NSM

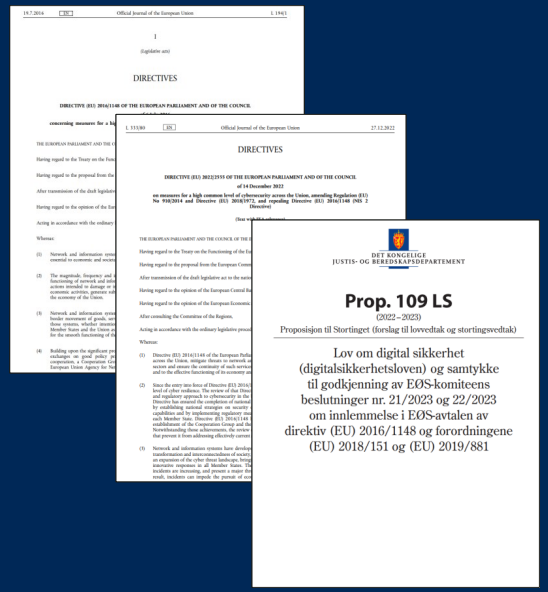
Ny lov om digital sikkerhet og gjennomføring av NIS/NIS2-direktivet

KiNS-konferansen 2025
Kristiansand

22.05.2025

Arbeid i flere spor

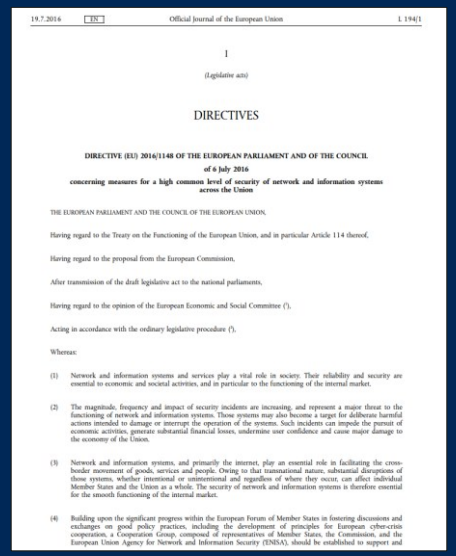
Regelverksutvikling



Hendelseshåndtering

Nasjonalt og internasjonalt samarbeid

Status for regelverksutviklingen



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

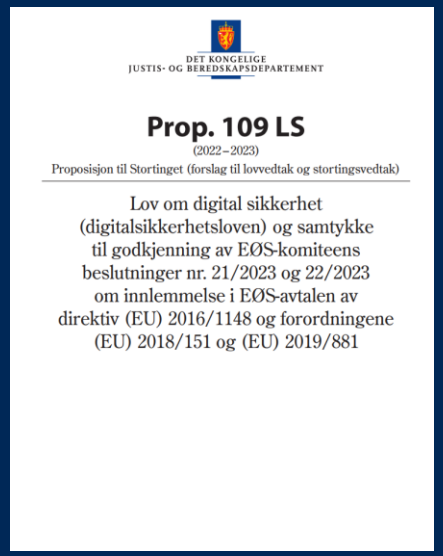
(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA), should be established to support and

NOU Norges offentlige utredninger 2018: 14

IKT-sikkerhet i alle ledd

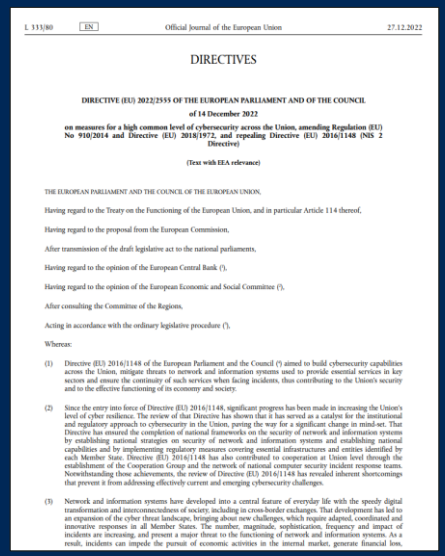
Organisering og regulering av nasjonal IKT-sikkerhet



DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 109 LS
(2022–2023)
Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council (4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

NIS 1 (2016)

Høring - utkast til ny lov (2018-2019)

