DeiC

> **DeiC Updates:**
ISO 27001 Certification Project,
DeiC/DKCERT GDPR Service for Universities,
Hosting the new Decentral Cyber and Information Security Unit for the
Danish Telecom Sector

Henrik Larsen

> **DeIC - facts**

> Established 2012

> The eight Danish universities and the Danish Agency for Science, Technology and Innovation signed an agreement covering 2012-2016

> Purpose: To ensure the optimal use of national e-infrastructure resources to benefit Danish research

> A virtual organization with approximately 50 employees, most of them based at the Technical University of Denmark

> **DeIC - facts**

> Established 2012

> The eight Danish universities and the Danish Agency for Science, Technology and Innovation signed an agreement covering 2012-2016

> Since prolonged a couple of times during evaluation

> 2019 Interim board – reorganizing before end of year

> 1 January 2020: A new DeiC – cooperation or corporate?

> **ISO 27001 Certification in DeiC**

> **ISO 27001 project – a never ending story?**

> Goal: Certification of DeiC/i2's VMware cluster according to international security standard DS/ISO/IEC 27001:2013 (now DS/EN ISO/IEC 27001:2017)

> Later: certification of several services in DeiC/i2

> Documentation (soon) in place

> Prescreening by external auditor 2016

> Internal audit reports 2017 and 2018

> Preaudit March 2019

> Certification audit June 2019

> **GDPR – "DPO-as-a-Service",**
a service from DKCERT

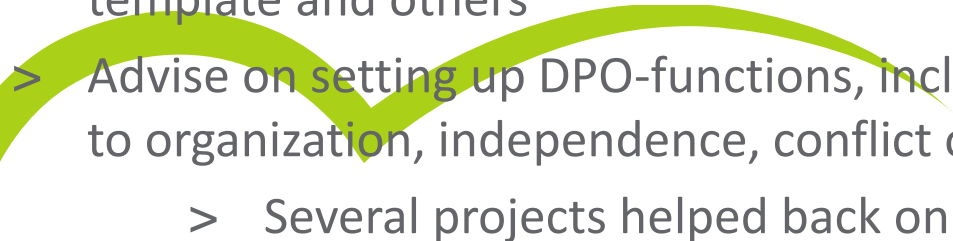Basic assumption 2017: From May 25th 2018

All educational institutions in Denmark will need a DPO!

But not all educational institutions will have to hire their own DPO

> DKCERT offers a DPO-service to institutions who do not wish to hire their own dedicated DPO. The DPO-service will:

> > Supply knowledge to support the implementation of the GDPR

> > Assume the role of independant DPO for the institution

> > Help manage ongoing challenges and dilemmas with personal data

> > Help to organize processes that comply with the regulation for processing personal data

> Before May 2018, we delivered interim DPO for two institutions
> After May 2018 we fill the DPO role for one university, one university of applied science, all three design and architectural schools plus a small research institution

> In addition the DKCERT GDPR-service does:

> Offer participation in a knowledge sharing network and development of the DPO-role at the universities

> > All Danish universities and universities of applied science participate

> Develop tools for use by DPOs, such as a data protection impact assessment template and others

> Advise on setting up DPO-functions, including handling challenges in relation to organization, independence, conflict of interest and impact

> > Several projects helped back on track

> If you wish to know more:

> www.cert.dk/en/services/DPO (in English)

> Project Manager/DPO, DKCERT:
Morten Eeg Ejrnæs Nielsen, morten.eeg@deic.dk

> Head of Security and Identity Services (DKCERT & WAYF), DeiC:
Henrik Larsen, henrik.larsen@deic.dk or henrik.Larsen@cert.dk

