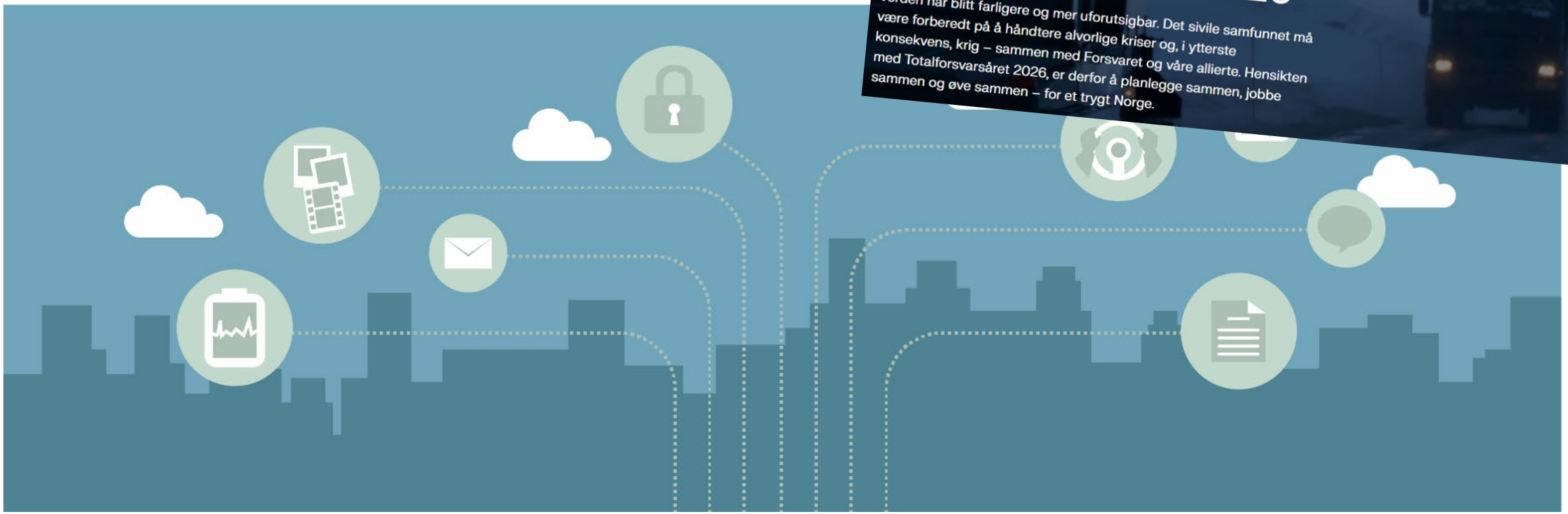
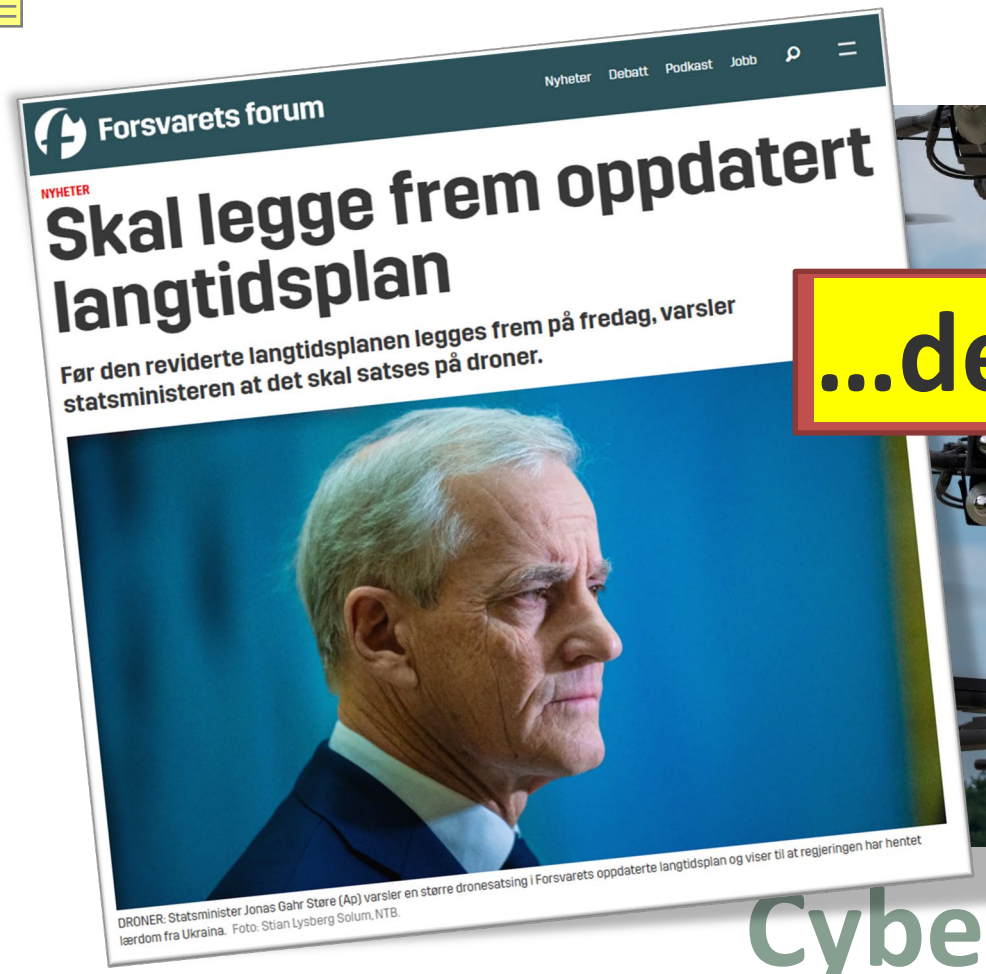


Cyberslagmark 2026
- med kommunen som frontlinje

Eirik Gulbrandsen | Spesialrådgiver seksjon Teknologi, Sikkerhet og Tilsyn

Datatilsynet



...det skal satses på droner.

