Værdien af standarder ift. europæisk lovgivning på cyberområdet

18. september 2023

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- 182 medarbejdere (april 2022)
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

Standarder får verden til at fungere lidt bedre

Billeder fra Standard Norge.

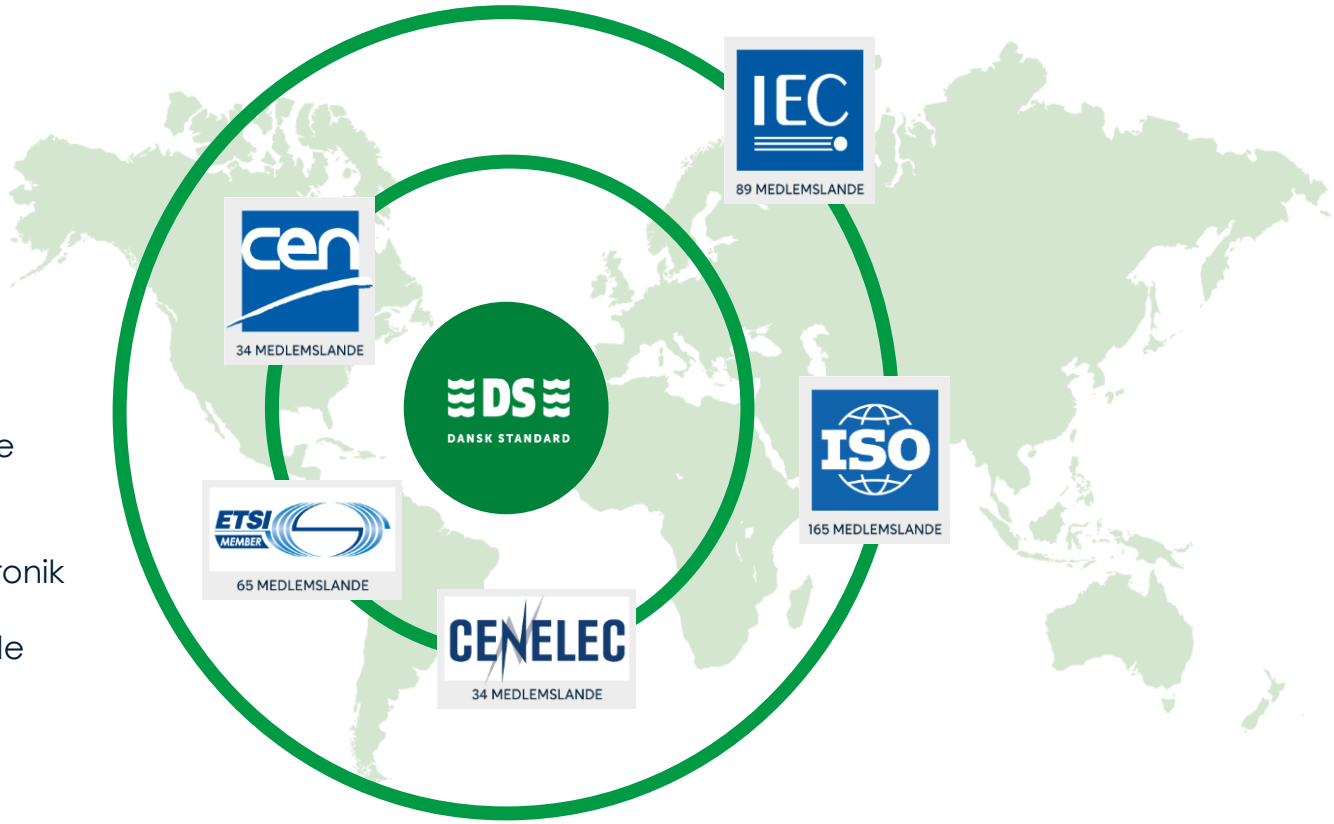
Din adgang til europæisk og international standardisering

