EU's initiativer inden for cybersikkerhed

24. maj 2022

- Der er mulighed for at stille spørgsmål undervejs gennem chatten.
- Præsentationerne sendes ud efterfølgende
- Vi optager webinaret

Dagens program

EU's største tech-initativer på det regulatoriske område

v/ Jesper Løffler Nielsen, Focus Advokater

Hvad er de nye krav i NIS2?

v/ Kia Slæbæk Jensen, Center for Cybersikkerhed

Hvad kommer der til at ske ift. Cybersecurity Act?

v/ Winn Nielsen, Erhvervsstyrelsen

Europæiske standarder for cyber- og informationssikkerhed

v/ Berit Aadal, Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- 168 medarbejdere (jan. 2021)
- 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.

Hvorfor er vi her i dag?

If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces.

And we should not just be satisfied to address the cyber threat, but also strive to **become a leader in cyber security**. It should be here in Europe where cyber defence tools are developed.

-Ursula von Der Leyen
State of the Union, 2021

FOCUS
ADVOKATER

EU's Digital Decade
– med særlig vægt på cybersikkerhed

v/Jesper Løffler Nielsen, Focus Advokater P/S

Jesper Løffler Nielsen

Profil

- Certificeret IT-advokat og associeret partner hos Focus Advokater P/S
- Rådgiver om GDPR, IT-kontrakter, cybersikkerhed samt juridiske aspekter ved nye teknologier

Forskning og undervisning

- Erhvervs-PhD i IT-ret (2013 – 2016)
- Ekstern lektor i IT-ret, Persondataret mv. (2010 -)
- En række UfR-artikler inden for IT-ret og databeskyttelse + enkelte bøger

Andet

- Ekstern DPO
- IDA Databeskyttelse
- Netværksleder for Technology Denmarks netværk: ”Innovation & Compliance”
- Blog om Tech & Jura på www.version2.dk
- Grundlægger af www.techjura.dk

FOCUS ADVOKATER

Agenda

1. Cybersikkerhed er i stigende grad (også) et juridisk anliggende

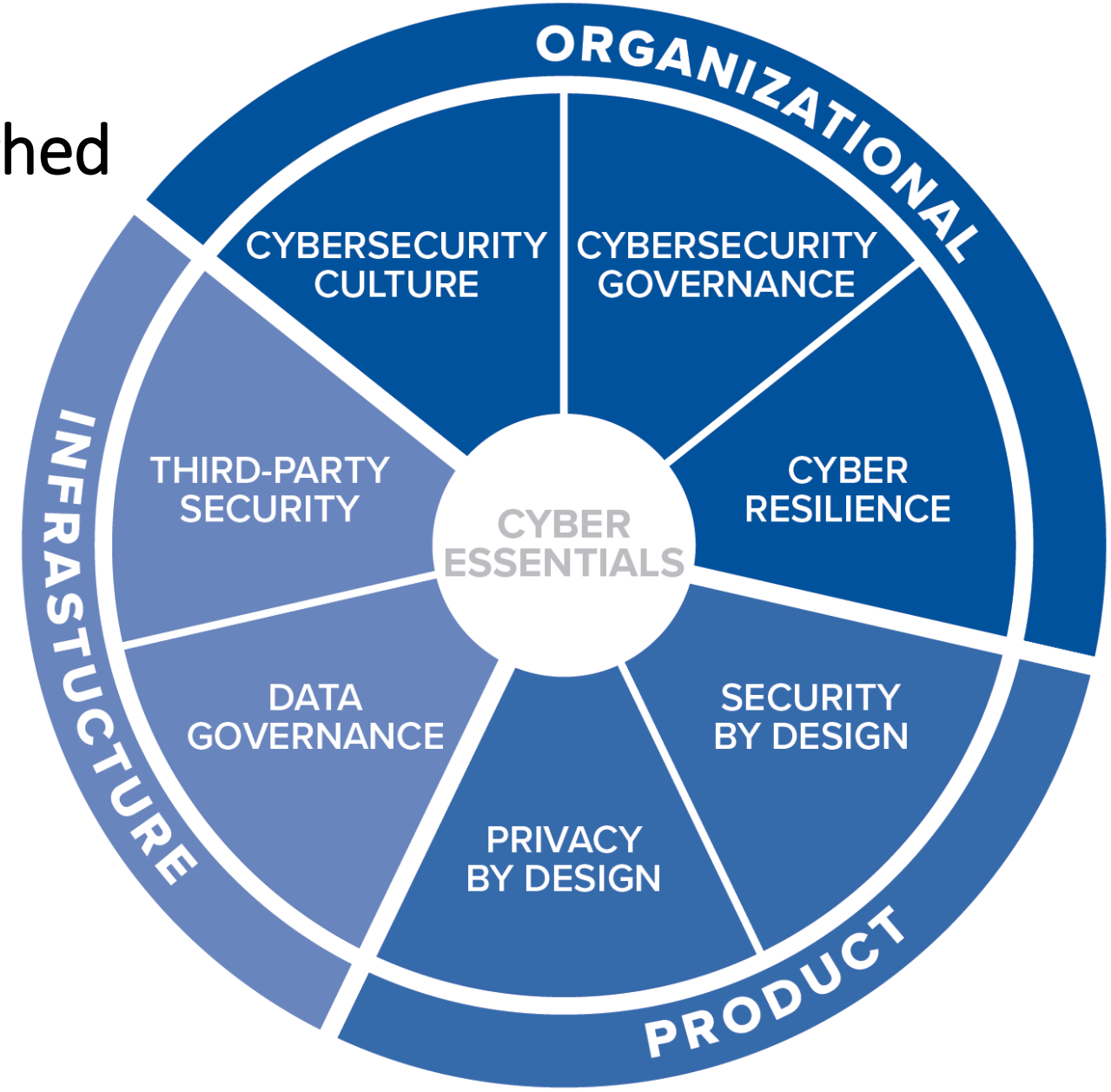
2. EU's regulering af cybersikkerhed

3. Afrunding: En god og en dårlig nyhed

CYBERSIKKERHED ER I STIGENDE GRAD (OGSÅ) ET JURIDISK ANLIGGENDE

Stigende interesse for cybersikkerhed

"A holistic approach to security"
Source: World Economic Forum, 2020



Stigende interesse for cybersikkerhed

Sikkerdigital.dk

- Erhvervsstyrelsens og Digitaliseringsstyrelsens fælles hjemmeside www.sikkerdigital.dk
- Adskillige vejledninger og skabeloner om *sikkerhed* og *leverandørstyring*

Bestyrelsesforeningen

- Vejledning: ”CYBERSIKKERHED FOR BESTYRELSER” (v. 3.0)

D-mærket

- Kriterie 1, 2, 3, 4 og 6 handler (bl.a.) om krav til sikkerheden

Stigende interesse for cybersikkerhed – også i kontrakter og udbud

Ny national strategi for cyber- og informationssikkerhed (december 2021)

- *"**Større fokus på it-sikkerhed ved offentlige it-indkøb og udbud***

  For at højne cyber- og informationssikkerheden hos de offentlige myndigheder, skal det afdækkes, hvordan it-sikkerhedsaspekter i højere grad kan tænkes ind i de offentlige ramme- og indkøbsaftaler, samt hvorvidt it-sikkerhedsniveauet i aftalerne er tilstrækkelig transparent for myndighederne."