Cyberslagmark 2026
- med kommunen som frontlinje

Eirik Gulbrandsen | Spesialrådgiver seksjon Teknologi, Sikkerhet og Tilsyn

AXIOS

Nov 13, 2025 - Technology

Chinese hackers used Anthropic's AI agent to automate spying

Sam Sabin

Add Axios on Google

Illustration: Sarah Grillo/Axios

Suspected Chinese operators used Anthropic's AI coding tool to target about 30 global organizations — and had success in several cases, the company said Thursday.

NRK Nyheter Sport Kultur Humor Distrikt Mer Logg på

Urix Urix forklarer Urix på NRK TV Urix i NRK Radio Korrespondentbrevet Nobels fredspris

Hevder Ukraina daglig angripes av hackere

Den ukrainske generalen Oleksandr Potii hevder åtti hackergrupper konstant angriper Ukraina. Nå inngår de et tett samarbeid om datasikkerhet med Norge.

Joakim Reigstad
Norden-korrespondent

Vi rapporterer fra Stockholm

Publisert 30. mai kl. 07:10
Oppdatert 30. mai kl. 10:23

...hevder åtti hackergrupper konstant angriper Ukraina.

– Hver dag opplever vi forskjellige former for cyberangrep. Vi ser direkte angrep mot vår finanssektor, energisektor, tele-kommunikasjon og logistikk, og selvfølgelig i den offentlige sektor.

Pål Wien Espen i Tek Norge: «Senest i går snakket jeg med den ukrainske søsterorganisasjonen til NSM. De ser en voldsom utvikling i hvordan KI brukes i cyberoperasjoner.»

2023 LAV

2024 SKJERPET

2025 SANNSYNLIG

«Russisk etterretning kan se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge i 2026.»

«Sabotasje mot norsk kritisk infrastruktur»

PST-sjefen: Mener russere sto bak norsk dam-sabotasje

«Passord123» angrepet...

– Dette er virkemidler og metoder som Russland benytter for å påvirke sikkerhetssituasjonen i andre land. Målet er å påvirke det norske samfunnet, spre uro og ustabilitet, samt kartlegge våre styrker og svakheter, sier PST-sjefen.

Den nye normalen

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

Tillit

Hva har det jøre?

Dårlig OT-sikkerhet = dår ngssikkerhet?

– 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 bruker vi det meste på militær opprustning, sier 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

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.

drive splitt og hersk på. Når vi

justis har i fredstid, sier han, og mener styrking av totalforsvaret er avgjørende for å bygge motstandskraft i samfunnet.

Tillit

personopplysninger har de
vurdering av personvernkonsekvensene ved å skulle
opprette en egen side på Facebook.

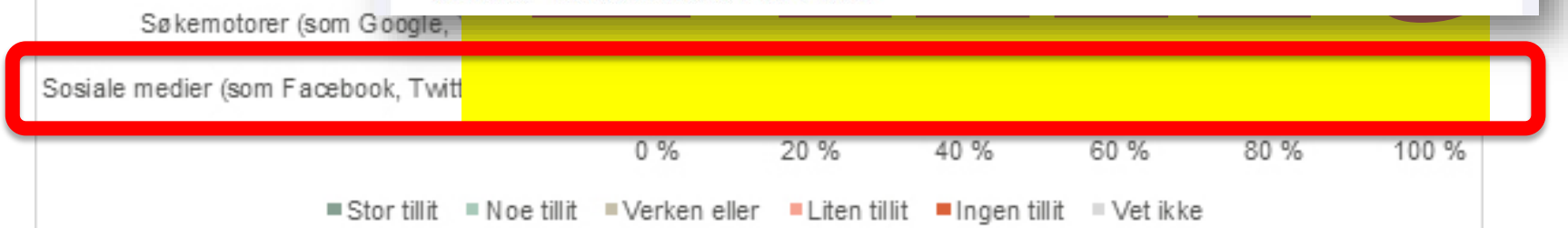
Alle som behandler personopplysninger må selv sørge for å etterleve pliktene i *personvernforordningen* (*GDPR*). Pliktene vil også gjelde når en virksomhet tar i bruk sosiale medier, for eksempel ved å opprette en egen side på Facebook.

Read in English

Norwegian DPA choose not to use Facebook

skader barn

Et opptak av Meta-grunnlegger Mark Zuckerbergs forklaring ble spilt av i retten i starten av mars. Foto: Jim Weber / AP / NTB



Fra fysiske til digitale demninger…

Bekreftar at personsensitiv data er lekka etter dataangrep i Østre Toten

Etterforskinga dei siste dagane har vist at data ligg ute på det mørke nettet. Kommunen seier persondata har hamna på «det mørke nettet».

GJENOPPRETTING: Alle desse datamaskinene måtte gjenopprettast etter angrepet. Kommunen var framleis utan alle system på plass ein månad etterpå.
FOTO: ANDERS BAKKERUD LARSEN / NRK

Marte Iren Noreng Trøen
Journalist

Line Fosser Vogt
Journalist

Dag Kessel
Journalist

Publisert 30. mars 2021 kl. 14:33
Oppdatert 31. mars 2021 kl. 22:07

Artikkelen er flere år gammel.

Oppdatert 31/3 kl. 22.00:

Kommunedirektøren i Østre Toten kommune seier ein stikkprøve som er gjort bekreftar at kriminelle har lagt ut personopplysningar på nett.

Hvordan bli mer motstandsdyktig?

Vi må være bedre forberedt på at Norge kan rammes av mer alvorlige sikkerhetstruende hendelser enn vi har erfart så langt.

Offentlige myndigheter, frivilligheten, næringsliv og andre virksomheter **må kartlegge egne verdier, kjenne egne sårbarheter og utvikle planer for bedre å motstå alvorlige hendelser.** Det er særlig viktig å raskt kunne gjenopprette drift.

«Økt systematikk i arbeidet med sikkerhet i offentlig, frivillig og privat sektor har en viktig rolle i arbeidet med norsk sikkerhet.»

90% av norske utsettes for «hendelser» (digitale angrep)

(de siste 10% vet ikke at det er blitt utsatt…)

6% sier de er i stand til å håndtere det

6 av 10 norske virksomheter ønsker å være aktiv del av totalberedskapen

3 av 10 sier de er det

Hva er det viktigste å gjøre den dagen det smeller?

DET SAMME SOM DU GJORDE I GÅR!