- International standardiseringsorganisation
- 167 medlemmer fra hele verden
- Mere end 23.000 publicerede standarder

- International organisation for elektronisk standardisering
- 89 medlemmer fra hele verden

- Europæisk standardiseringsorganisation
- 34 medlemmer
- Anerkendt af EU-Kommissionen til at udvikle og godkende europæiske standarder

- Europæisk organisation der udvikler standarder for elektronik
- 34 medlemmer
- Anerkendt af EU-Kommissionen til at udvikle og godkende europæiske standarder



- Europæisk organisation der udvikler standarder og informations- og kommunikationsteknologier
- Mere end 900 medlemmer i hele verden fra 65 forskellige lande
- Anerkendt af EU-Kommissionen til at udvikle og godkende europæiske standarder

Koblingen mellem standarder og EU-regulering

Standarder er frivillige indtil nogen gør dem bindende

- Aftale mellem 2 parter
- Love, bekendtgørelser, regler
- **EU-lovgivning**

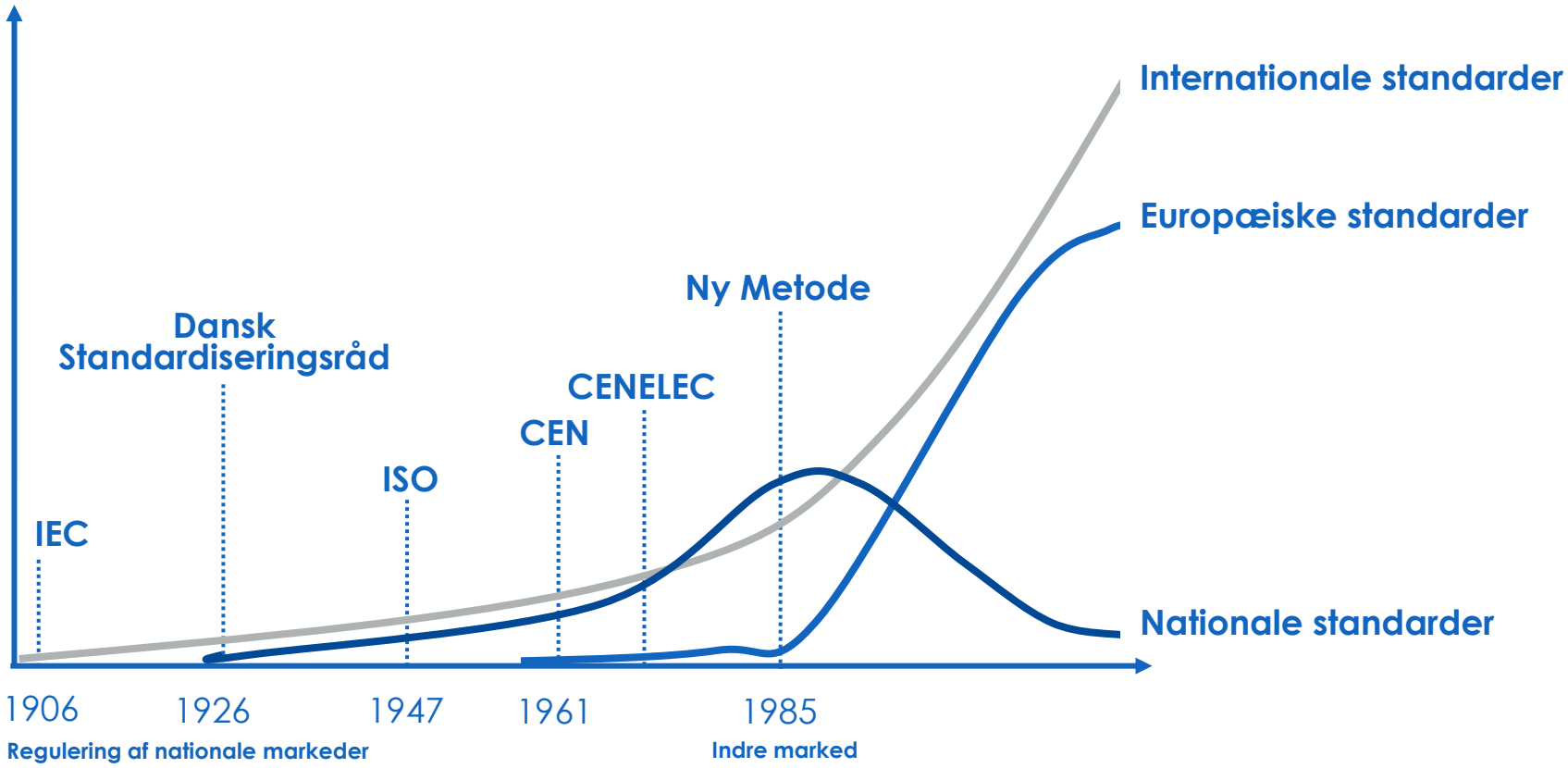
Standardernes rolle ift. europæisk lovgivning