- *"**Styrket sikkerhedstilsyn med systemleverandører og databehandlere***

  Der udarbejdes en omkostningseffektiv basismodel for tilsynsopgaven med henblik på at styrke og effektivisere myndighedernes tilsyn med databehandlere og systemleverandører inden for informationssikkerhed og databeskyttelse. På baggrund af resultatet kan der gennemføres en konceptafprøvning af tilsynsmodellen på én eller flere it-systemer i staten."

Overblik over gældende regler

Generelle krav

- Databeskyttelsesreglerne,
  inkl. en række sikkerhedsrelaterede krav

Sektorspecifikke krav

- Krav om/anbefaling ift. offentlige myndigheders efterlevelse af informationssikkerhedsstandarden ISO 2700X
- En række særregler for visse sektorer, herunder tele-, medie- og IT-sektoren, den finansielle sektor, forsyningsvirksomheder, transport, bankvæsen, sundhedssektoren mv.

Indirekte "krav" ift. sikkerhed

- IT-sikkerhed er (i stigende grad) et ledelsesanliggende, også juridisk set
  - Fx Selskabslovens §115, nr. 2: *"sikre en forsvarlig organisation… etableret de fornødne procedurer for risikostyring og interne kontroller"*
- Kun beskyttelse af forretningshemmeligheder, hvis tilstrækkelig sikkerhed
  - Lov om forretningshemmeligheder § 2, nr. 1, litra c

EU'S REGULERING AF CYBERSIKKERHED

FOCUS ADVOKATER

Væsentligste strategier og regulering (ikke udtømmende!)

Cybersikkerhed

- **S: Cybersecurity Strategy**
- (F: ePrivacy)
- F: Cybersecurity Act
- D: NIS2 (!)
- F: DORA (finanssektor) (!)
- D: Critical Entities Resilience (CER)
- F: Cybersecurity Regulation
- F: Information Security Regulation
- ? : Cyber Resilience Act

Data-økonomien

- **S: Data Strategy**
- F: Free Flow of Data
- D: Open Data
- F: Data Governance Act (!)
- F: Data Act
- F: European Health Data Space
- ?: Vehicle Data

Konkrete teknologier

- **S: AI Strategy + Blockchain Strategy**
- F: Platform-to-Business forordning/P2B
- F: Digital Services Act (!)
- F: Digital Markets Act (!)
- F: AI Act
- D: Machinery Directive (revision)
- F: MICA + Pilote Regime (kryptoaktiver)
- F: EUid framework
- ?: Evaluering af produktansvarsreglerne

Type af dokument

S = Strategi
F = Forordning
D = Direktiv

Status

Almindelig tekst = Endeligt vedtaget
(!) = Politisk enighed, endelig ordlyd mangler
Blå = Forhandles pt. i EU
Grå = Varslede regler/Impact Assesment

FOCUS ADVOKATER

EU-regulering med krav til cybersikkerhed (ikke udtømmende)

Lovgivning	Indhold
Cybersecurity Act Vedtaget – Er trådt i kraft	Styrket **samarbejde mellem EU-lande**, flere beføjelser til **ENISA** samt indførelse af nye **cybersikkerheds-certificeringsordninger.** Certificeringsordninger er dog stadig under udarbejdelse.
NIS2-direktivet Politisk aftale maj 2022 - træder i kraft 21 måneder efter endelig vedtagelse	Cybersikkerhedskrav til **en lang række sektorer**. Direktivet er en opfølgning på Net- og informationssikkerhedsdirektivet – bedre kendt som NIS, der trådte i kraft i 2018.
DORA (finanssektor) Politisk aftale i trilog forhandlinger i maj 2022	Cybersikkerhedskrav til **finanssektoren** → skærpede sammenlignet med NIS2
Critical Entities Resilience (CER) Forhandles pt. i EU, men øjensynligt tæt på at opnå enighed	Cybersikkerhedskrav til **kritiske enheder** → skærpede sammenlignet med NIS2
Cybersecurity Regulation + **Information Security Regulation** Forslag fremsat i maj 2022	Krav til *cybersikkerhed* OG *informationssikkerhed* i **EU-institutioner** → skærpede sammenlignet med NIS2
Cyber Resilience Act Pt. høringsperiode frem til 25. maj	(Formentlig) Krav til cybersikkerhed i produkter, med særlig fokus på **IoT og digitale løsninger.**

Krav til produkter (”Security by Design”)

Citat fra EU-Kommissionens Q&A om den nye “Cybersecurity Strategy”

“How will the Internet of Things be made secure?

Every connected thing contains vulnerabilities that can be exploited and affect other services, networks or even entire economies.

Internal Market rules include safeguards against insecure products and services. Certification under the Cybersecurity Act aims at incentivising safe products and services without compromising on performance…

However, we need an even more comprehensive approach. The Commission already plans to update rules under the Radio Equipment Directive. It will also consider new horizontal rules for all connected products and associated services, including a new duty of care for connected device manufacturers to address software vulnerabilities, requiring the continuation of software and security updates as well as ensuring, at the end of life, deletion of personal and other sensitive data. This would complement both the General Product Safety Regulation (which is to be updated in 2021 but does not address cybersecurity directly) and ‘the right-to-repair obsolete software' initiative presented in the Circular Economy Action Plan.”

Vedtaget – I kraft august 2024

Krav til produkter (”Security by Design”)

Ny “Delegated Act” til radioudstyrs-direktivet (Januar 2022)

“Why is the Commission strengthening cybersecurity of wireless devices?

The Commission is concerned that the design of wireless devices sold in the EU does not guarantee a sufficient level of cybersecurity, personal data protection and privacy of their users. In recent years, products have been identified on the EU market that take advantage of a weak level of security of certain categories of wireless devices and are vulnerable to attacks or theft of personal data, or allow recording of children's play.

With the requirements adopted today, manufacturers of wireless devices will now have to include technical features to improve the level of cybersecurity of such devices before placing them on the European market.”

→ Nye standarder er pt. under udarbejdelse

Varslet regulering – pt. i høring

Krav til produkter (”Security by Design”)

(Måske) kommende “Cyber Resilience Act”

“Digital products and ancillary services create opportunities for EU economies and societies. But they also lead to new challenges – when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities.”

Next to essential cybersecurity requirements, the initiative would place obligations on economic operators, and introduce provisions on conformity assessment, on the notification of conformity assessment bodies, and on market surveillance.

