The changing face of European regulation and what it means

15 May 2025

Your speakers today

Amit Tyagi
Partner, London

T +44 20 7367 3578
E amit.tyagi@cms-cmno.com

Lars Jøstensen
Partner, Oslo

T +47 228 26 993
E lars.jostensen@cms-kluge.com

Aurélia Viémont
Partner, Luxembourg

T +352 26 27 53 54
E aurelia.viemont@cms-dblux.com

Eline Teichert
Advocaat, Amsterdam

T +31 20 301 63 68
E eline.teichert@cms-dsb.com

Today’s agenda

01
Network and Information Systems Directive 2 (“NIS 2”)

02
Digital Operational Resilience Act (“DORA”)

03
European Cyber Resilience Act (“CRA”)

04
UK Cyber Regulation

05
Class Actions

01

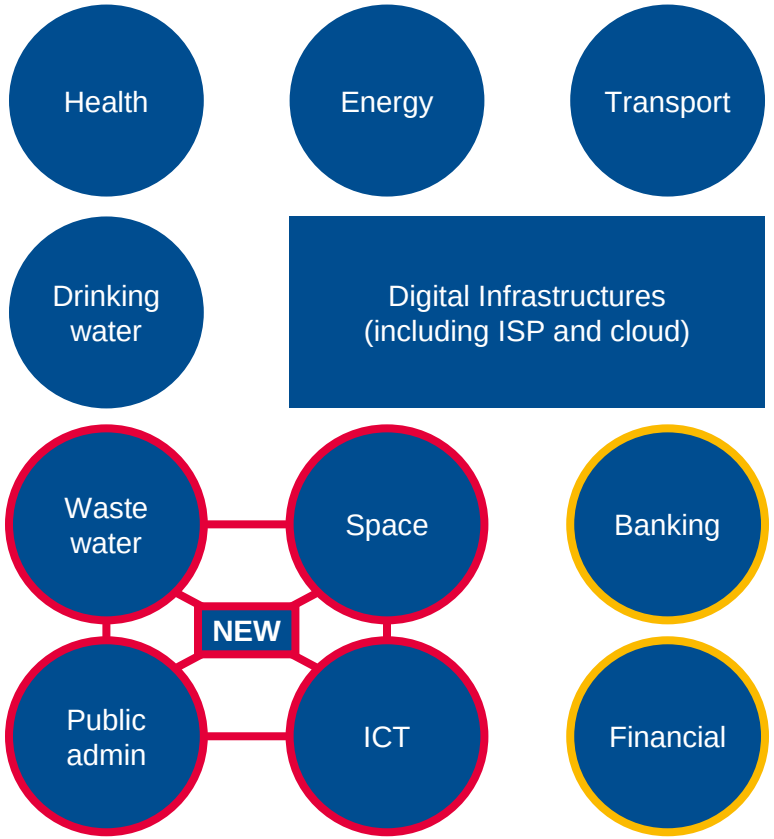
Network and Information Systems Directive 2 (“NIS 2”)

NIS2 in a nutshell

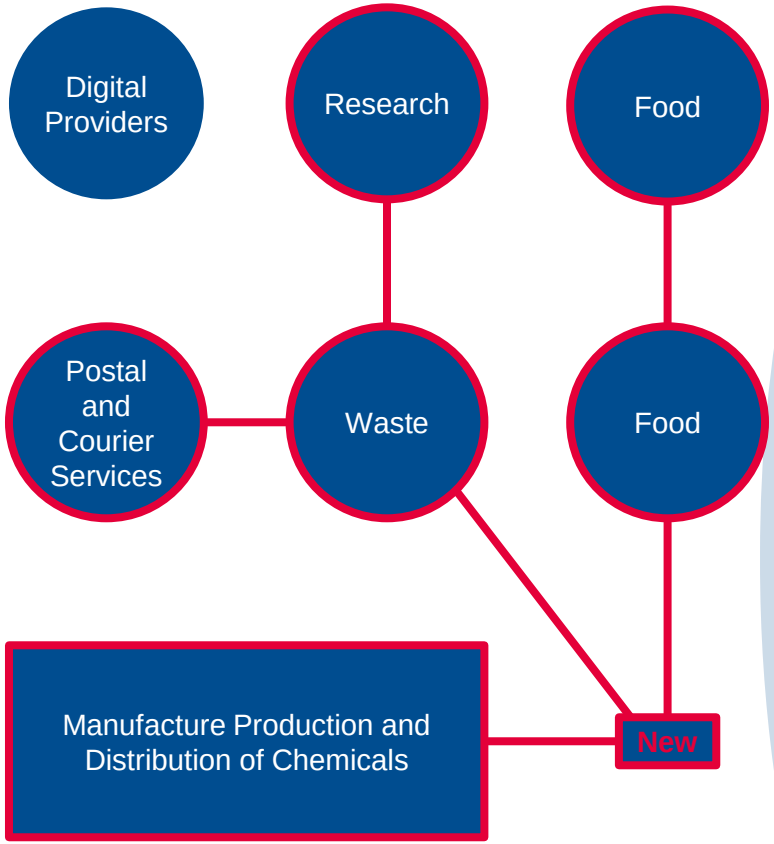
- Applicable to a wide variety of critical sectors
- Introducing strong overall IT security requirements from board to frontline, incl. supply chain
- Incident notification obligations
- Fines: EUR 7/10m or 1.4/2% annual worldwide turnover (important entities/essential entities)
- Member States to increase accountability for management bodies
- Member States to implement NIS2 by 17 October 2024 (minimum harmonisation, local differences expected)