*Pvf 32.1.d) evne til å **gjenopprette** tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,*

Vi må være bedre forberedt på at Norge kan rammes av mer alvorlige sikkerhetstruende hendelser enn vi har erfart så langt.

*Offentlige myndigheter, frivilligheten, næringsliv og andre virksomheter **må kartlegge egne verdier, kjenne egne sårbarheter og utvikle planer for bedre å motstå alvorlige hendelser.** Det er særlig viktig å raskt kunne gjenopprette drift.*

Eksempler på rammeverk for konkretisering av art 32-krav

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

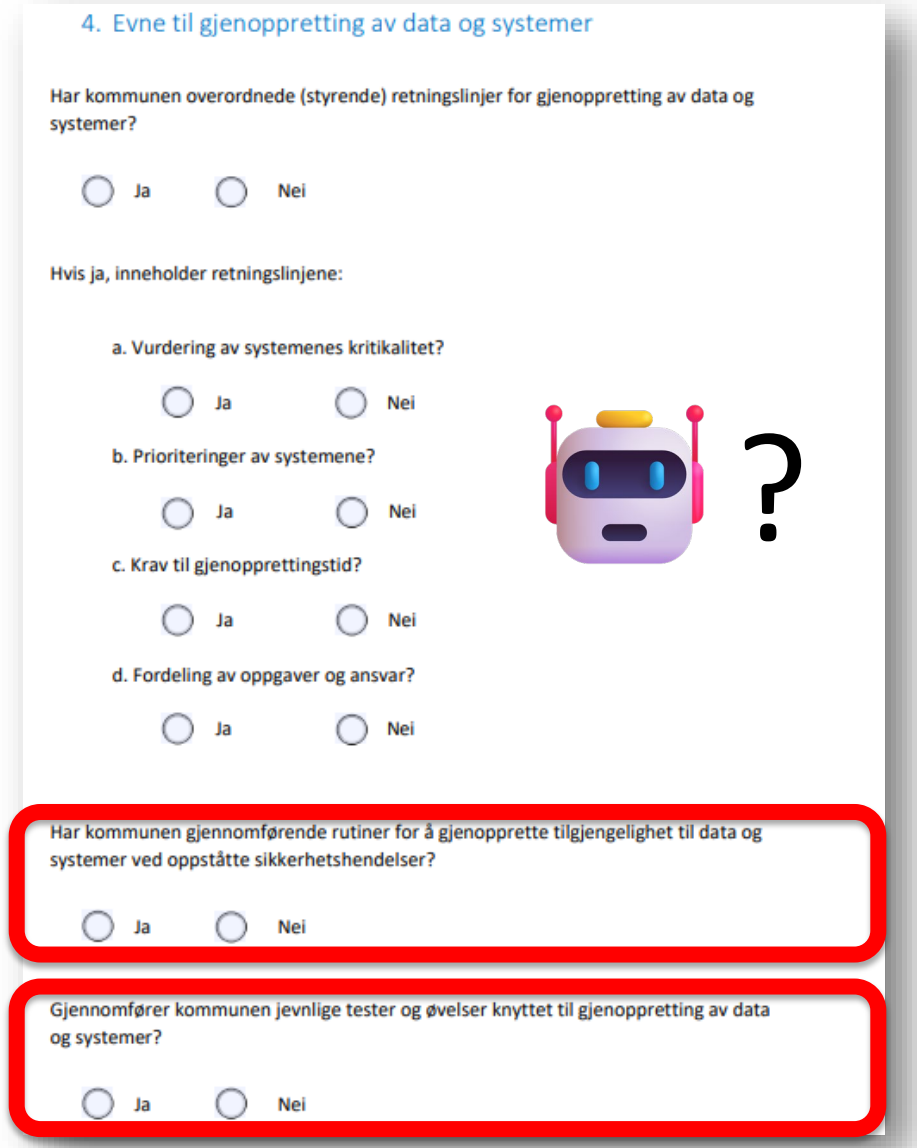
Hva betyr det i praksis?

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

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

2026 →

DET SAMME SOM DU GJORDE GÅR?



Men hvordan skal vi klare å håndtere både personvern, ransomware, phishing og navigere GDPR, DSL, NIS2, Grunnpri…

Men hvordan skal vi klare å håndtere både personvern, ransomware, phishing og navigere GDPR, DSL, NIS2, Grunnpri…

2. Overordnet felles styringssystem for informasjonssikkerhet og personvern

Har kommunen et etablert styringssystem for å ivareta arbeidet med informasjonssikkerhet og personvern?

Ja Nei Delvis

Felles styringssystemer

2. Overordnet felles styringssystem for informasjonssikkerhet og personvern

Har kommunen et etablert styringssystem for å ivareta arbeidet med informasjonssikkerhet og personvern?

- ○ Ja
- ○ Nei
- ○ Delvis

Felles sikkerhet i forvaltningen

Felles anbefalinger gir samordnet hjelp

NSM Datatilsynet Digdir KS dfø Helsedirektoratet

§ 4-2. *Vurdering av risiko*

Sikkerhetsloven

Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

§ 7. *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

Digitalsikkerhetsloven

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

§ 10. *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Artikkel 32. *Sikkerhet ved behandlingen*

GDPR

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 organisat
sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

Artikkel 24. *Den behandlingsansvarliges ansvar*

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.

Ledelsens styring og oppfølging

Ha oversikt og prioritere

Vurdering av risiko

Måling, evaluering og revisjon

Overvåking og hendelseshåndtering

Kompet
kultur

ing

Kommunikasjon

NSM Datatilsynet Digdir KS dfø Helsedirektoratet

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

LS-1 Gi føringer

Virksomhetsledelsen skal gi føringer for hvordan styringen av informasjonssikkerhet og personopplysningsvern skal fungere som en del av den helhetlige styring basert på virksomhet Føringene skal inneh virksomhetens inform virksomhetens oppg

Virksomhetsledelsen har ansvaret for å gi føringer for

- struktur og innhold i styringsaktivitetene
- roller og myndighet i arbeidet med styring av informasjonssik personopplysningsvern
- delegering av oppgaver for å styre inform personopplysningsvern til ledere som e område (risikoeiere).
- hvordan risikoeiere skal forstå, vurdere kriterier for å akseptere risiko
- hvordan risikoeiere skal sørge for inneby tjenester som behandler personopplysn
- hvordan styringsaktivitetene skal gjenn

Gir evne til

- helhetlig styring av arbeidet med i personopplysningsvern.
- å styre hva som skal gjøres, og hvem som skal gjøre det

Ledelsens styring og oppfølging (LS)

ng og kontroll i
ekkelig
vern.