In practice, essential cybersecurity requirements – whether they are regulated altogether in one wide-ranging (‘horizontal’) piece of legislation or on an ad hoc basis – would translate into harmonised standards specific for the different categories of products. Globally, developing such cybersecurity standards could contribute to boosting the EU’s leadership on standard setting by shaping standards for digital products and ancillary services that could serve as global benchmarks”

Krav til produkter (”Security by Design”)

ANDRE EKSEMPLER

→ **Maskindirektivet** (pt. under revision)

- Cybersikkerhed har været et emne undervejs i lovgivningsprocessen
- Det forventes, at den endelige ordlyd alene vil henvise til eksisterende regulering, fx at cybersikkerheds-certificering (jf. Cybersecurity Act) bliver en del af *”Conformity Assesments”* for maskiner og robotter i fremtiden

→ **”AI Act”** (forhandles pt. i EU)

- ”High Risk”-løsninger underlægges en række krav til cybersikkerhed, fx i artikel 9 (”*Risk Management System*”) og 15 (”*Accuracy, robustness and cybersecurity*”)

→ **”EU Data Spaces”** (pt. udkast til sundhedssektor, 9 mere på vej):

- *“Technical data infrastructure: participants in common European data spaces will be encouraged to use the common technical infrastructure and building blocks which will allow the data spaces to be built in an efficient and coordinated manner. The common technical infrastructure will have to take due account of the existing and emerging sectoral frameworks, and integrate the cybersecurity-by-design principle and respect the data protection by design and by default obligations enshrined in the General Data Protection Regulation (GDPR)”*

AFRUNDING

Opsummering

Den dårlige nyhed

- Der er rigtig mange lovkrav på vej, som stiller forskellige krav til cybersikkerhed, og pt. er det hele meget uoverskueligt
- Hertil kommer, at man også skal navigere i et stadigt stigende antal standarder, certificeringer mv. med vægt på sikkerhed

Den gode nyhed

Selvom de forskellige lovkrav er meget forskelligt udformet og formuleret, så er grundkravene langt hen af vejen de samme:

- Governance (= politikker og procedurer) + ledelsesforankring
- Risikovurderinger
- Teknisk sikkerhed
- Leverandørstyring
- Incident håndtering
- Awareness, test, audits mv.
- ”Security by Design” (!)

FOCUS ADVOKATER

Stigende krav til ”Governance”/modenhed ift. cybersikkerhed

Krav	GDPR	Sektorkrav (fx NIS2, DORA, RCE, off. myndigheder mv)	ISO27001	D-mærket
Governance, politikker og procedurer + ledelsesforankring	Art. 5(2) + 24	Ja	Ja	Kritierie 1 og 2
Risikovurderinger	Art. 25 + 32 + 35	Ja	Ja	Kritierie 1
Teknisk sikkerhed	Art. 25 + 32	Ja (særligt kryptering)	Ja	Kriterie 3
Leverandørstyring og ”Security by Design”	Art. 25 + 28	Ja	(Ja)	Kriterie 4 og 6
Incident håndtering	Art. 33 + 34	Ja!	(Beredskab)	(Kriterie 1 – Beredskab)
Awareness, test, audits mv.	Art. 5(2) + 24 + 28 + 32	Ja	Ja	(Kriterie 1 og 2)

Stigende krav til ”Security by Design”
(= krav til cybersikkerhed i fysiske og/eller digitale løsninger)

Eksempler på lovkrav

- (GDPR art. 25 → Data Protection by Design)
- (NIS2-direktivet → Krav til leverandørstyring)
- Radioudstyrsdirektivet (pt. under revision)
- Maskindirektivet (pt. under revision)
- AI Act
- Data Spaces
- Cyber Ressillience Act

Standarder, certificeringer mv.

- En lang række vejledninger fra ENISA + kommende “*Cybersecurity Certifications*”
- OWASP, herunder *“Top 10 Securiy Risks”* for fx. “*Web Applications*” og “*IoT*”
- Dansk Standard, fx DS/PAS 2600:2021 (*IoT*)
- ISO/IEC 27400 - *Cybersecurity — IoT security and privacy — Guidelines* (Under udvikling)