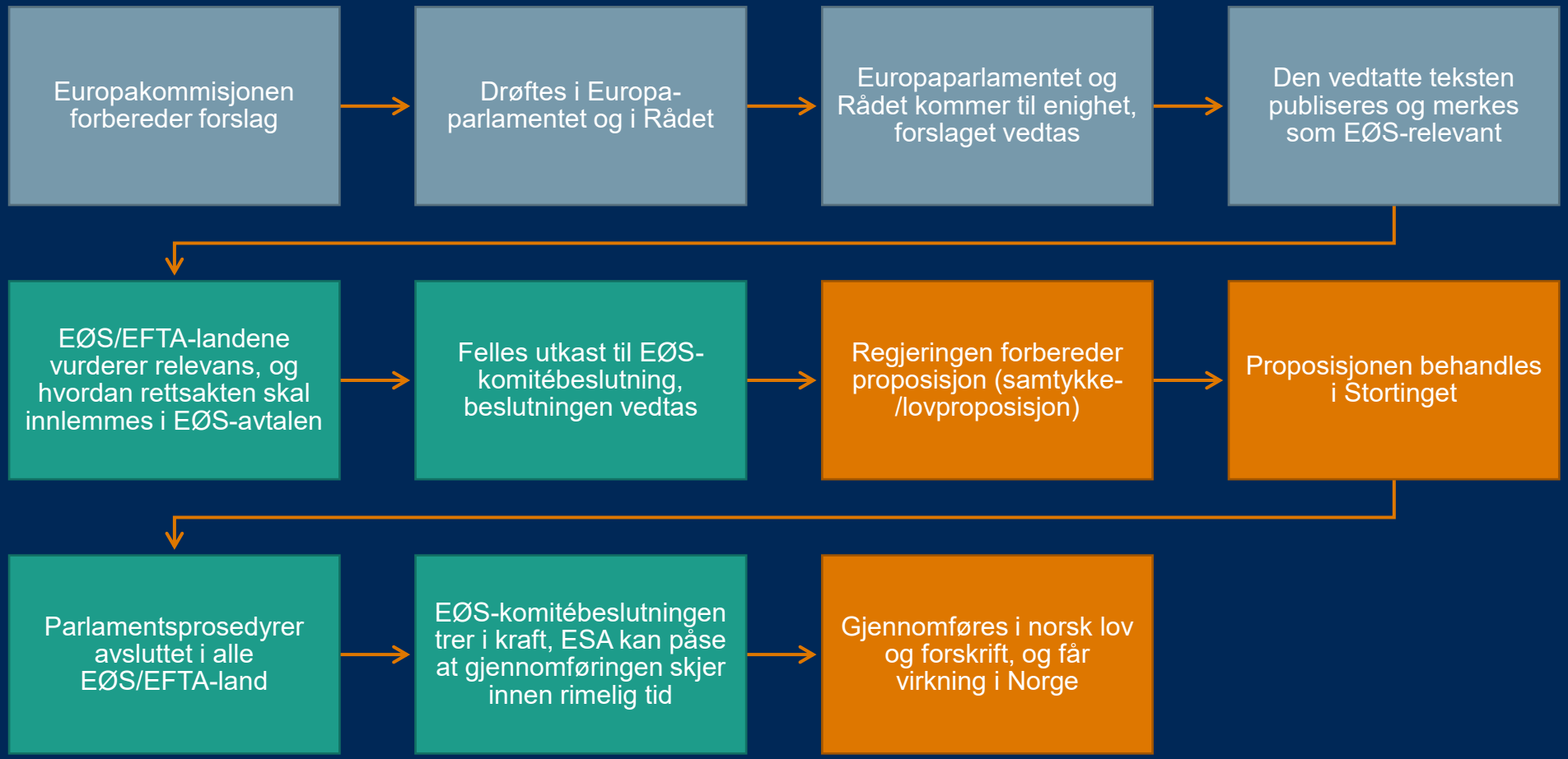
Prop. 109 LS (2022-2023) Lov om digital sikkerhet

NIS 2 (2022)