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

ene som en del av

det øvrige arbeidet med
sningsvern

eidet med informasjonssikkerhet og

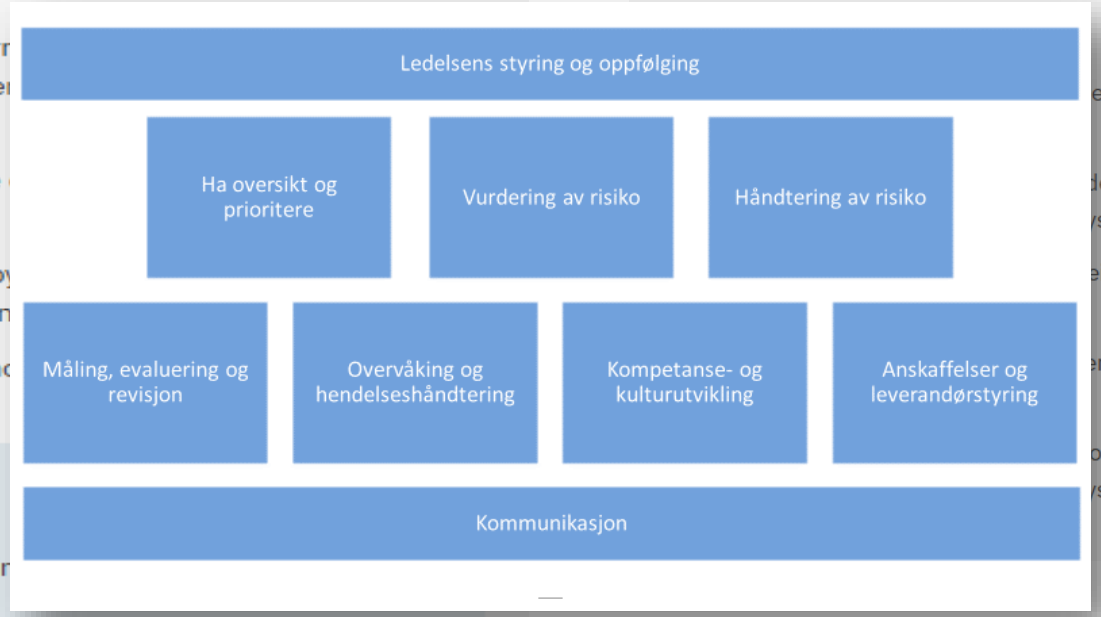
erer godt og gjøre nødvendige

og tjenester har tilstrekkelig
sningsvern

Innhold

NÅR DET SMELLER, SÅ KLARER VI Å:
GJØRE DET SAMME SOM VI GJORDE I GÅR!

Tilsyn 👍



NSM Datatilsynet Digdir KS dfø Helsedirektoratet

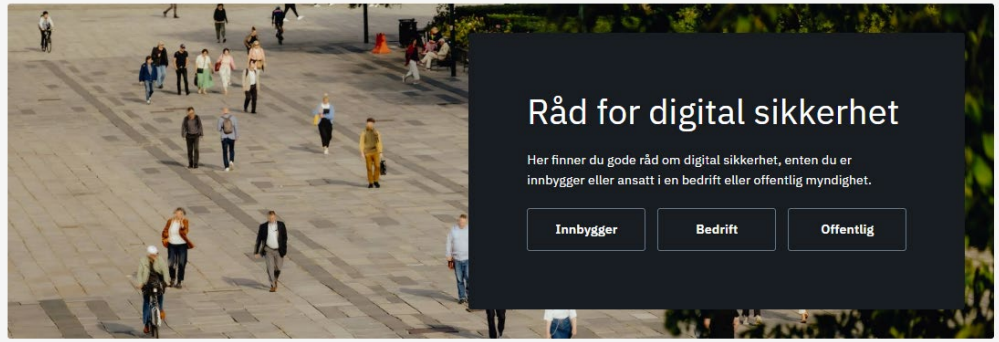
sikkert.no

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

Bedrift Offentlig

Digitalsikkerhetsloven og -forskriften

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Styring av informasjonssikkerhet og personopplysningsvern

Hjem › Offentlig › Styring av informasjonssikkerhet og personopplysningsvern

Ledelsens styring og oppfølging (LS)

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

→

Håndtering av risiko

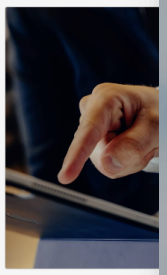
sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Digitalsikkerhetsloven og -forskriften

Her finner du informasjon og veiledning for virksomheter som omfattes av digitalsikkerhetsloven. Digitalsikkerhetsloven retter seg mot to kategorier av

Hjem › Offentlig › Digitalsikkerhetslov



Varsle om hend… etter digitalsikkerhet

Virksomheter som omfattes … digitalsikkerhetsloven plikter … hendelser. Les mer om hvord… tidsfrister som gjelder.

→

Innbygger Be…

Trussel-…

Les de åpne tru…

Etterretningstj…

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Cybersjekk

Cybersjekk sjekker virksomhetens digitale sikkerhetstilstand.

Cybersjekk er en tjeneste hvor norske virksomheter kan sjekke egen digital sikkerhetstilstand. Tjenesten viser deg hvor du bør gjøre tiltak, og hvordan du gjør det.

Fakta om Cybersjekk

- Ta i bruk tjenesten på cybersjekk.no.
- Det er mulig å svare på hele eller deler av sjekken og få anbefalinger knyttet til disse delene.
- Cybersjekken kan benyttes så mange ganger dere ønsker. Prøv sjekken igjen når dere har fått på plass nye sikkerhetstiltak.
- Etter hvert som din virksomhet får på plass sikkerhetstiltak, vil dere få forslag til tiltak som forsterker sikkerheten ytterligere.
- Cybersjekk bygger på grunnprinsippene for IKT-sikkerhet og ytterligere digitale råd fra NSM. NSMs grunnprinsipper for IKT-sikkerhet er tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Tiltakene tar for seg kartlegging og beskyttelse av egne systemer samt tiltak for å oppdage og håndtere hendelser.