Ny hjemmeside: www.techjura.dk

Er stadig i en betaudgave
-
FEEDBACK MODTAGES GERNE

Tech Jura

BETA UDGAVE

Regulering Tech/Jura Leksikon Artikler Om Techjura.d

CENTER FOR CYBERSIKKERHED

NIS2 – formål og forhandlinger

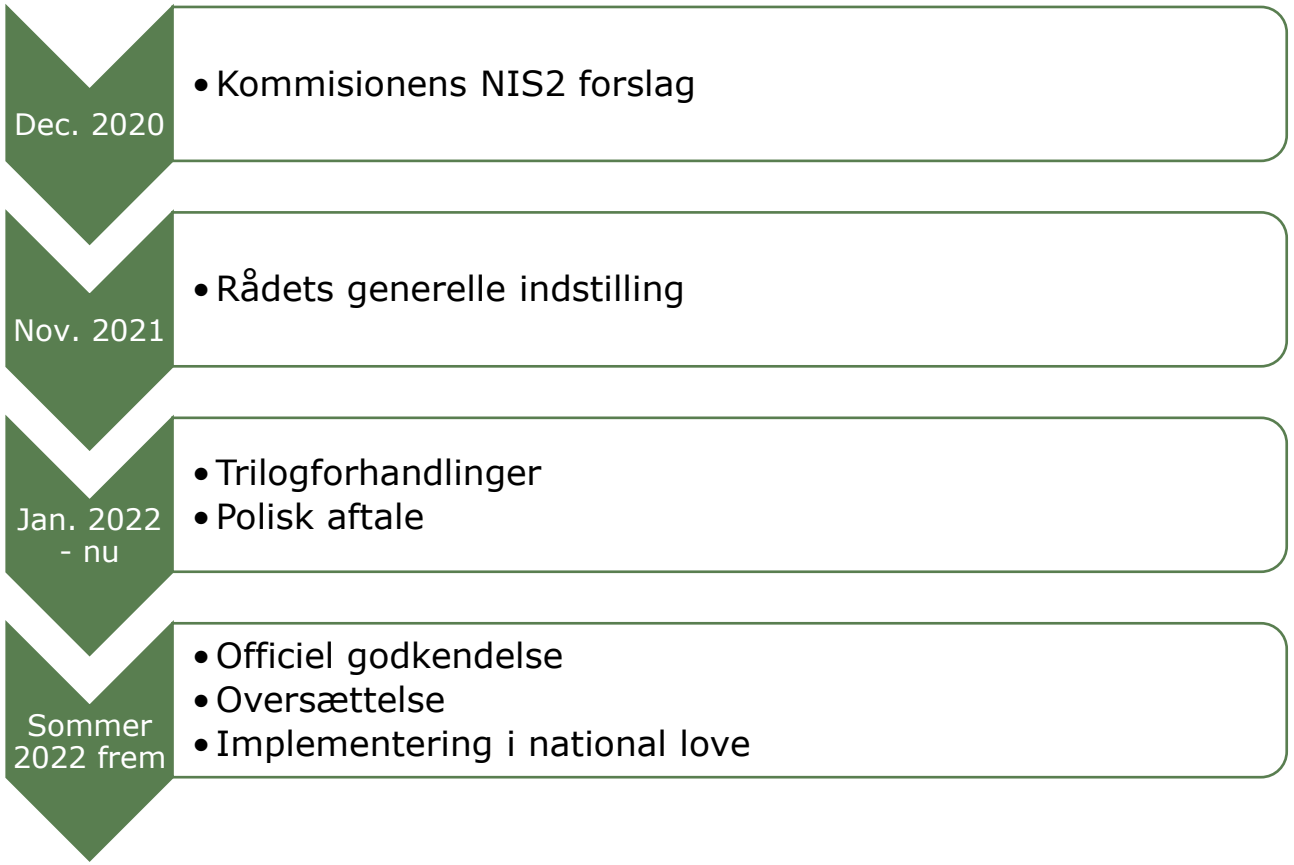
NIS1 vs. NIS2

- Fortsat et direktiv
- Udvidelse af ansvarsområdet
- Mere specifikke krav
- Fra Operatører af Væsentlige Tjenester til Vigtige og Væsentlige Enheder
- Harmonisering både ift. krav, nationale strategier og videndeling
- Minimumslovgivning for fremtidig sektorlovgivning

Formål

- Fælles højt cybersikkerhedsniveau i EU
- Styrke resiliens på cybersikkerhedsområdet
- Sikre væsentlige og vigtige tjenester er beskyttede mod cyber angreb
- Sikre videndeling om grænseoverskridende cyberhændelser
- Sikre fælles udgangspunkt for nationale CSIRT'er, strategier nogle nationale politikker

Status for forhanlingerne



Hvilken betydning får NIS2 (1)

- Ledelsesansvar – ledelsen skal kunne tage beslutninger, have viden og tage ansvar
- Krav til tekniske og organisatoriske foranstaltninger for cybersikkerheden i net- og informationssystemer ved omfattede virksomheder og myndigheder
- Foranstaltninger ved de net- og informationssystemer, der bruges til at levere virksomhedens eller myndighedens samfundsvigtige tjeneste

Tekniske, (operationelle) og organisatoriske foranstaltninger

Foranstaltninger der som minimum skal stilles krav om i national lovgivning	
Politikker for risikoanalyse og informationssystemsikkerhed	Basal computer hygiejne og cybersikkerhedsuddannelse
Håndtering af hændelser	Politikker om brug af kryptografi og kryptering
Driftskontinuitet og krisestyring	HR sikkerhed og adgangskontrol og asset management
Leverandørsikkerhed	Multifaktor autentificering
Sikkerhed ved erhvervelse, udvikling vedligeholdelse af net- og informationssystemer	Politikker og processer til at vurdere effektiviteten af foranstaltningerne

Hvilken betydning får NIS2 (2)

- Udvidet krav om underretning om sikkerhedshændelser (24 timer)
- Øget tilsyn samt udvidede tilsynskapaciteter
- Flere muligheder for håndhævelse, herunder mulighed for bøder

Hvem er omfattet af NIS2?

- Nyt begreb: væsentlige og vigtige enheder
- I specifikke sektorer oplistet i bilag til NIS2
- Generelt store og mellemstore virksomheder samt offentlig forvaltning (der er undtagelser)
- Forskel:
  - Tilsyn: ex ante vs. Ex post
  - Graden af krav kan variere

Sektorer i NIS2: Bilag 1: Samfundsvigtige

- Energi
- Transport
- Søfart
- Bank og finansielle markedsinfrastrukturer (undtages ved DORA)
- Sundhed
- Vand
- Spildevand
- Digital infrastruktur (bl.a. udbydere af internetudvekslingspunkter, DNS-tjeneste, tillidstjenester)
- Rumfart
- Offentlig forvaltning

Sektorer i NIS2: Bilag 2: Understøttende

- Post- og kurertjenester
- Affaldshåndtering
- Fremstilling, produktion o distribution af kemikalier
- Fremstilling, bearbejdning og produktion af fødevarer
- Fremstilling af bl.a. medicinsk udstyr, computere, elektronisk udstyr, maskiner, motorkøretøjer samt andre transportmidler
- Digitale udbydere (udbydere af onlinemarkedspladser, onlinesøgemaskiner, sociale netværkstjenester)

CENTER FOR CYBERSIKKERHED

Kastellet 30 / Holsteinsgade 63
2100 København Ø

Telefon: +45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Forordningen om cybersikkerhed

24. Maj 2022

Winn Nielsen
winnie@erst.dk

ERHVERVSSTYRELSEN

Agenda

- Formål med forordningen om Cybersikkerhed
- Indhold af forordningen
- Status for certificeringsordninger mv.
- Implementering af forordningen i DK
- Målbillede for tværministerielt samarbejde
- Målbillede for cybersikkerhed og Cloud
- Cyber resilience Act

Formål

- Europæisk ramme for cybersikkerhedscertificering af informations- og kommunikationsteknologi
- Understøtte det indre marked ved at øge cybersikkerhedsniveauet i EU
- Harmoniseret tilgang til europæiske cybersikkerhedscertificeringsordninger
- Skabe et digitalt indre marked for IKT-produkter, -tjenester og -processer

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed)

Frivillig ordning

- Cybersikkerhedscertificeringen er **frivillig**, medmindre andet er fastsat af EU eller medlemsstaterne.
- Kommissionen vurderer regelmæssigt effektiviteten og anvendelsen af de vedtagne ordninger, og om ordninger skal gøres obligatoriske.
- Den første vurdering foretages senest den 31. december 2023 og derefter mindst hvert andet år.

Tre tillidsniveauer

- **Grundlæggende**
  Minimere de kendte grundlæggende risici for hændelser og cyberangreb. Evalueringsaktiviteterne skal som minimum omfatte en gennemgang af den tekniske dokumentation.
- **Betydeligt**
  Minimere kendte cybersikkerhedsrisici og risikoen for hændelser og cyberangreb udført af aktører med begrænsede færdigheder og ressourcer.
  Evalueringsaktiviteterne skal som minimum omfatte følgende: en gennemgang med henblik på at påvise, at der ikke er offentligt kendte sårbarheder, og afprøvning af at de nødvendige sikkerhedsfunktioner udføres korrekt.
- **Højt**
  Minimere risikoen for avancerede cyberangreb udført af aktører med betydelige færdigheder og ressourcer.
  Evaluering som ovenfor, samt en vurdering af modstandsdygtighed over for drevne angribere ved hjælp af penetrationstest.

