, er endret på eller er utilgjengelige, eller at det er sannsynlig at dette har skjedd og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Tilgangsstyring **mangler, gir ikke effektiv beskyttelse, har feilet eller er blitt omgått**, slik at uvedkommende har fått tilgang til personopplysninger, har endret på eller gjort dem utilgjengelige, og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Uautorisert eller utilsiktet publisering av personopplysninger som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Manglende evne til effektiv gjenoppretting av tilgang til personopplysninger etter at disse har vært utilgjengelige og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Kastede dokumenter som skulle vært makulert og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

Mistede, gjenglemte eller frastjålne personopplysninger hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter:

- Som et resultat av dataangrep hvor opplysninger ikke er kryptert eller ikke er kryptert på en måte som effektivt beskytter mot den spesifikke hendelsen
- Datamaskin, nettbrett eller telefon der innholdet ikke er kryptert
- Minnepinne eller lignende der innholdet ikke er kryptert
- Papirdokumenter

Forsendelsesfeil som inneholder beskyttelsesverdige personopplysninger og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter.

- Pakker, brev eller e-post sendt til feil mottaker(e)
- Forsendelser til riktig mottaker, men utilsiktede opplysninger om andre personer

Er potensielle brudd og sårbarheter brudd?

- I hovedsak er et brudd knyttet til en faktisk hendelse med faktiske konsekvenser som sannsynligvis kan medføre risiko for de registrertes rettigheter og friheter
  - En hendelse kan utløses av uønskede tilsiktede handlinger av eksterne eller interne aktører, eller skyldes utilsiktede handlinger av eksterne eller interne aktører

- Hvis det oppdages sårbarheter og svakheter som innebærer at man ikke har behandlet personopplysninger etter kravene i forordningen og dette utgjør en risiko for registrerte, skal saken meldes til Datatilsynet

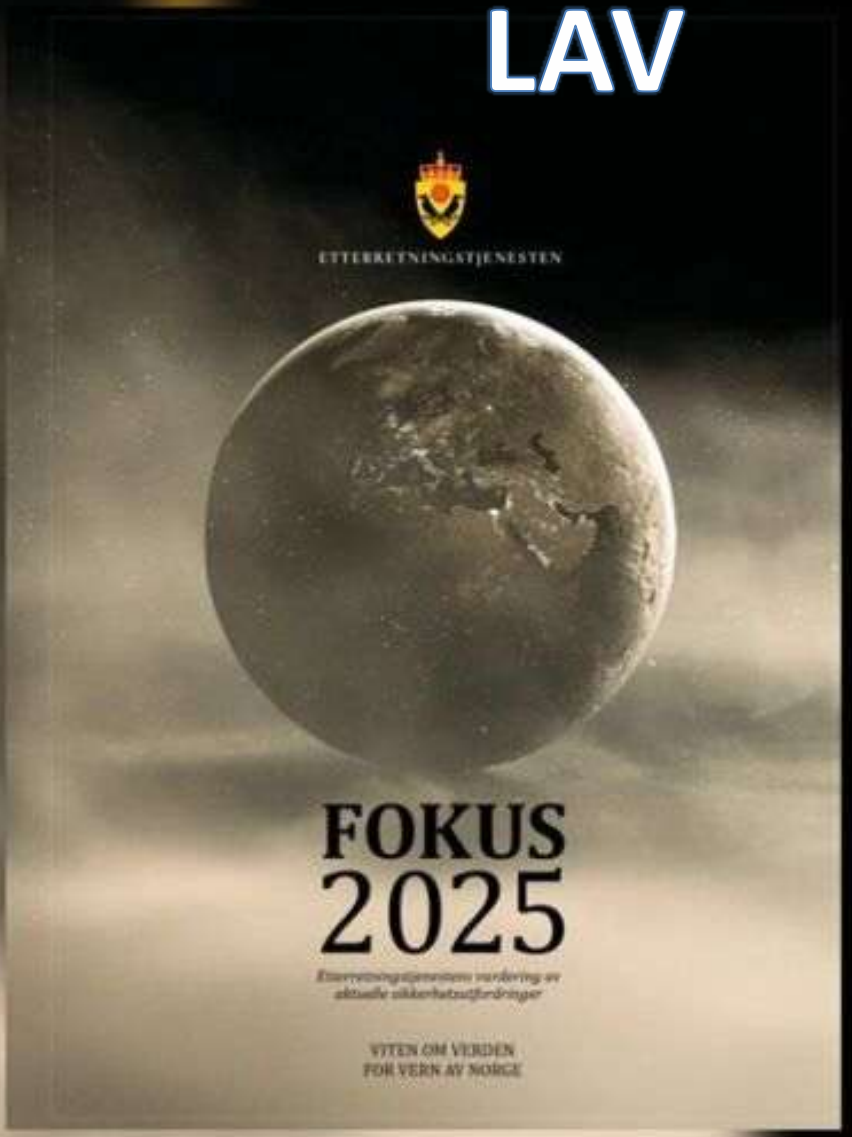
- Hvis det oppdages sårbarheter og svakheter som innebærer at man ikke kan behandle personopplysninger etter kravene i forordningen, og man ikke har iverksatt egnede og korrigerende tiltak (eller stoppet behandling), skal saken meldes til Datatilsynet*