Ny lovproposisjon NIS2

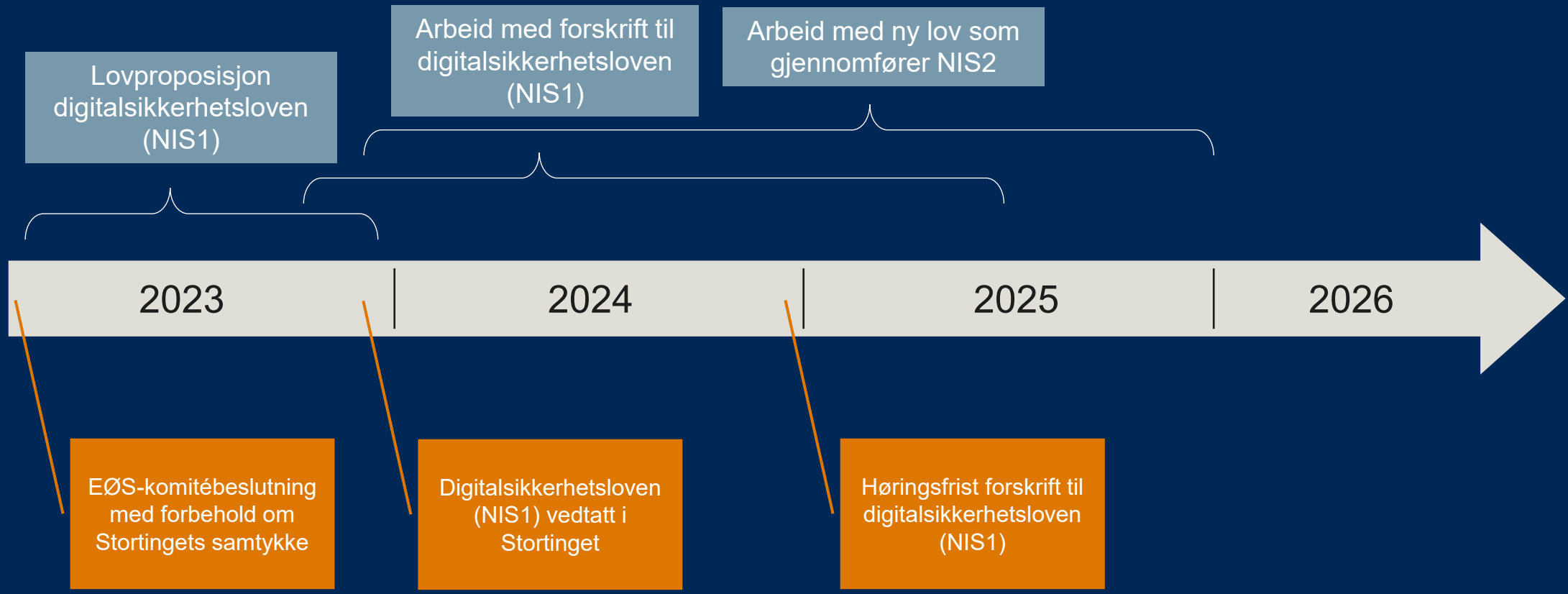
NSM

Hvordan EU-rettsakter blir til norsk rett (forenklet)



Basert på Lovdata/Europalov

Status for regelverksutviklingen



Lov om digital sikkerhet gjennomfører NIS1

- Lov vedtatt i Stortinget i desember 2023
- Forslag til forskrift på høring med frist 11. desember 2024
- 97 høringssvar – til gjennomgang tidlig 2025
- Forskriften skal fastsettes av Justis- og beredskapsdepartementet

NIS2-direktivet ses i sammenheng med CER-direktivet nasjonalt

- Critical Entities Resilience-direktivet (CER) – motstandsdyktighet i samfunnsviktige virksomheter («non-cyber»)
- Ny Stortingsmelding legger opp til en ny lov som gjennomfører både NIS2- og CER-direktivet
- Erstatter digitalsikkerhetsloven

Fremme forslag om ny lov om grunnsikring av samfunnsviktige virksomheter

Regjeringen vil foreslå en ny lov om grunnsikring av samfunnsviktige virksomheter. Loven skal ses i sammenheng med arbeidet med å forberede implementeringen av direktivene om sikkerhet i nettverk og informasjonssystemer (NIS2-direktivet) og kritiske enheters motstandsdyktighet (CER-direktivet). Den nye loven skal stille felles krav til grunnsikring hos virksomheter som er viktige for at samfunnet fungerer, i fred, krise og krig.