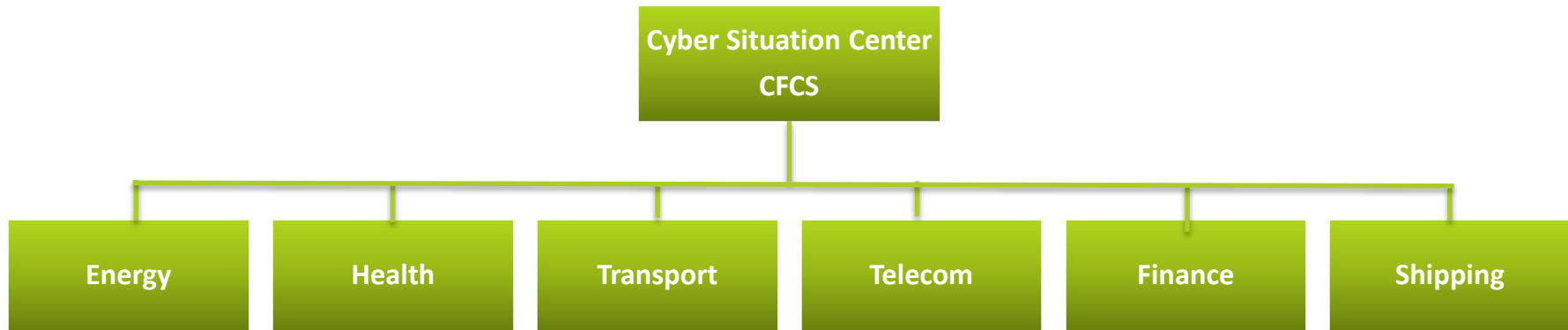> **DKCERT hosting the new Decentral Cyber and Information Security Unit for the Danish telecom sector**

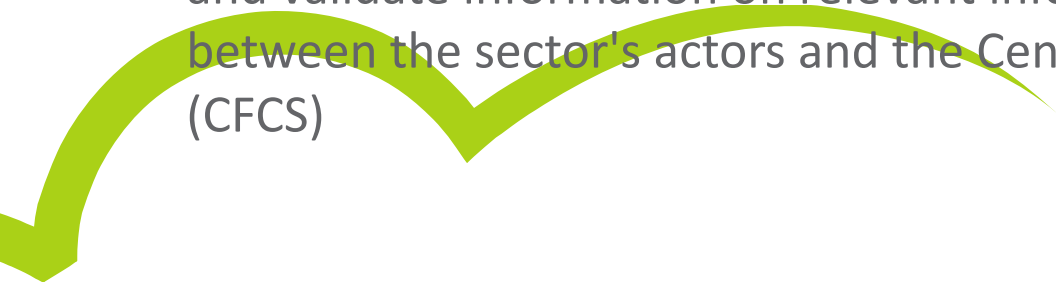National strategi for cyber- og informationssikkerhed

https://www.fm.dk/publikationer/2018/
national-strategi-for-cyber-og-
informationssikkerhed

> **Sectoral security strategies and Decentralized Cyber and Information Security entities (DCIS) in six critical infrastructure sectors (Initiative 3.1)**

```
                    ┌─────────────────────┐
                    │ Cyber Situation Center │
                    │        CFCS          │
                    └─────────────────────┘
```

| Energy | Health | Transport | Telecom | Finance | Shipping |

> **DCIS**

> A DCIS contributes to the implementation of sectoral threat assessments, monitoring, crisis exercises, security building, knowledge sharing, guidance etc.

> The primary task of the DCIS is to communicate, request, create and validate information on relevant information security issues between the sector's actors and the Center for Cyber Security (CFCS)

> **Telecom-DCIS**

> A DCIS contributes to the implementation of sectoral threat assessments, monitoring, crisis exercises, security building, knowledge sharing, guidance etc.