Produkter, tjenester og processer

Forordningen omfatter tre ting:

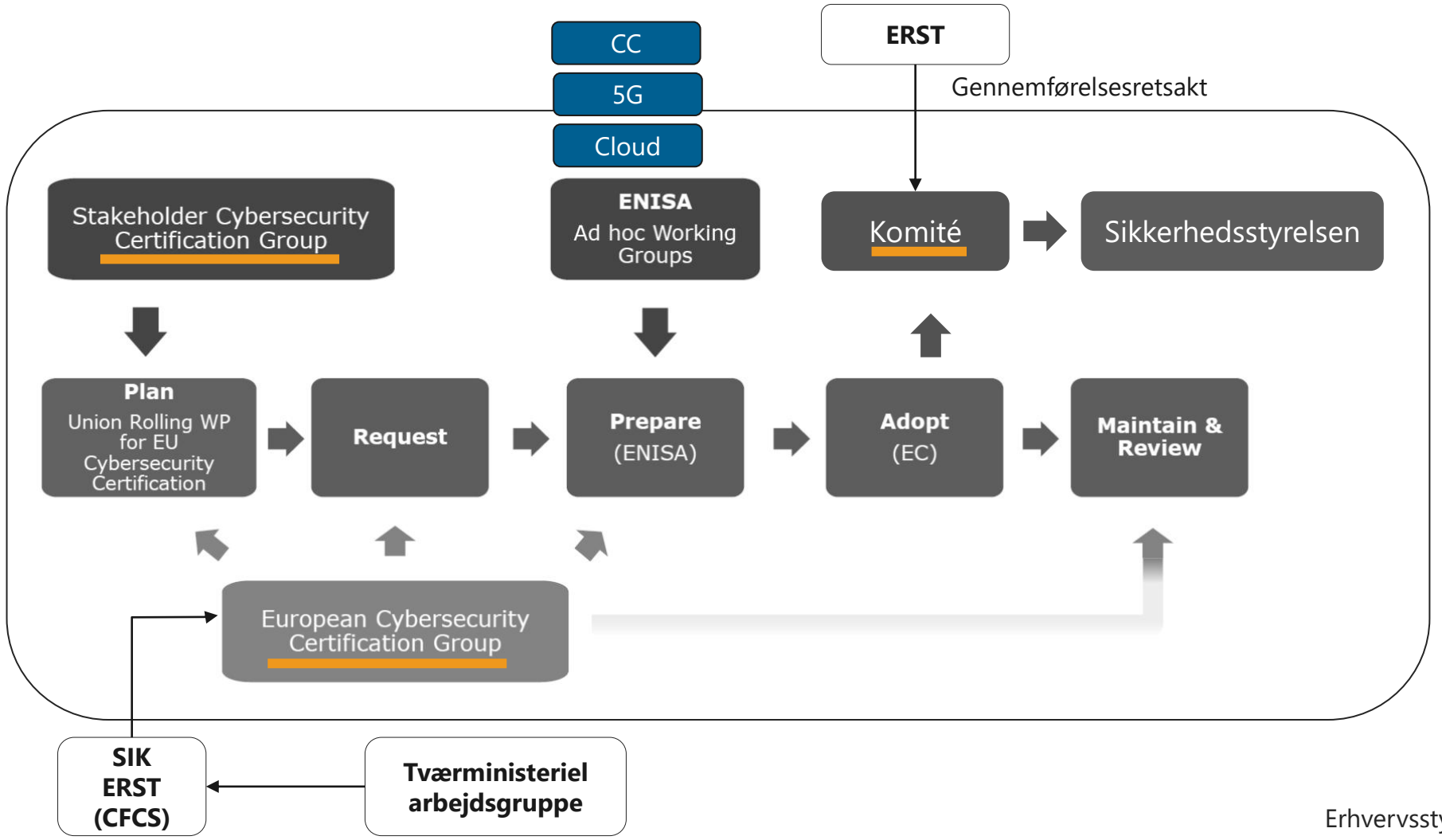
- **Produkter -** Fysiske enheder og softwareprodukter
- **Processer –** Aktiviteter der udføres for at udforme, udvikle, levere eller vedligeholde et produkt eller en service
  - Fx proces for at holde øje med nye sårbarheder
  - Fx udviklingsproces eller kvalitetssikring
- **Tjenester**
  - kan være et "produkt" i sig selv, fx cloud tjenester eller andre services
  - Kan også være opdatering og patchning af produktet

Status på implementeringen

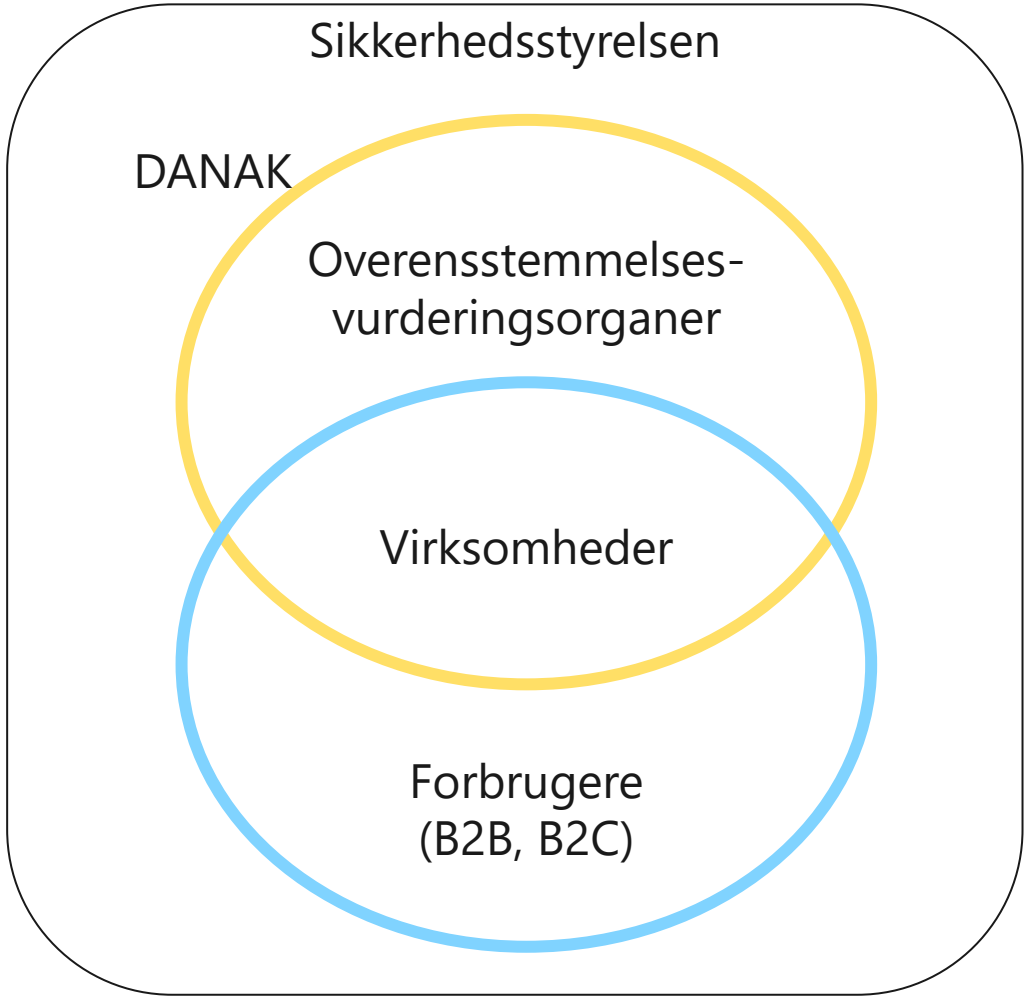
- **Lov,** der udpeger Sikkerhedsstyrelsen som myndighed, i kraft 28. juni 2021
- **Certificeringsordninger på vej**
- **EUCC- Common criteria** (Udkast til gennemførelsesretsakt på vej) bruges primært på højsikkerhedsprodukter, forsvar og betalingskort.
- **Cloud Tjenester** (forventet leverance fra arbejdsgruppen Q3, 2022)
- **5G** (forventet leverance fra arbejdsgruppen Q3, 2022)
- **Øvrige kandidater jf. rullende arbejdsprogram**
  - IOT
  - IACS (Industrial Automation Control Systems)