Standarder anvendes til at udfylde lovgivning: harmoniserede standarder – standardiseringsanmodninger

Standarder kan anvendes som inspiration til og evt. forløber for lovgivning

Standarder som et alternativ til lovgivning: markedsregulering

Standarder er et vigtigt redskab i globaliseringen



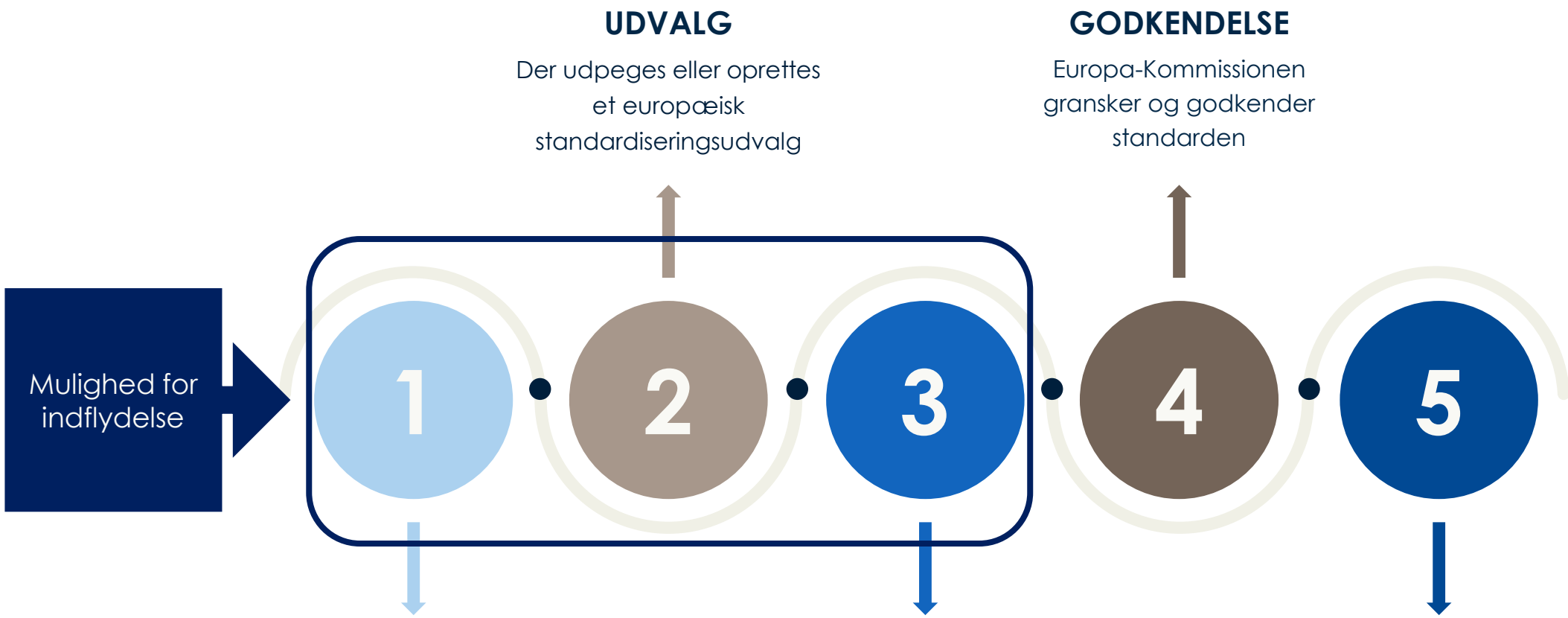
EU-kommissionen bruger standardisering til at skabe harmonisering

