

# Navigating DORA & other regulatory challenges together

Mirella Daurer  
September 26, 2024



# Regulatory field - challenges



# Many regulatory challenges

For example:

- ⚡ DORA
- ⚡ NIS2
- ⚡ GDPR
- ⚡ AI Act

L 333/80 [EN] Official Journal of the European Union

**DIRECTIVES**

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT  
of 14 December 2022  
on measures for a high common level of cybersecurity across the Union  
No 910/2014 and Directive (EU) 2018/1972, and repealing 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 of the Council (4) all across the Union, mitigate threats to network and information systems security and ensure the continuity of such services when facing incidents, this 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 the implementation of the Directive, paving the way for the Directive has ensured the completion of national frameworks on the security by establishing national strategies on security of network and information systems and by implementing regulatory measures covering essential in each Member State. Directive (EU) 2016/1148 has also contributed to the establishment of the Cooperation Group and the network of national contact points. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 that present a focus addressing effectively current and emerging cybersecurity.

(3) Network and information systems have developed into a central feature of transformation and interconnectivity of society, including in cross-border or an expansion of the cyber threat landscape, bringing about new challenges, innovative responses in all Member States. The number, magnitude, and impact of incidents are increasing and present a major threat to the functioning of the result, incidents can impede the pursuit of economic activities in the area.

(4) OJ C 213, 14.6.2022, p. 22.  
(5) OJ C 26, 14.7.2021, p. 176.  
(6) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 4 July 2014 (2014/148/EU) on measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2014).

4.5.2016 [EN] Official Journal of the European Union

**REGULATIONS**

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT  
of 27 April 2016  
on the protection of natural persons with regard to the processing of  
movement of such data, and repealing Directive 95/46/EC (General  
(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 Economic and Social Committee (1),  
Having regard to the opinion of the Committee of the Regions (2),  
Acting in accordance with the ordinary legislative procedure (3),  
Whereas:

(1) The protection of natural persons in relation to the processing of personal data is one of the fundamental rights and freedoms of the Charter of Fundamental Rights of the European Union (4) and of the Treaty on the Functioning of the European Union (TFEU) (5) provide that every person has the right to the protection of his or her personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of personal data, whatever their nationality or residence, respect their fundamental right to the protection of personal data. This Regulation is intended to ensure a high level of protection of personal data and to contribute to the functioning of an area of freedom, security and justice and of an economic union, by strengthening and the convergence of the economies within the internal market.

(3) Directive 95/46/EC of the European Parliament and of the Council (6) fundamental rights and freedoms of natural persons in respect of processing of personal data between Member States.

(4) OJ C 229, 31.7.2012, p. 90.  
(5) OJ C 90, 13.12.2012, p. 127.  
(6) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and decision of the Council of 24 October 1993 (1993/54/EC) of the European Parliament and of the Council of 24 October 1993 on the protection of personal data and on the free movement of such data (OJ L 281, 23.11.1993).

27.12.2022 [EN] Official Journal of the European Union L 333/1

**REGULATIONS**

**REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 14 December 2022  
on digital operational resilience for the financial sector and amending Regulations (EC)  
No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011  
(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),  
Acting in accordance with the ordinary legislative procedure (3),  
Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectivity also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer financing, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance

(1) OJ C 143, 26.8.2021, p. 1.  
(2) OJ C 155, 30.4.2021, p. 38.  
(3) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

Very important and pre-conditions, but not the core (commercial) service!



# In practice



## What we see

- ⚡ Some exchange of information on higher level
- ⚡ Different approaches on detailed level
- ⚡ Meaning: efficiency and effectiveness potential





# Collaboration

# How could financial entities cooperate more in practice?

- ✦ Alignment on **how** and **operational**
- ✦ Think of for example:
  - Definitions
    - ‘Service which can be subcontracted’, ‘subcontractor’, ‘subprocessor’
  - Template (information) documents
    - Due diligence checks, data transfer impact analyses
  - Practical alignment
    - Pooled audits and testing, supplier asking consent

# Keylane L&P proposal

⚡ Idea is:

- User groups on compliance
- Not commercials!
- Engage non-functionals
- Alignment on compliance topics we run into in daily practice
- 2x per year

⚡ We would be happy to support and facilitate

⚡ Would this work?



**Thank you  
for listening!**

**Questions  
& Answers**



# Coffee break