Tilblivelsen af en Certificeringsordning

Tilblivelsen af en Certificeringsordning



Udbud og efterspørgsel ift. cybersikkerhedscertificering – forbundne kar



Målbillede for cybersikkerhed (og Cloud)

1. Øge cybersikkerhedsniveauet generelt
2. Let at være i for virksomheder
3. Horisontal regulering – gerne NLF
4. Referencer til fælles standarder
5. Ambition om fælles sikkerhedsniveauer
6. Efterleve GDPR men åbne for kommende løsninger

Høringssvar til Cyber resilience act

Sidste frist 25.5!!

1. A common set of minimum requirements
2. Using the New Legislative framework as basis
3. Coherence and reuse of standards
4. Covering Products, services and processes
5. Building on international standards
6. Technology neutral

Tak for ordet!

Europæiske standarder for cyber- og informationsikkerhed

Berit Aadal, Dansk Standard

Hvorfor skal I vide noget om standarder for cyber- og informationssikkerhed?

Læren fra det store Mærsk-hackerangreb: Disse 27 punkter skal du have styr på

(Illustration: Maersk)

Sidste år var Mærsk under belejring af NotPetya-ransomware-angrebet i ni dage, hvilket kostede det danske erhvervsflagskib op mod to milliarder kroner. Her er it-direktørens tjekliste for it-beredskabet, inden du selv skal afværge et ransomware-angreb.

Hackerangreb har kostet Demant over en halv milliard kroner

(Illustration: Demant)

Hackerangrebet har haft store økonomiske konsekvenser for virksomheden, der efterhånden har fået alle systemer og servere op at køre.

6 ud af 10 danske virksomheder ramt af cyberangreb

17/12/20

I det seneste år har 6 ud af 10 danske virksomheder været udsat for minimum én sikkerhedshændelse, hvilket er det højeste niveau i fire år. Virksomhederne bliver særligt ramt af de såkaldte phishing-angreb, hvor et ud af tre er relateret til COVID-19-pandemien. Det viser PwC's Cybercrime Survey 2020.

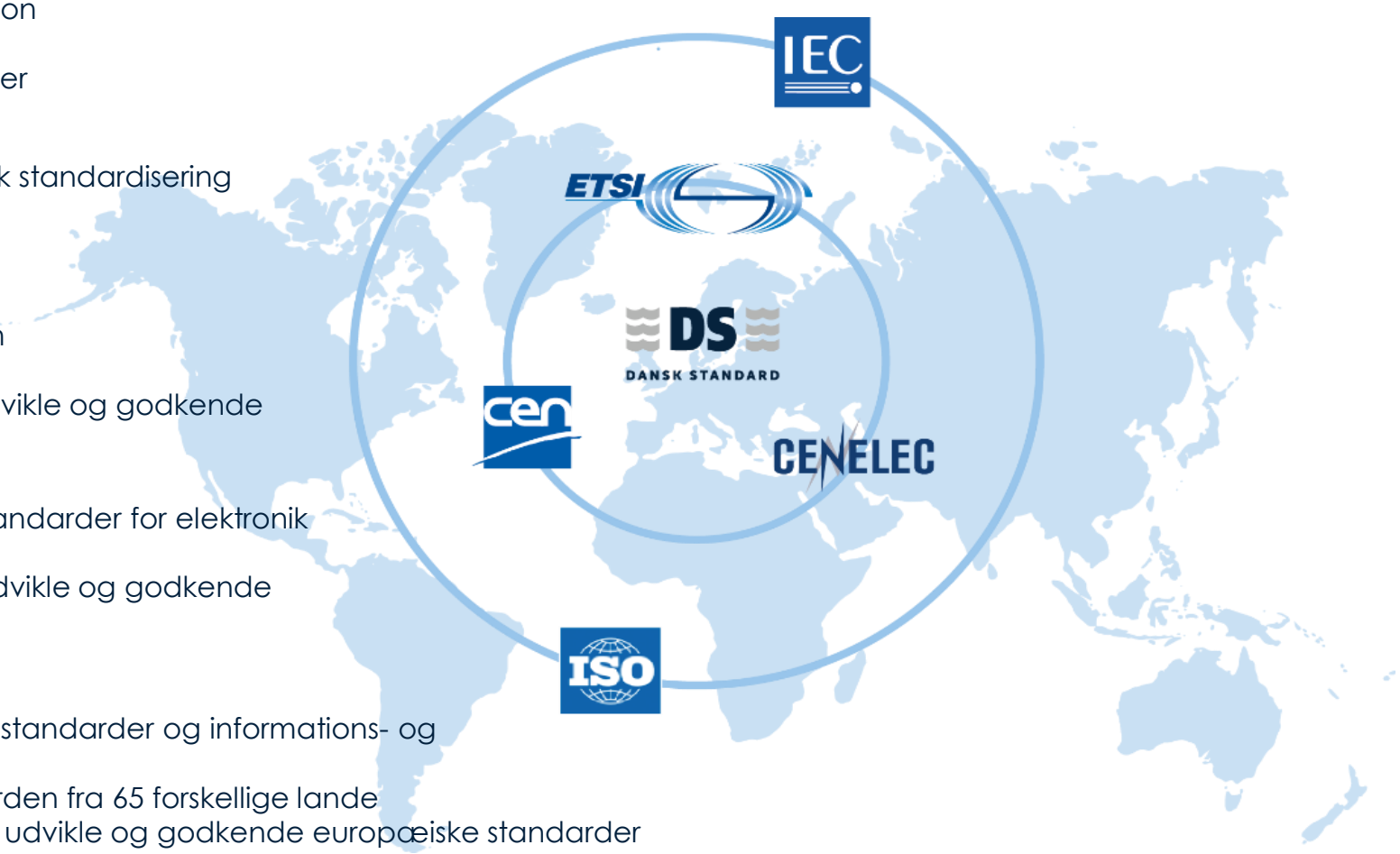
Europæisk og international standardisering

- 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

Standarder er frivillige indtil nogen sætter dem i kraft!