Kilde: Meld. St. 9 (2024–2025)
Totalberedskapsmeldingen — Forberedt på kriser og krig
10. januar 2025

NSM

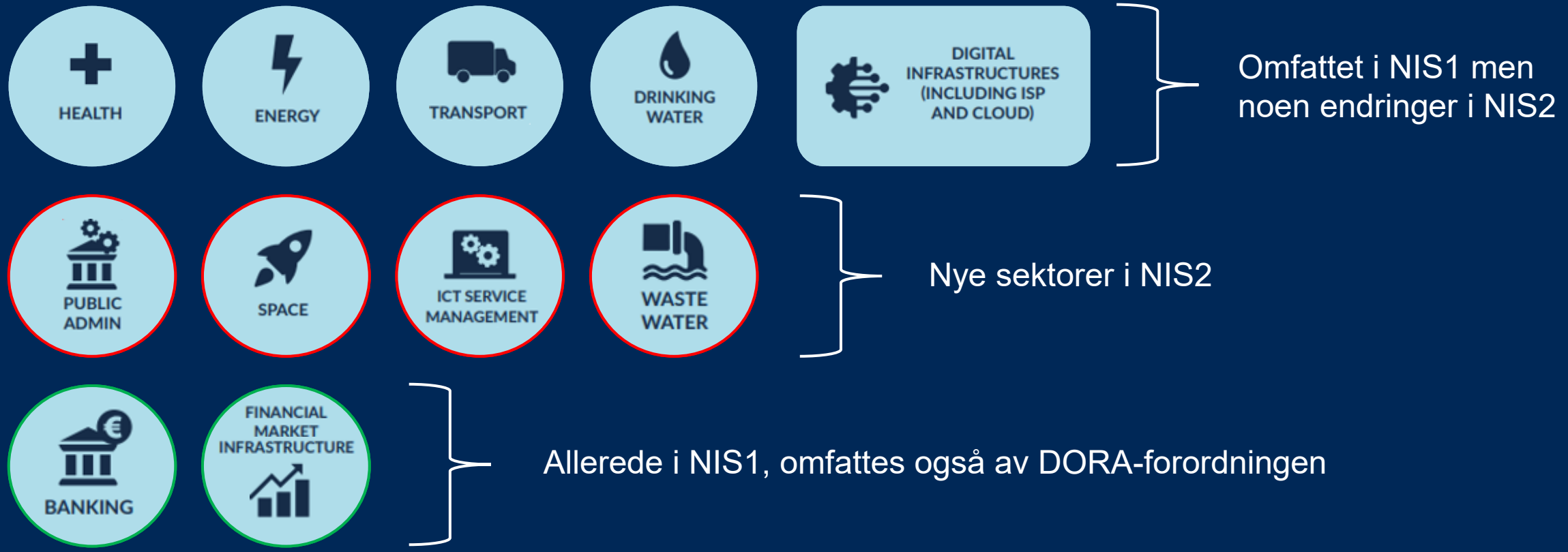
Overordnede krav i NIS-direktivet

Hvert land skal sørge for et økt nivå av digital sikkerhet ved å:

1. Pålegge virksomheter plikt til å iverksette tiltak for digital sikkerhet
2. Pålegge virksomheter varslingsplikt til myndighetene ved alvorlige IKT-sikkerhetshendelser som er egnet til å ramme samfunnsviktige tjenester
3. Utarbeide en nasjonal strategi for digital sikkerhet
4. Etablere eller utpeke tilsynsmyndigheter for digital sikkerhet
5. Etablere eller utpeke et nasjonalt kontaktpunkt overfor andre land
6. Etablere eller utpeke responsmiljøer (CSIRTs)

NSM

Virkeområde – «Sectors of high criticality» (NIS2 vedlegg I)



Kilde: NCSC-IE

NSM

Virkeområde – «Other critical sectors» (NIS2 vedlegg II)

Kilde: NCSC-IE

NSM

Noen områder er særlig relevante for kommunene

Opp til hvert enkelt land om lokal offentlig forvaltning *i seg selv* skal omfattes ut fra en risikovurdering

Noen sektorer der kommunene kan være tjenestetilbydere eller eiere

Terskelverdier som utgangspunkt – hovedregel (NIS2)

Sektor (NIS2)	Store virksomheter (>= 250 ansatte)	Mellomstore virksomheter (50-249 ansatte)	Små virksomheter
Vedlegg I	KRITISKE	VIKTIGE	*Ikke omfattet*
Vedlegg II	VIKTIGE		*Ikke omfattet*

- Følger etablert definisjon i EU for små, mellomstore og store virksomheter
- I tillegg til antall ansatte kommer terskler knyttet til omsetning

NSM

Terskelverdier som utgangspunkt – noen spesielle unntak (NIS2)