Cybersjekk er utarbeidet av Nasjonal sikkerhetsmyndighet. Formålet med Cybersjekk er å gjøre det enklere å komme i gang med cybersikkerhet. Verktøyet gir et raskt overblikk over egen digitale sikkerhet og deler konkrete tiltak tilpasset virksomheten som vil bedre sikkerhetsnivået ytterligere. Det tar 30 minutter å gjennomføre undersøkelsen.

Slik fungerer tjenesten:

- Spørsmålene er organisert i 11 kategorier.
- Svart på alle eller du kategoriene som er aktuelle for deres virksomhet.
- Basert på svarene oppgitt får dere forslag til de viktigste tiltakene som …

Cybersjekk

Hvor godt sikret er din virksomhet?

Cybersjekk er en tjeneste hvor norske virksomheter kan sjekke egen digital sikkerhetstilstand.

Verktøyet gir et raskt overblikk over egen digitale sikkerhet og deler prioriterte tiltak tilpasset virksomheten som vil bedre sikkerhetsnivået ytterligere. Det tar 30 minutter å gjennomføre undersøkelsen.

Les gjerne brukerguiden før du setter i gang.

Cybersjekk er utarbeidet av Nasjonal sikkerhetsmyndighet.

Start undersøkelsen

Spørsmål 1/2

Ledelse

Hvordan involverer ledelsen seg i sikkerhetsarbeidet?

Du kan velge flere alternativer

- [ ] IKT-sikkerhet er jevnlig et tema i virksomhetens ledermøter
- [ ] Ledelsen blir målt av styret (eller tilsvarende) på IKT-sikkerhet
- [ ] Ledelsen går foran som gode eksempler og snakker om IKT-sikkerhet i intern kommunikasjon
- [ ] Ledelsen gir arbeid med IKT-sikkerhet tilstrekkelig prioritet og ressurser

---

- (•) Ingen av disse

Les mer om ledelsens ansvar

Innhold

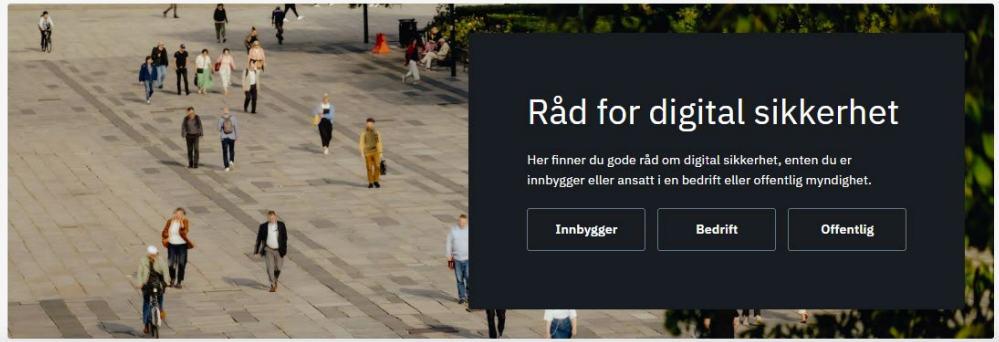
sikkert.no

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)

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Styring av informasjonssikkerhet og personopplysningsvern

Hjem › Offentlig › Styring av informasjonssikkerhet og personopplysningsvern

Ledelsens styring og oppfølging (LS)

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

→

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Digitalsikkerhetsloven og -forskriften

Her finner du informasjon og veiledning for virksomheter som omfattes av digitalsikkerhetsloven. Digitalsikkerhetsloven retter seg mot to kategorier av tilbyder; de som tilbyr samfunnsviktige tjenester og de som tilbyr digitale tjenester.

Hjem › Offentlig › Digitalsikkerhetsloven og -forskriften

Varsle om hendelser etter digitalsikkerhetsloven

Virksomheter som omfattes av digitalsikkerhetsloven plikter å varsle om hendelser. Les mer om hvordan og hvilke tidsfrister som gjelder.

→

sikkert.no

Innbygger Bedrift Offentlig Om oss Søk

Cybersjekk

Cybersjekk sjekker virksomhetens digitale sikkerhetstilstand.

Cybersjekk er en tjeneste hvor norske virksomheter kan sjekke egen digital sikkerhetstilstand. Tjenesten viser deg hvor du bør gjøre tiltak, og hvordan du gjør det.

Fakta om Cybersjekk

- Ta i bruk tjenesten på cybersjekk.no.
- Det er mulig å svare på hele eller deler av sjekken og få anbefalinger knyttet til disse delene.
- Cybersjekken kan benyttes så mange ganger dere ønsker. Prøv sjekken igjen når dere har fått på plass nye sikkerhetstiltak.
- Etter hvert som din virksomhet får på plass sikkerhetstiltak, vil dere få forslag til tiltak som forsterker sikkerheten ytterligere.
- Cybersjekk bygger på grunnprinsippene for IKT-sikkerhet og ytterligere digitale råd fra NSM. NSMs grunnprinsipper for IKT-sikkerhet er tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Tiltakene tar for seg kartlegging og beskyttelse av egne systemer samt tiltak for å oppdage og håndtere hendelser.

Cybersjekk er utarbeidet av Nasjonal sikkerhetsmyndighet. Formålet med Cybersjekk er å gjøre det enklere å komme i gang med cybersikkerhet. Verktøyet gir et raskt overblikk over egen digitale sikkerhet og deler konkrete tiltak tilpasset virksomheten som vil bedre sikkerhetsnivået ytterligere. Det tar 30 minutter å gjennomføre undersøkelsen.

Slik fungerer tjenesten:

- Spørsmålene er organisert i 11 kategorier.
- Svart på alle eller du kategoriene som er aktuelle for deres virksomhet.
- Basert på svarene oppgitt får dere forslag til de viktigste tiltakene som

Effektiv 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.