Standarder sættes i kraft på 3 måder

- Aftale mellem 2 parter
- Dansk Lovgivning, love, bekendtgørelser, regler
- EU-lovgivning, Direktiver, CE-mærkning

Europæisk komité: Cybersecurity and Data Protection

Formål:

- Udvikle europæiske standarder, der imødekommer de europæiske behov.
- Adoptere internationale standarder som europæiske.

Der udarbejdes 'rene' europæiske standarder på områder, hvor der mangler standarder til at understøtte europæisk regulering (Radiodirektivet, eIDAS, GDPR, NIS mm.)

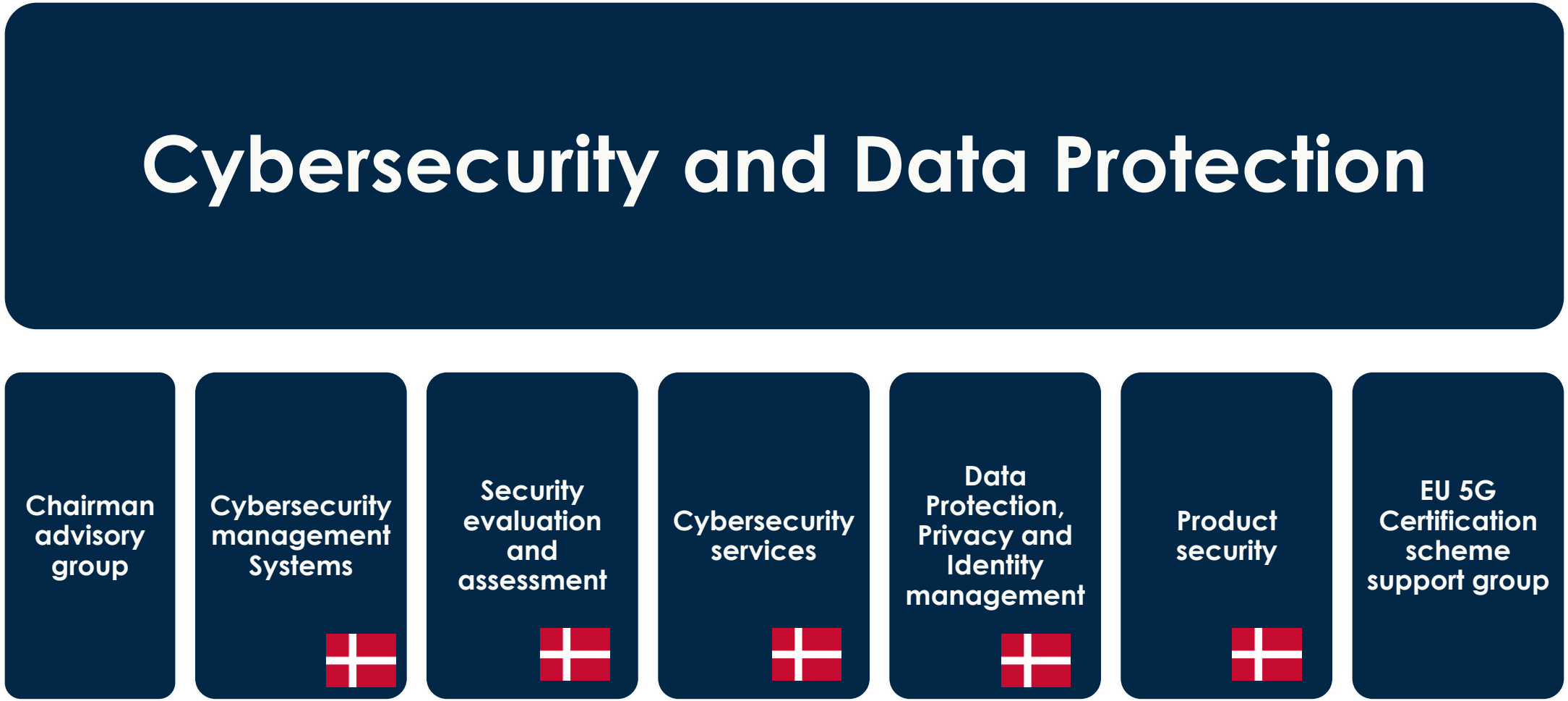
Komitéen har et tæt samarbejde med ENISA omkring de europæiske certificerings-ordninger og med Europakommissionen om de cybersikkerhedsrelaterede standardiseringsanmodninger under Radiodirektivet.

25 udgivne standarder (alle er internationale standarder, der er adopteret)

24 standarder under udvikling (heraf 11 internationale standarder, der skal adopteres)

Link til oversigt over standarder fra komiteen (CEN/CLC/JTC13)

Arbejdsgrupper under den europæisk komite



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

'Rene' europæiske standarder under udvikling (1/2)

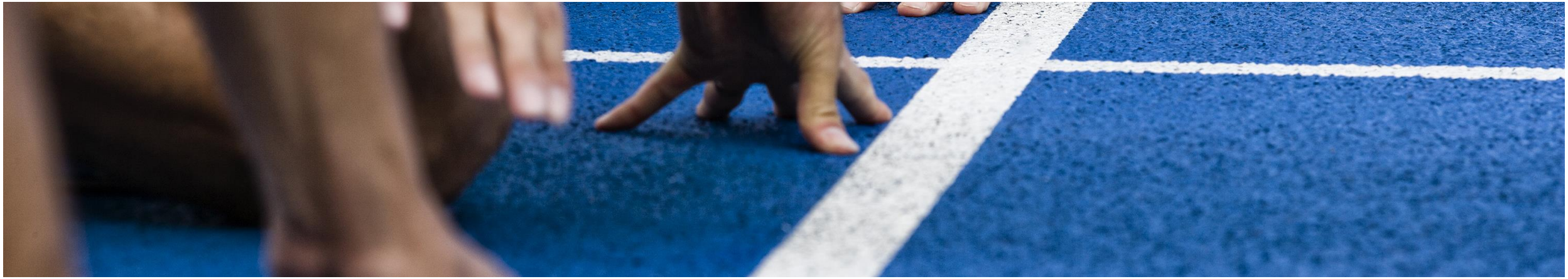
- EN XXX Managed Security Services Providers Requirements
- EN XXX Common framework for vertical information security or cybersecurity control sets
- CEN/CLC TS XXX Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services – WG2
- CEN/CLC TS XXX Requirements for Conformity Assessment Bodies certifying Cloud Services – WG3
- EN XXX Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products – WG3
- EN 17640 Fixed time for cybersecurity evaluation methodology for ICT products – WG3 og WG6 (forventes udgivet i efteråret 2022)
- EN17529 Data protection and privacy by design and by default (M/530) – WG5 (Udgives lige straks)