- Sårbarheter kan være alvorlige tekniske og organisatoriske feil og svakheter knyttet til personopplysningssikkerhet som kan medføre risiko for de registrerte hvis ikke tiltak gjennomføres. Dette omfatter også feil og mangler i prosesser, tjenester, programvare og systemer som ikke direkte skyldes eksterne hendelser

** Hvis man ikke selv er i stand til å redusere høy risiko til egnet nivå, som regel dokumentert gjennom personvernkonsekvensvurdering (DPIA), er det nødvendig med en forhåndsdrøftelse med Datatilsynet (en formell prosess). Virksomheten kan ikke selv velge å akseptere høy risiko ved behandling av personopplysninger (artikkel 36).*

2023

LAV



2024

SKJERPET

2025

SANNSYNLIG

«Sabotasje mot norsk kritisk infrastruktur»

Den nye normalen

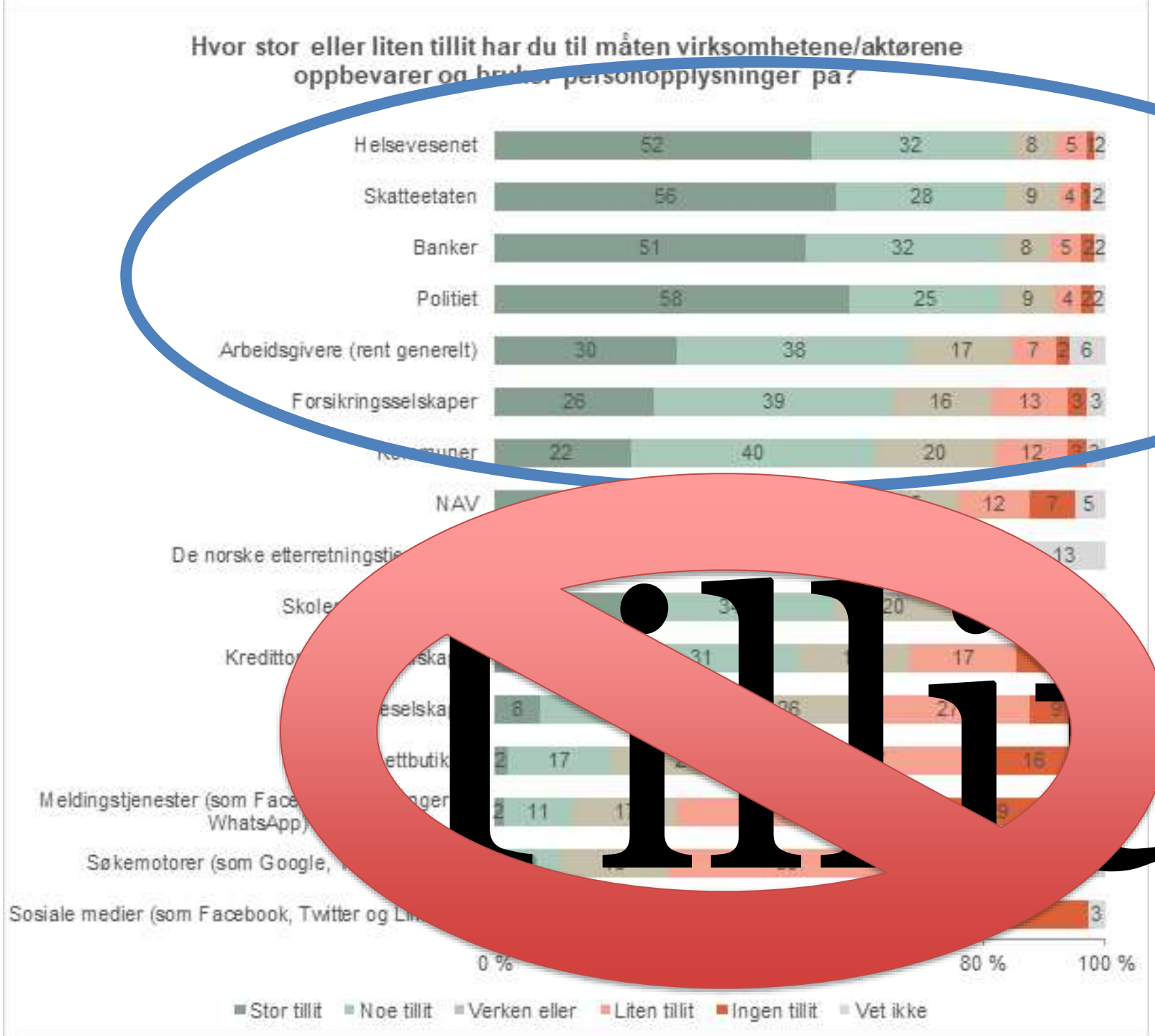
«Den sikkerhetspolitiske situasjonen er i kraftig endring. Det innebærer nye og sammensatte trusler som krever nye sikkerhetstiltak og kunnskapsutviklin