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-passkeys-fido2

Effektiv sterk autentisering (Kommunetilsyn 2023-2026)

3. Autentisering og tilgangsstyring

Har kommunen en overordnet (styrende) retningslinje som beskriver krav til autentiseringsløsninger?

◯ Ja ◯ Nei

Hvis ja, skiller denne mellom forskjellige brukergrupper og systemer?

◯ Ja ◯ Nei

Har kommunen dokumentert oversikt over hvilke autentiseringsløsninger som benyttes for de ulike systemene?

◯ Ja ◯ Nei

Oppgi kommunens primære sikkerhetsmekanisme for autentisering av brukere og systemer:

◯ Brukernavn og passord
◯ Multifaktor/2-faktor
◯ Sterk autentisering («phishingresistent autentisering»)
◯ Annen

Gjennomførte kommunen risiko- og sårbarhetsanalyser før valg av gjeldende autentiseringsløsning(er)?

◯ Ja ◯ Nei

Artikkel 32

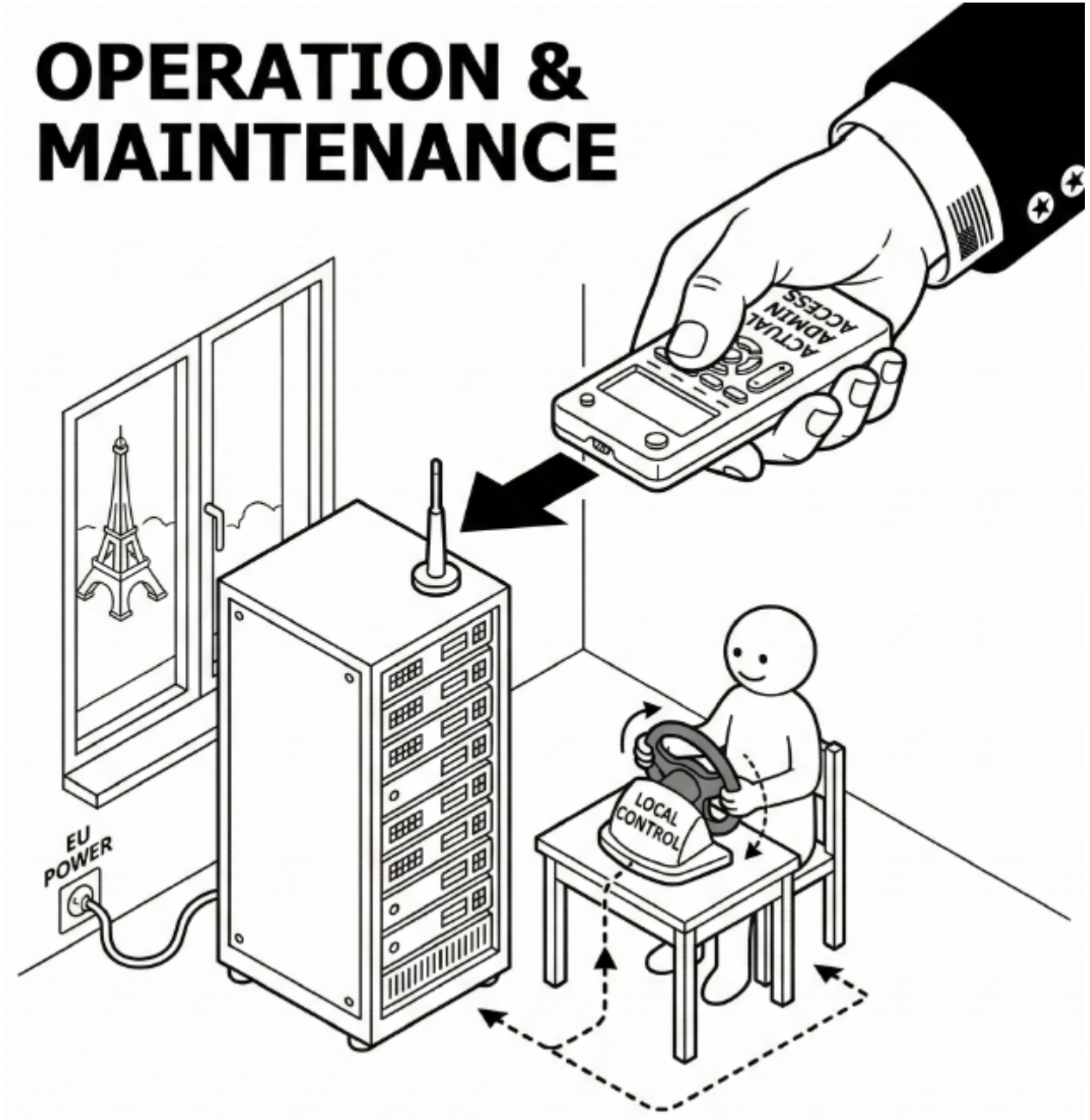
…skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen

Når gjennomførte kommunen sist en evaluering av autentiseringsløsningens effektivitet?