Gamle metode:
- Alle produktkrav i politisk proces
- Langsomt
- Besværligt

1985

Den Nye Metode:
- Rammedirektiv med de væsentlige krav
- Produktkrav i standarder
- Mandat og kontrakt
- Harmoniserede standarder

Fra EU-lovgivning til standard



ANMODNING

Europa-Kommissionen udsteder en standardiseringsanmodning

UDVALG

Der udpeges eller oprettes et europæisk standardiseringsudvalg

UDARBEJDELSE

Nationale eksperter kan skrive og kommentere udkast

GODKENDELSE

Europa-Kommissionen gransker og godkender standarden

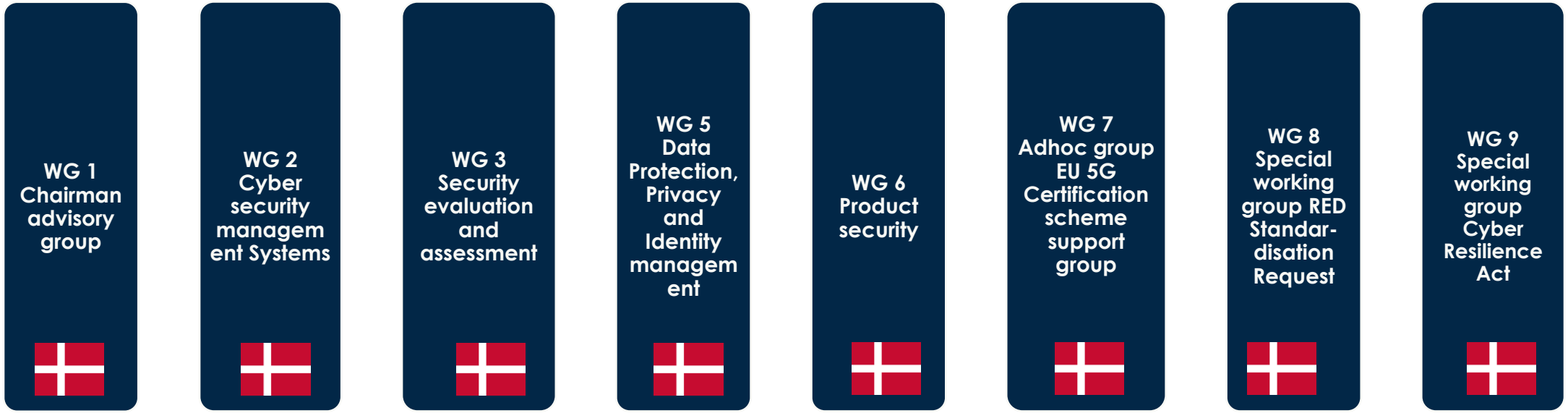
OFFENTLIGGØRELSE

Standarden offentliggøres i EU's officielle Tidende (OJEU)

Europæisk standardisering på cyberområdet

Europæisk standardisering – cyber- og informationssikkerhed

JTC 13 Cybersecurity and Data Protection



Derudover Ad Hoc Grupper om cybersecurity of AI og post quantum.

Deltagende eksperter: Brugere, undervisere, praktikere, "produkt-ejere" etc.