Hva har dett jøre?

Dårlig OT-sikkerhet = dårli gssikkerhet?

– Vi lever i en ny tid. Vår nye hverd e fremover krever at vi tar grep. Faren er at tr kere enn de åpne demokratienes evne til å beskytte seg.

Tillit


Hvor stor eller liten tillit har du til måten virksomhetene/aktørene
oppbevarer og bruker personopplysninger på?
Helsevesenet 52 32 8 5 2
Skatteetaten 56 28 9 4 2
Banker 51 32 8 5 2
Politiet 58 25 9 4 2
Arbeidsgivere (rent generelt) 30 38 17 7 6
Forsikringsselskaper 26 39 16 13 3 3
22 40 20 12
NAV 12 7 5
13
17
16
3
0 %
80 %
100 %
Stor tillit
Noe tillit
Verken eller
Liten tillit
Ingen tillit
Vet ikke

– Vi ruster oss til feil krig

Det er ikke sannsynlig at Russland går til krig mot Europa, mener forsvarsekspert. De vil derimot angripe oss der vi er svakest.

Russerne skjønner at de ikke kan slå oss militært. Likevel... Tormod Heier.

Forsvarsevnen er ikke avhengig først og fremst av masse jagerfly og mange stridsvogner. Den er avhengig av et tett, tillitsbasert forhold mellom borgerne og myndighetene.

Tormod Heier
professor ved Forsvarets høyskole

Målet er ikke bare å kunne slå tilbake et angrep, men å avskrekke Russland ved å vise at landet er forberedt, utholdende og vanskelig å destabilisere.

– Det er ikke noen tvil om at Tormod Heier har rett i at sammensatte trusler, bruk av andre typer virkemidler enn krig, er kommet for å bli, sier forsvarssjefen.

Kristoffersen peker på cyberangrep, påvirkningsoperasjoner og sabotasje som voksende utfordringer. Han mener, som Heier, at dette er trusler som i all hovedsak må løses av andre enn forsvaret:

– Vår oppgave er først og fremst å forsvare oss mot militære angrep i Norge, sikre norsk frihet og territoriell integritet, sier forsvarssjefen.