‘Rene’ europæiske standarder under udvikling (2/2)

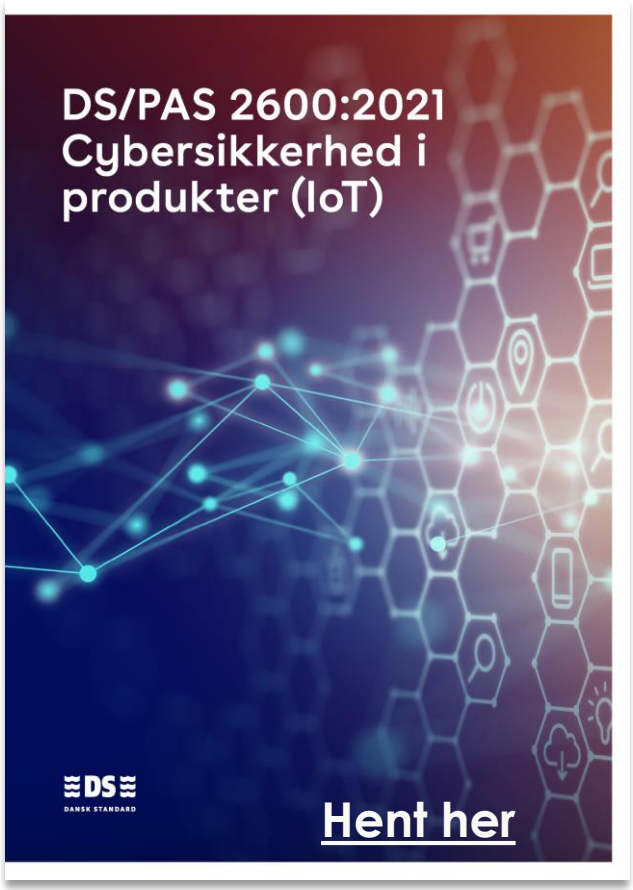
- CEN/CLC TR1 Data protection and privacy by design and by default - Technical Report on applicability to the videosurveillance industry - State of the art (M/530) – WG5
- CEN/CLC TR2 Privacy management in products and services - Biometric access control products and services (M/530) – WG5
- EN 17740 Requirements for professional profiles related to personal data processing and protection - WG5
- EN 17799 Personal data protection requirements for processing operations – WG5
- EN XXX Privacy Information Management System per ISO/IEC 27701 - Refinements in European context – WG5 (forventes udgivet i starten af 2023)
- CEN/CLC TS xxx Protection Profile for Smart Meter - Minimum Security requirements – WG6
- EN XXX Guidelines on sectoral cybersecurity assessment (har relation til ENISA/Cybersecurity Act)

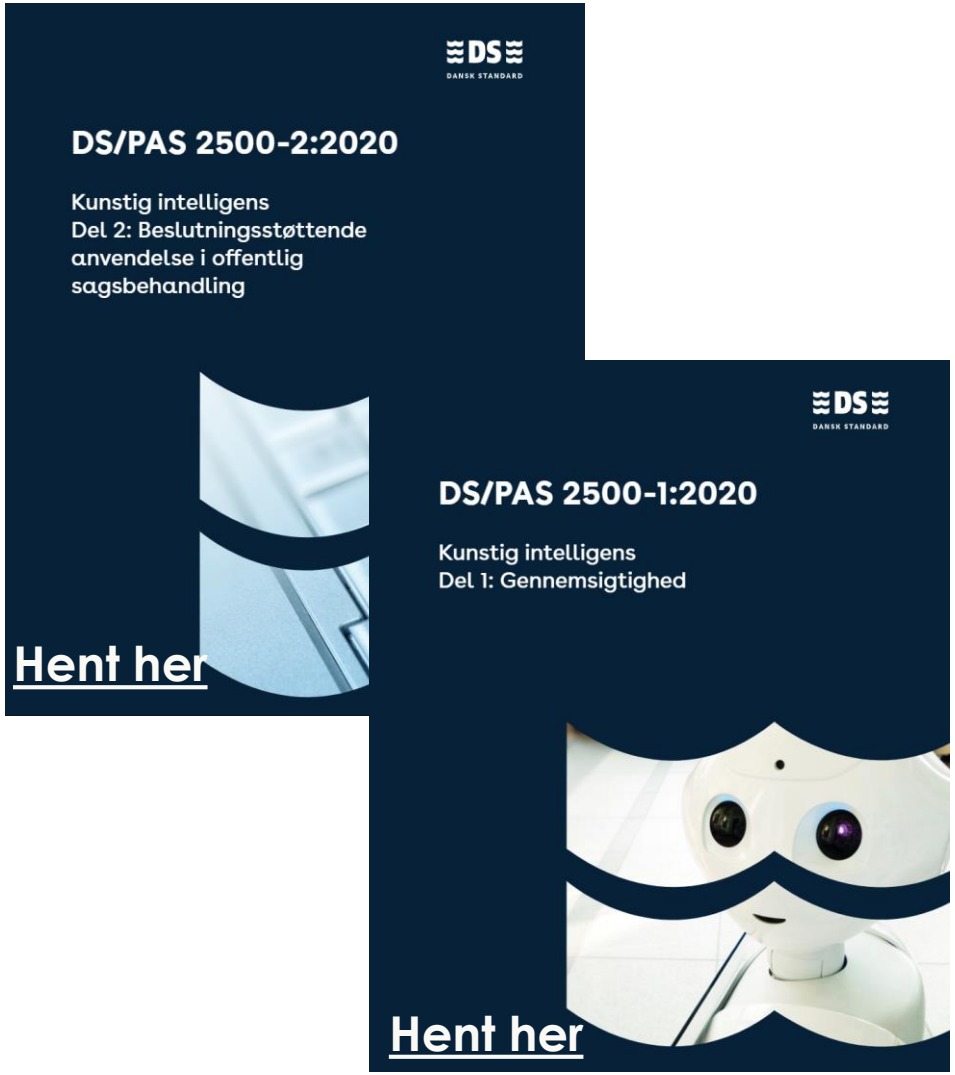
Værdien af at anvende standarder

- Klar på fremtidens markedskrav
- Konkurrencefordel
- Styr på Business Continuity
- Compliance
- Skab tillid til jeres produkt/service – og til jeres virksomhed
- Muliggør interoperabilitet
- Fælles forståelse af krav, sikkerhed og kvalitet



Gratis publikationer fra Dansk Standard





Spørgsmål

DANSK STANDARD

Kontakt

Berit Aadal
2622 4696
baa@ds.dk

Tak for i dag