Formålet med Europæisk standardisering ift. cyber- og informationssikkerhed

- Udvikle europæiske standarder, der imødekommer de europæiske behov. Evt. i forbindelse med at understøtte europæisk regulering

- Adoptere internationale standarder som europæiske.

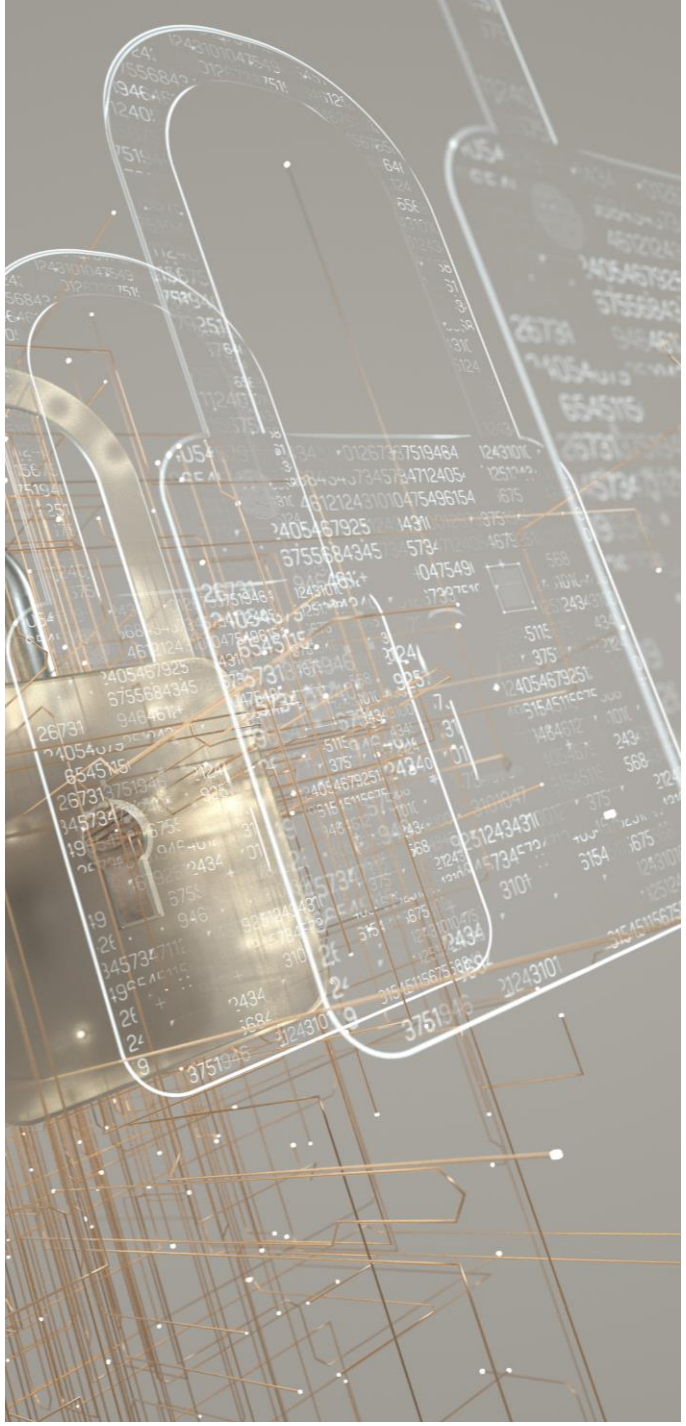
Det europæiske standardiseringsarbejde foregår i tæt dialog med henholdsvis ENISA (The European Union Agency for Cybersecurity) og Europakommissionen.