– Det er ikke et militært svar på det her. Det er et ansvar som justis har i fredstid, sier han, og mener styrking av totalforsvaret er avgjørende for å bygge motstandskraft i samfunnet.

Det mest sannsynlige angrepet mot Europa mener Heier er hybride sabotasjeaksjoner. Som kapping av kabler på havbunn, strømforsyning til byene, sabotasje av oljeinstallasjoner. I tillegg påvirkningsaksjoner, som polariserer og skaper mistillit mellom folk.

– Russerne tar jo ikke land ved å sabotere en sjøkabel, hvilken effekt har denne typen angrep?

– Jo, men slike angrep skaper frykt og engstelse i de tusen hjem. For hvis kommunale tjenestetilbud forsvinner, og befolkningen ikke lenger føler seg trygge der de bor, vil også tilliten til myndighetene få en knekk. Det bidrar til polarisering i samfunnet.

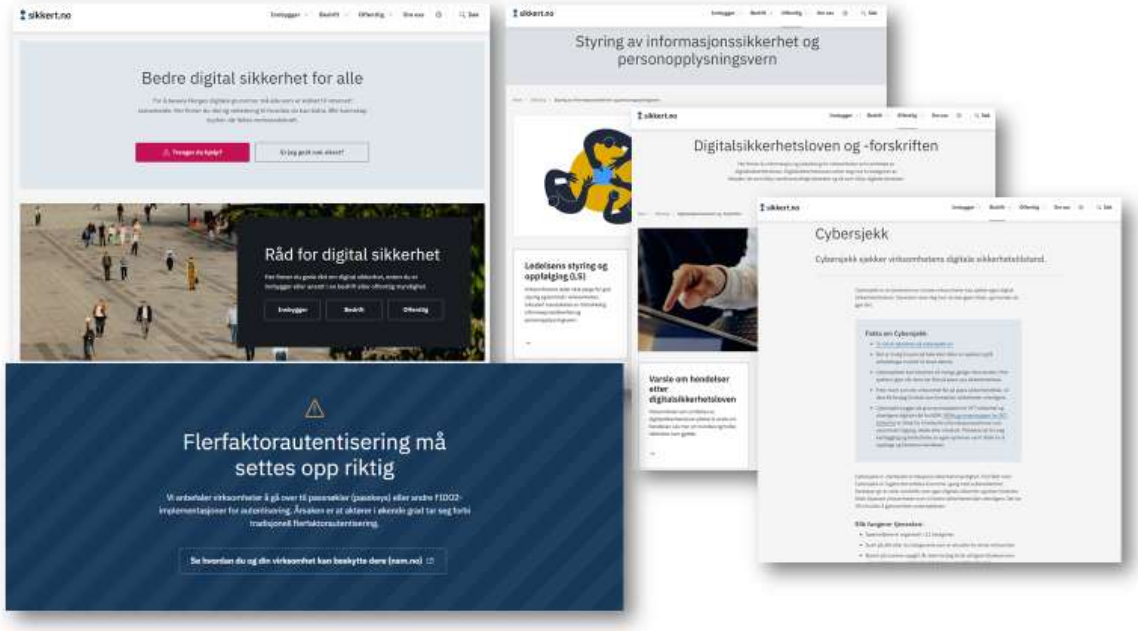
land på det?

assisk måte å drive splitt og hersk på. Når vi svekkes vi.

Totalforsvarsåret 2026 – samarbeid på tvers

Totalforsvarsåret 2026

Verden har blitt farligere og mer uforutsigbar. Det sivile samfunnet må være forberedt på å håndtere alvorlige kriser og, i ytterste konsekvens, krig – sammen med Forsvaret og våre allierte. Hensikten med Totalforsvarsåret 2026, er derfor å planlegge sammen, jobbe sammen og øve sammen – for et trygt Norge.



Eirik Gulbrandsen

Datatilsynets seksjon for Teknologi, Sikkerhet og Tilsyn

eirik.gulbrandsen@datatilsynet.no

Datatilsynet

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

datatilsynet.no
personvernbloggen.no