◯ Mindre enn 6 mnd
◯ 6 - 12 mnd
◯ 1– 2 år
◯ Mer enn 2 år
◯ Aldri

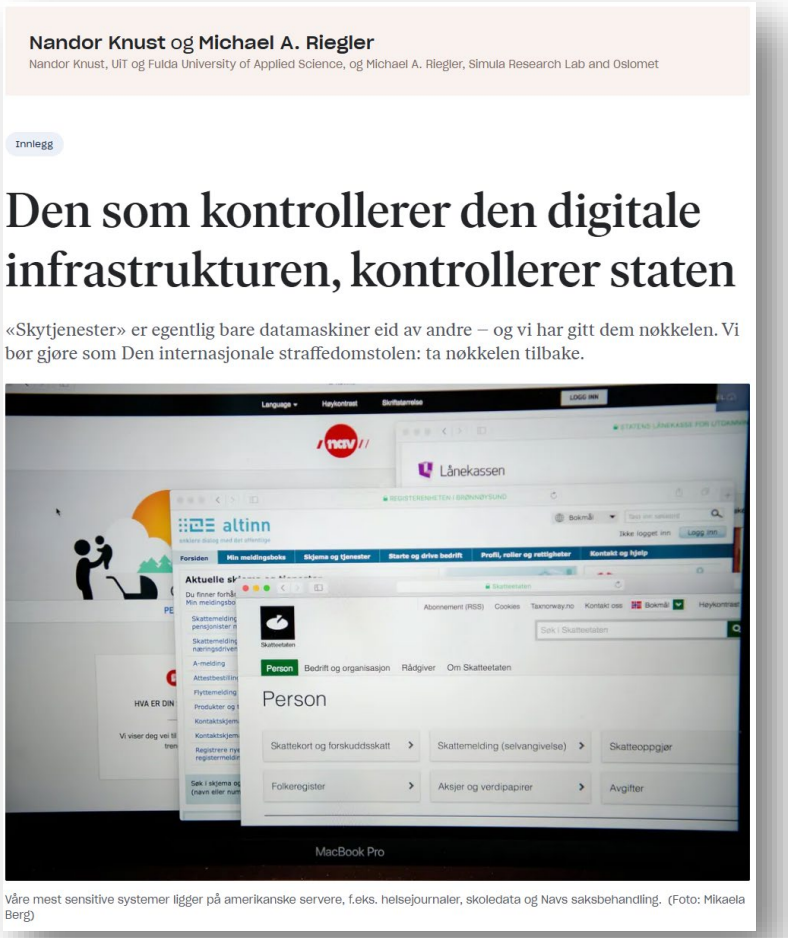
Artikkel 32.1.d

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


OPERATION &
MAINTENANCE
ACTUAL ADMIN ACCESS
EU POWER
LOCAL CONTROL


Microsoft Entra ID
Identities
Endpoints
Microsoft Entra ID
Microsoft Defender for Identity
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Microsoft Defender for Cloud
Microsoft Information Protection
Microsoft Cloud App Security
Applications
Data
Infrastructure
Network

Digital suverenitet-as-a-service?



Nandor Knust og Michael A. Riegler

Nandor Knust, UiT og Fulda University of Applied Science, og Michael A. Riegler, Simula Research Lab and Oslomet

Innlegg

Den som kontrollerer den digitale infrastrukturen, kontrollerer staten

«Skytjenester» er egentlig bare datamaskiner eid av andre – og vi har gitt dem nøkkelen. Vi bør gjøre som Den internasjonale straffedomstolen: ta nøkkelen tilbake.

Våre mest sensitive systemer ligger på amerikanske servere, f.eks. helsejournaler, skoledata og Navs saksbehandling. (Foto: Mikaela Berg)

Sage Journals

Search this journal | Enter search terms...

Advanced search

Browse by discipline | Information for

Media, Culture & Society

Impact Factor: 3.3 / 5-Year Impact Factor: 4.

Open access | Research article | First published online November 11, 2025

Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty

Rafael Grohmann and Alexandre Costa Barbosa View all authors and affiliations

OnlineFirst | https://doi.org/10.1177/01634437251395003

Contents | PDF/EPUB | Cite | Share options | Information, rights and permissions

Abstract

This article introduces the concept of sovereignty-as-a-service to describe how Big Tech companies, specifically Microsoft, Amazon, and Google/Alphabet, are strategically redefining digital sovereignty through their programs of cloud infrastructure. Drawing on critical discourse analysis of official materials released between 2022 and 2023, we show how these companies respond to regulatory pressures, particularly in Europe, by offering modular and branded solutions that frame sovereignty as a technical, legal, and infrastructural matter. Rather than sovereignty being exercised over platforms, it is now provisioned by them, on their terms. We argue that sovereignty-as-a-service constitutes a form of discursive capture that empties the concept, aligning it with the ideological legacy of the Californian Ideology. In this reframing, digital sovereignty becomes a service to be purchased, configured, and optimized through proprietary platforms. By conceptualizing sovereignty as a site of contested meanings open to appropriation, this article contributes to critical debates on digital sovereignty and technology governance.

Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty

En nasjon av Microsoft-avhengige

Skatteetaten omgår statens fellesavtale for å fortsette med Microsoft. Kostnadene ved å bytte, gjør en exit-strategi nærmest umulig.

Statens egen digitaliseringsstrategi legger vekt på fleksibilitet og sikkerhet. Likevel har mange bundet seg hardt til Microsoft, skriver Digis kommentator. Bildet er fra Microsofts lokaler i Bjørvika i Oslo. Foto: Marius B. Jørgenrud

Microsoft fjerner volumrabatt – det kan gi million-smell

Fra 1. november endrer Microsoft prismodellen for programvare. Det betyr vesentlig dyrere lisenser for mange bedrifter og etater.

Lytt til artikkelen – 2m

Teams, Word, e-post og Copilot. Mange store norske virksomheter har gjort seg avhengig av programvare fra Microsoft. Foto: Lindsey Wasson/AP/NTB

Nav sier til Digi at de har hatt en økning på Microsofts SaaS-lisenser på 30 til 40 prosent de siste fire–fem årene.

En slik innlåsningseffekt burde være med i de økonomiske kalkylene fra start, både når man anskaffer programvare og skytjenester.

Når man står der med skjegget i datasenteret og ikke kommer ut, er det allerede for sent.

Men det finnes etater som tenker annerledes. **Nav** har lenge fokusert på at det skal være mulig å bytte leverandør.

De sier at deres viktigste fagsystemer ville vært oppe igjen etter bare noen dager hvis de brått mistet tilgangen til Microsoft, Google og Amazon Web Services (AWS).

Nav har kopi av alle data og programkode for fagsystemene sine og kan raskt flytte dem til egne interne miljøer.

Også Statistisk sentralbyrå (SSB) jobber for å redusere avhengighet og innlåsing. De har brukt åpen kildekode siden 2018 og har lært opp statistikere i Python og versjonskontroll på GitHub.

SSB bruker åpen kildekode på både plattformer, applikasjoner og lagringsløsninger. Slik blir de også mer fleksible til å bytte leverandør.

Stivere Microsoft-priser: Må ut med flere titalls millioner mer

– At prisene øker, gjør det enda mer aktuelt å undersøke ulike alternativer, sier IT-sjefen i Nav.