Europæiske standarder for cyber- og informations-sikkerhed

39 udgivne standarder (alle undtagen fire er ISO/IEC standarder, der er adopteret)

26 standarder under udvikling (heraf 12 ISO/IEC standarder, der skal adopteres og 14 nye)

- Managed Security Services Providers Requirements
- Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services
- Requirements for Conformity Assessment Bodies certifying Cloud Services
- **EN 18031-1 Common security requirements for internet connected radio equipment (M/585)**
- **EN 18031-2 Common security requirements for radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment (M/585)**
- **EN 18031-3 Common security requirements for internet connected radio equipment processing virtual money or monetary value (M/585)**
- **CEN/CLC TR Privacy management in products and services - Biometric access control products and services (M/530)**
- EN 17740 Requirements for professional profiles related to personal data processing and protection
- EN 17799 Personal data protection requirements for processing operations
- **EN 17926 Privacy Information Management System per ISO/IEC 27701 - Refinements in European context**
- EN 17927 Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products
- Scheme for certification of PII processing operations against JTC013037 (EN 17926)
- Scheme for certification of personal data processing operations against EN 17799
- Guidelines on sectoral cybersecurity assessment



Cyber- og informationssikkerhed

Danske virksomheder og organisationer skal forholde sig til en del lovgivning på cyberområdet:

- **NIS2**
- DORA
- Cyber Security Act
- Cyber Solidarity Act
- **Radioudstyrsdirektivet – cybersikkerhedskrav**
- **Cyber Resilience Act**

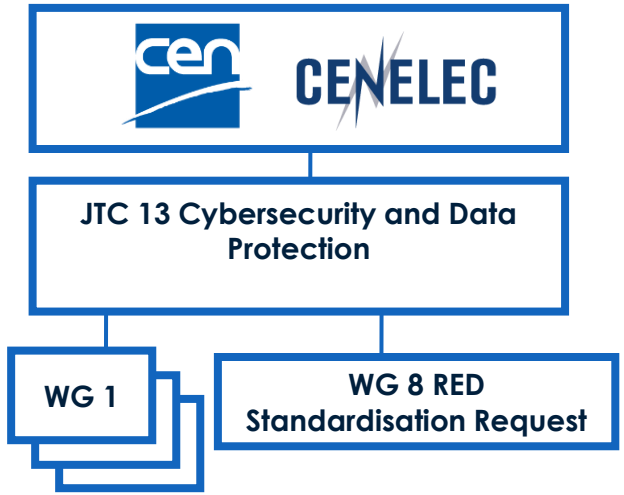
NIS2 direktivet

Ingen direkte krav til standarder, men anbefalinger om at kigge i den retning.

> Artikel 25
>
> Standardisering
>
> 1. For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

ISO/IEC27001 og ISO/IEC 27002 er et godt udgangspunkt for arbejdet med NIS2 compliance. De minimumskrav der er opstillet i NIS2 flugter godt med de krav og foranstaltninger, som standarderne opererer med.

Radioudstyrsdirektivet - tre harmoniserede standarder undervejs



EN 18031-1 Common security requirements for radio equipment – Part 1: Internet connected radio equpment

EN 18031-2 Common security requirements for radio equipment – Part 2: Radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