Sektor (NIS2)	Type virksomhet	Store virksomheter	Mellomstore virksomheter	Små virksomheter
Digital infrastruktur	Kvalifiserte tillitstjenester	KRITISKE	KRITISKE	KRITISKE
	DSN-tjenestetilbydere, unntatt rotnavnetjenere	KRITISKE	KRITISKE	KRITISKE
	Toppnivådomeneregister	KRITISKE	KRITISKE	KRITISKE
	Tilbydere av elektronisk kommunikasjon	KRITISKE	KRITISKE	VIKTIGE
	Ikke-kvalifiserte tillitstjenester	KRITISKE	VIKTIGE	VIKTIGE
Offentlig forvaltning	Sentral offentlig forvaltning, unntatt nasjonal og offentlig sikkerhet, forsvar, domstoler, nasjonalforsamlinger, sentralbanker	KRITISKE	KRITISKE	KRITISKE
	Regional offentlig forvaltning, opp til det enkelte land om lokal offentlig forvaltning skal omfattes ut fra en risikovurdering	VIKTIGE	VIKTIGE	VIKTIGE

- Noen typer virksomheter omfattes uavhengig av størrelse
- Virkeområdet må vurderes nærmere i en ny lov som gjennomfører NIS2 i Norge

NSM

Cybersecurity risk-management measures (NIS2 art. 21)

- Iverksette hensiktsmessige og proporsjonale tiltak for å håndtere risiko knyttet til nettverk og informasjonssystemer
- Skal ta hensyn til beste praksis, internasjonale/europeiske standarder, og kostnader, for å sikre at tiltakene er tilpasset den identifiserte risikoen knyttet til nettverk og informasjonssystemer
- Proporsjonalitet vurderes ut fra virksomhetens eksponering, størrelse og betydning, og sannsynligheten for uønskede hendelser
- «All hazards approach»

NSM

Cybersecurity risk-management measures (forts.)

Det forebyggende sikkerhetsarbeidet i virksomheten skal minst omfatte:

- Informasjonssikkerhetspolicy for virksomheten og retningslinjer for risikovurderinger
- Planer for hendelseshåndtering
- Planer for driftskontinuitet, inkludert backup og gjenoppretting
- Sikkerhet i leverandørkjeder
- Sikkerhet i anskaffelser, utvikling og vedlikehold av informasjonssystemer, inkludert deling av informasjon om sårbarheter
- Retningslinjer og rutiner for å vurdere effekten av sikkerhetstiltak
- Grunnleggende informasjonssikkerhetstiltak og opplæring av personell
- Retningslinjer og rutiner for tilgangskontroll og personellsikkerhet
- Retningslinjer og rutiner for bruk av kryptering der dette er hensiktsmessig
- Retningslinjer og rutiner for bruk av flerfaktorautentisering og kontinuerlig autentisering, og sikre tale-, meldings- og videotjenester, der dette er hensiktsmessig