> The primary task of the DCIS is to communicate, request, create and validate information on relevant information security issues between the sector's actors and the Center for Cyber Security (CFCS)

> DKCERT has entered a contract with a new association of telecom operators to host the Telecom-DCIS as per 1st June

> **Settlement amending the Danish Cyber Security Center Act**

> The proposal extends the Centre's powers to prevent digital attacks on key public institutions and private companies

> Certain companies may in future be forced to join the so-called network security service

> The newly formed Advisory Board for cyber and information security will be transformed into a public-private cyber security council with shared presidency
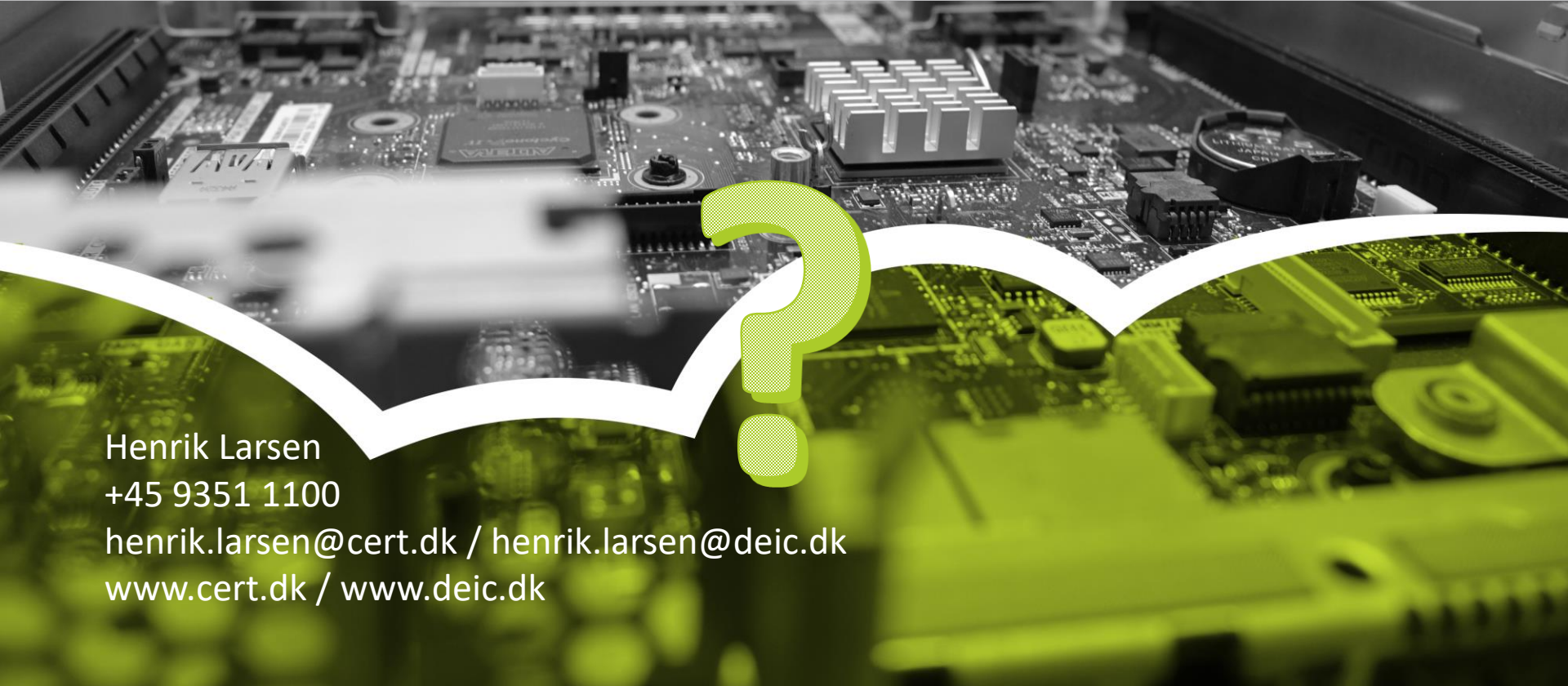
Henrik Larsen
+45 9351 1100
henrik.larsen@cert.dk / henrik.larsen@deic.dk
www.cert.dk / www.deic.dk