Lytt til artikkelen – 5m

Nav, som er en av Norges største arbeidsgivere, merker det godt når Microsoft flikker på prisene sine. Colourbox.com

- ✓ *Sett deg inn i alternativene, også de europeiske*

- ✓ *Vær klar over at de amerikanske teknologigigantene har satset milliardbeløp på skytjenester og KI, noe som genererer et voldsomt press på salg av deres tjenester*
- ✓ *Bygg strategisk og teknisk kompetanse på alternativer*
- ✓ *Bygg bestillerkompetanse og trygghet i ledelsen*
- ✓ *Ha en plan – det blir svært «trangt i døra» - og dyrt - når alle plutselig MÅ lære seg nye ting for å realisere alternativer…*

DIGI Ledige stillinger Nyhetsbrev Nyhetsstudio Tips oss Attack-konferansen 27. nov

ICC kaster ut Microsoft

Få måneder etter at Karim Khan ble kastet ut av Microsoft-kontoen, dropper hele domstolen tech-kjempen til fordel for tysk-utviklet programvare.

Lytt til artikkelen – 2m

Karim Khan, Sjefsanklager i den internasjonale straffedomstolen havnet på vårparten midt i debatten om europeisk digital uavhengighet. Foto: Mary Altaffer

openDesk

Redesigning collaboration

From word processing and project management to secure communication: openDesk gives you the right tools for everyday public administration.

Level up to a truly sovereign workplace

- Open standards and modular architecture allow you to stay flexible and avoid dependencies on individual commercial vendors.
- Use openDesk in any browser, on any device – in the office, on the road, or at home.
- Thanks to local hosting and strict data protection standards, you retain full control over your data and processes.

- Calendar
- Chat
- Contacts
- Document management
- Email
- File storage
- Identity & access management
- Knowledge
- Notes
- Project management
- Task management
- Video conferencing

B1 SYSTEMS
Collabora Online
element by the creators of Matrix
Nextcloud
Nordeck
OpenProject
Stay Open. OX
STACKIT A Brand of Schwarz Digits
univention be open.
XWIKI

Datatilsynet forventer ikke …

- … at man slutter å overføre til USA eller bruke amerikanske tjenester
- … at man kan bytte ut alle amerikanske tjenester med europeiske alternativer
- … at endringer kan utføres over natten

Datatilsynet forventer …

- … at man følger med og er forberedt på å gjøre endringer

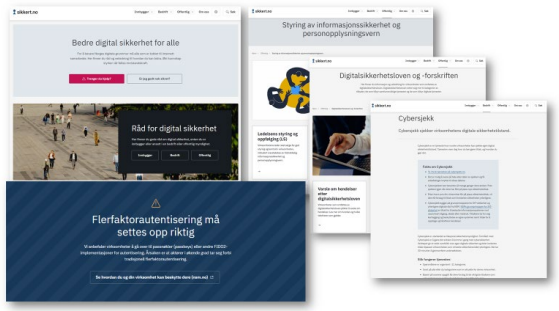
- … at man er særlig bevisst ved nye anskaffelser

- … at man tenker beredskap – har en plan!
  - *Hvilke type behandlinger/tjenester vil kunne påvirkes?*
  - *Hvilke vil sannsynligvis ikke påvirkes?*
  - *Hvilke er kritiske for virksomheten?*
  - *Hvilke er mindre kritiske?*
  - *Hvilke alternative tjenester kan helt eller delvis dekke behovet?*
  - *Hvilken kompetanse er nødvendig?*
  - *«Exit» = diversifisering = robusthet =* **Digital suverenitet**

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. H
med Totalforsvarsåret 2026, er derfor å planlegge sammen, j
sammen og øve sammen – for et trygt Norge.



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

Innhold

- Introduksjon
- Ledelsens styring og oppfølging (LS)
- LS-1 Gi føringer
- LS-2 Sørge for budsjett til arbeidet
- LS-3 Kommunisere viktighet
- LS-4 Løfte og håndtere problemstillinger gjennom linjen
- LS-5 Virksomhetsledelsens gjennomgang

Innbygger | Bedrift | Offentlig

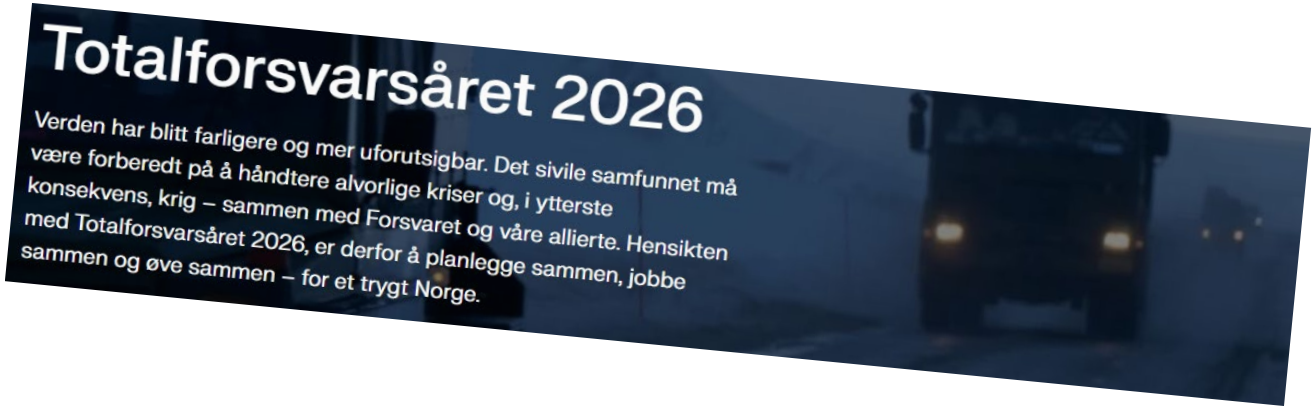
Trussel- og risikovurderinger 2026

Les de åpne trussel- og risikovurderingene for 2026 fra NSM, PST, Etterretningstjenesten og politiet.

Varsler tilsyn med alle Norges kommuner

Som en del av Totalforsvarsåret 2026, har Datatilsynet satt i gang et omfattende *tilsyn* med hvordan norske kommuner sikrer personopplysninger.

NSM | Datatilsynet | Digdir | KS | dfø | Helsedirektoratet



Hva er det viktigste å gjøre den dagen det smeller?

DET SAMME SOM DU GJORDE I GÅR!

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