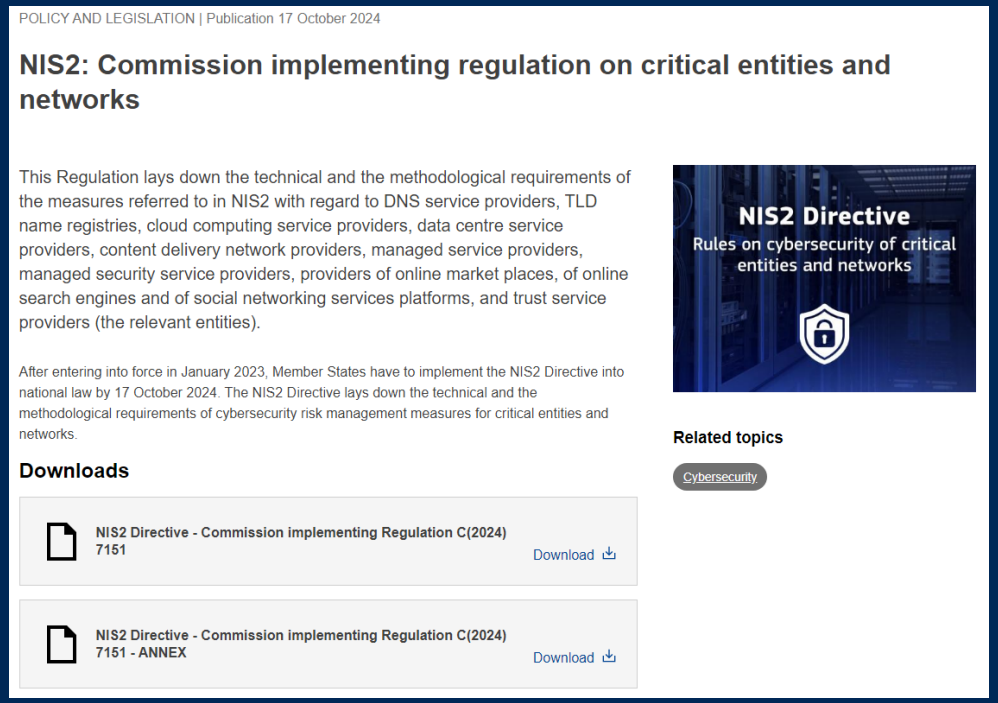
NSM

Ny *gjennomføringsrettsakt* utdyper krav til digital infrastruktur

- Vedtatt i EU 17. oktober 2024
- Utdyper begrepet «betydelig hendelse» som ligger til grunn for varslingsplikten
- Vedlegget utdyper sikkerhetskravene i artikkel 21 (NIS2)

Gjelder for

- Skytjenesteleverandører
- Datasentertjenesteleverandører
- DNS
- Registerenhet for toppnivådomene (TLD)
- CDN
- Administrerte IKT-tjenester, administrerte sikkerhetstjenester
- Tillitstjenester
- … og digitale tjenestetilbydere: Nettbaserte markedsplasser, søkemotorer og sosiale medier-plattformer


POLICY AND LEGISLATION | Publication 17 October 2024

NIS2: Commission implementing regulation on critical entities and networks

This Regulation lays down the technical and the methodological requirements of the measures referred to in NIS2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (the relevant entities).

After entering into force in January 2023, Member States have to implement the NIS2 Directive into national law by 17 October 2024. The NIS2 Directive lays down the technical and the methodological requirements of cybersecurity risk management measures for critical entities and networks.

Related topics

Cybersecurity

Downloads

NIS2 Directive - Commission implementing Regulation C(2024) 7151 — Download

NIS2 Directive - Commission implementing Regulation C(2024) 7151 - ANNEX — Download

NSM

Vedlegget til gjennomføringsrettsakten utdyper krav om:

1. Policy on the security of network and information systems
2. Risk management policy
3. Incident handling
4. Business continuity and crisis management
5. Supply chain security
6. Security in network and information systems acquisition, development and maintenance
7. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
8. Basic cyber hygiene practices and security training
9. Cryptography
10. Human resources security
11. Access control
12. Asset management
13. Environmental and physical security

NB: Europakommisjonen har hjemmel i NIS2 til å vedta tilsvarende rettsakter for andre typer virksomheter

NSM

Varslingsplikten (NIS2 Art. 23) - når skal virksomheten varsle?

- Virksomheter skal varsle om betydelige hendelser som rammer nettverk og informasjonssystemer, som er egnet til å påvirke tjenesteleveransen
- "All hazards" – ikke avgrenset til tilsiktede handlinger, ikke avgrenset til cyberdomenet

Det legges opp til følgende frister for varsling:

- "Early warning" uten unødig opphold og senest innen 24 timer
- Statusoppdatering innen 72 timer – deretter statusoppdatering ved behov
- Utdypende hendelsesrapport innen én måned

- Virksomheten skal også varsle kunder/brukere om alvorlige hendelser

NSM

Hvem skal virksomheten varsle til?

- Direktivet legger opp til kontinuitet – og *lov om digital sikkerhet* legger opp til å benytte eksisterende myndighetsstruktur i størst mulig grad
- Departementene utpeker myndigheter med sektoransvar som skal føre tilsyn og gi veiledning tilpasset sektorens egenart – sannsynligvis vil eksisterende sektortilsyn få viktige roller

NSM

Roller og oppgaver i tre spor

NSM

Forholdet til sektorregelverk

- Noen av kravene er delvis ivaretatt i gjeldende sektorregelverk i dag
- Men krav i ulike sektorregelverk varierer
  - Stilles i varierende grad konkrete krav til digital sikkerhet
  - Krav om varsling til myndighet ved uønskede hendelser varierer
  - Tilsyn med og kompetanse innen digital sikkerhet varierer
- Der krav i sektorregelverk minst tilsvarer kravene som følger av ny lov om digital sikkerhet, medfører ny lov sannsynligvis ikke store endringer for virksomhetene
- Dersom det *ikke* stilles tilsvarende krav til digital sikkerhet eller krav om varsling i sektorregelverk, så vil slike krav følge av ny lov, eventuelt gjennom tilpasninger i sektorregelverk

NIS og lov om digital sikkerhet kan forstås som en «grunnplanke» for digital sikkerhet som stiller minimumskrav på tvers av viktige tjenesteleverandører i ulike sektorer

NSM

Fra «soft law» til kodifisering innen digital sikkerhet?