EN 18031-3 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

Cyber Resilience Act

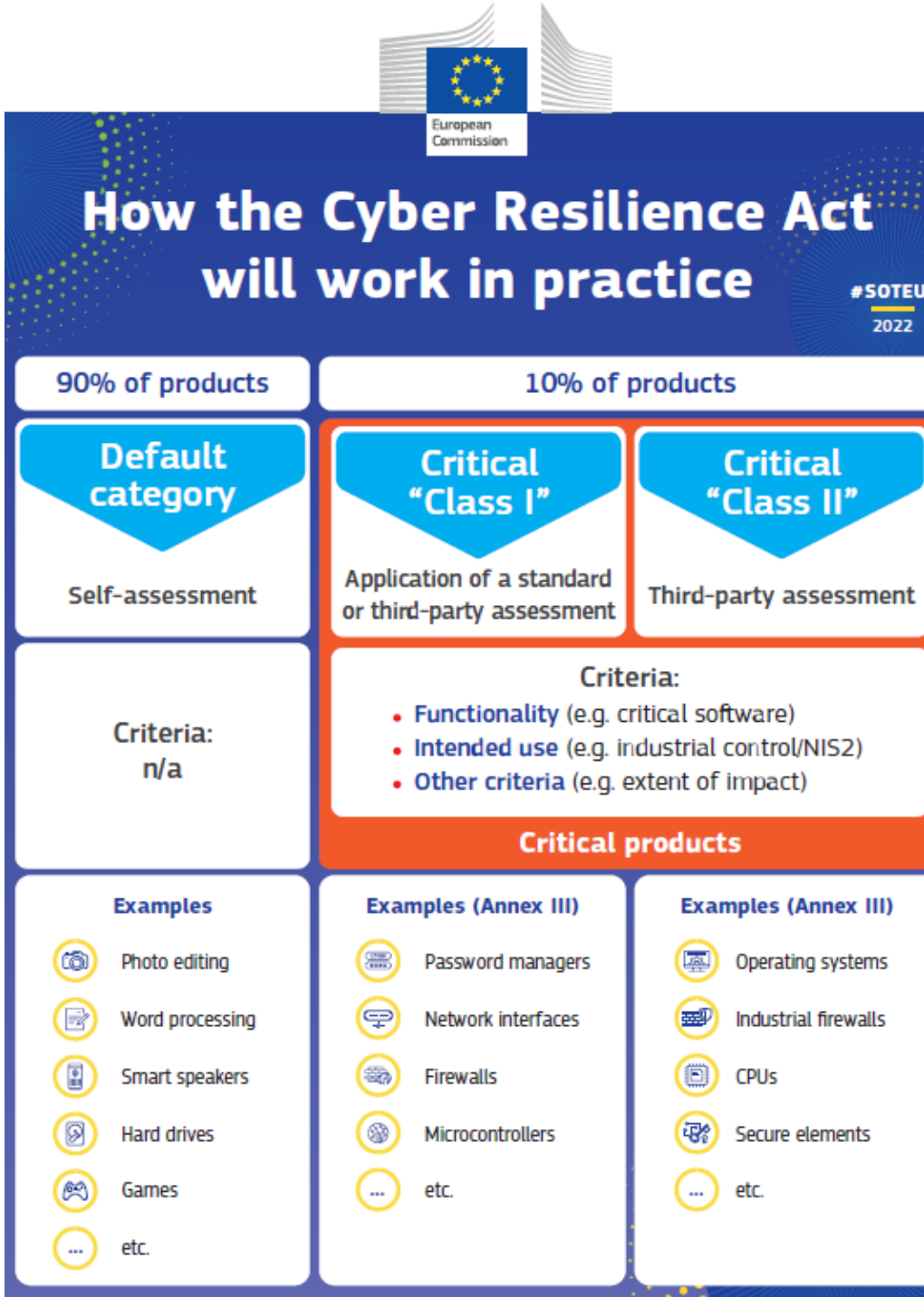
Krav om fokus på cybersecurity i design og udvikling af produkter med digitale elementer.

Følger New legislative Framework - Conformity assessment (selvvurdering eller via tredjepart) CE-mærkning.

CEN/CLC har udarbejdet et position paper til forslaget ift. Cyber Resilience Act.

Der er udarbejdet et udkast til en standardiseringsanmodning, der fremsætter en lang række krav. Der nedsættes nu en gruppe, der drøfter det udkast.

CEN/CLC bliver modtagere at den kommende standardiseringsanmodning. Der er allerede nedsat en arbejdsgruppe til formålet i den europæiske komité. De er allerede i gang med det forberedende arbejde.



Spørgsmål?

Kontakt

Berit Aadal
Seniorkonsulent

Dansk Standard
Göteborg Plads 1
DK-2150 Nordhavn
E-mail: baa@ds.dk
D: +45 39966296
M: +45 26224696