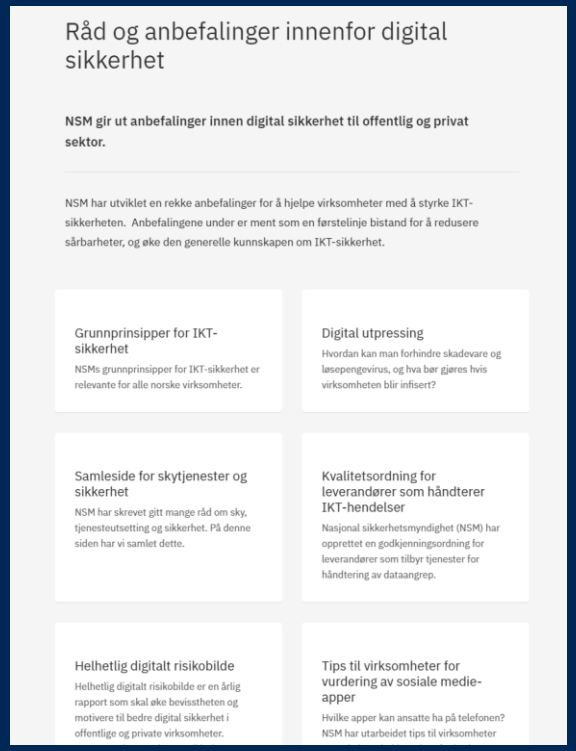
Med noen viktige unntak som det sikkerhetsgraderte og personvern, har digital sikkerhet historisk ofte vært regulert gjennom såkalt «soft law»

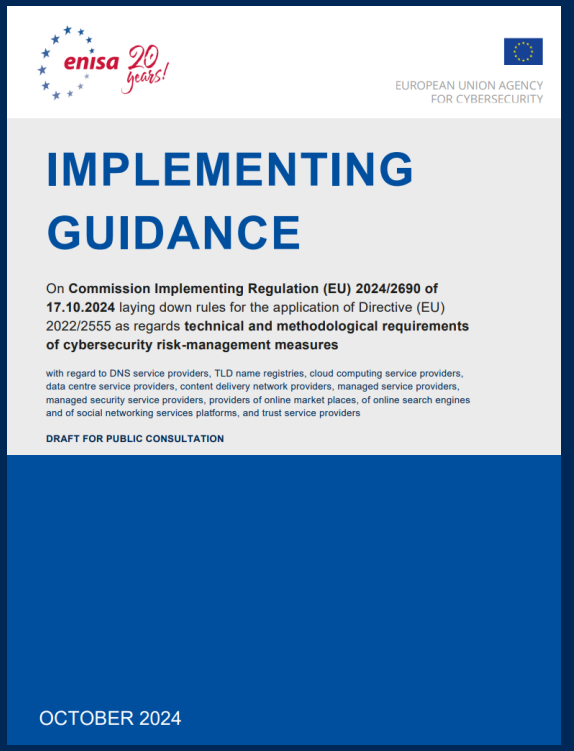
- Ikke-bindende men normativt
- Standarder, anbefalinger, retningslinjer, «beste praksis» eller prinsipper som påvirker atferd og beslutninger

NIS/NIS2 representerer en kodifisering eller overgang til rettslig bindende krav

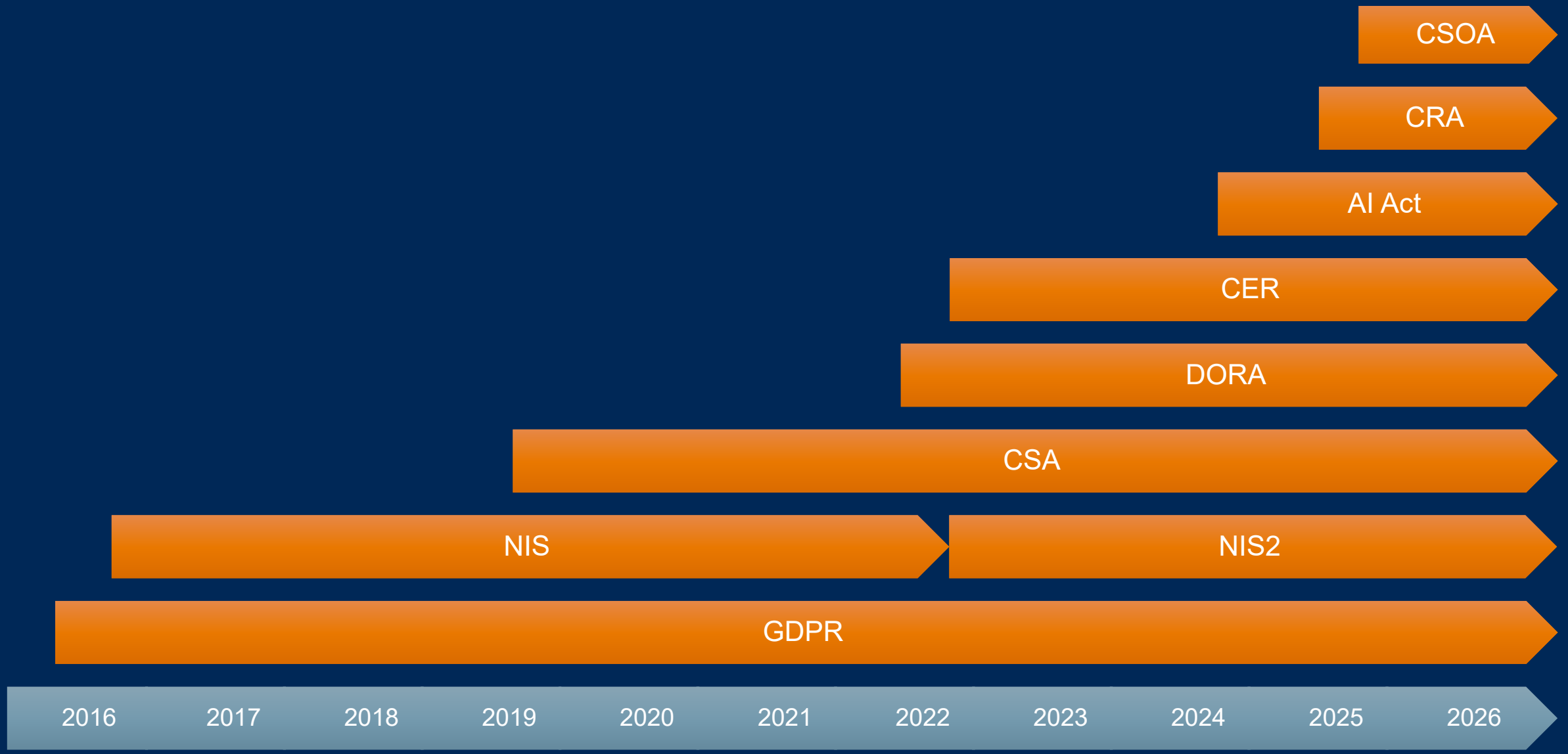
- Normer, anbefalinger og god praksis blir tydeligere rettslig forankret
- Krav om risikostyring og varsling
- Tilsyn og overtredelsesgebyrer

Veiledning til virksomheter – evolusjon, ikke revolusjon





NSM


CSOA
CRA
AI Act
CER
DORA
CSA
NIS
NIS2
GDPR
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026

NSM

Noen spørsmål virksomheter bør drøfte

- Har vår virksomhet definert mål, strategier og policy for digital sikkerhet?
- Har vi god oversikt over informasjonssystemer som er viktige for å ivareta våre kritiske aktiviteter?
- Kjenner vi konsekvensene for vår virksomhet dersom data og informasjonssystemer blir utilgjengelige, endres eller blir kjent for uvedkommende?
- Arbeider vi systematisk med risikohåndtering, inkludert for digital sikkerhet? Bygger dette på anerkjente standarder og rammeverk for digital sikkerhet?
- Har vi iverksatt sikkerhetstiltak som er tilpasset vårt risikobilde?
- Hvilke kritiske avhengigheter har vi i våre leverandørkjeder? Hvilke leverandører er vi avhengige av for at våre informasjonssystemer skal være sikre og fungere? Hvilke krav stiller vi til leverandører?
- Har vi en oppdatert plan for hendelseshåndtering innen digital sikkerhet?
- Er vårt arbeid med forebyggende digital sikkerhet og vår sikkerhetsorganisasjon forankret i ledelsen? Rapporterer vi til ledelsen på mål og strategier for digital sikkerhet?

Svarene kan gi en indikasjon på modenhet og områder virksomheten bør prioritere

Tlf. 67 86 40 00
www.nsm.no