NIS2: sectors in scope

Highly critical



Other critical



Which obligations do organisations face under NIS2?

- Registration obligation
- Duty of care to implement technical and organisational security measures and prevent/mitigate incidents
- Knowledge and training obligations for directors
- Reporting obligation (phased)
- Supervision and enforcement activities

Examples of minimum measures under NIS2

- Policies on risk analysis and IT security
- Incident handling
- Business continuity (back-up management, disaster recovery, crisis management)
- Supply chain security
- Security in acquisition, development and maintenance of IT, including vulnerability management
- MFA where appropriate
- Basic cyber hygiene and training

Considerations for insurers

Increased demand for adequate coverage to be expected

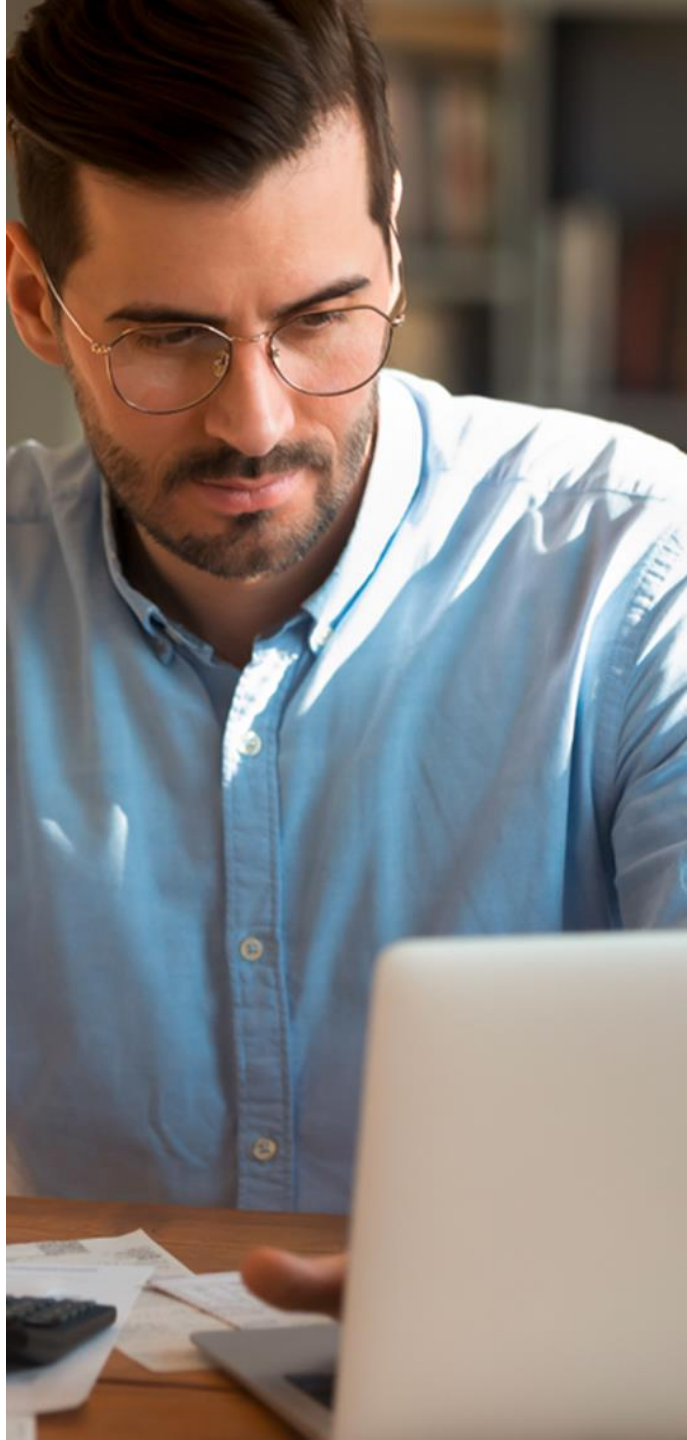
– Entities directly in scope of NIS2

– But also: entities in NIS2 supply chains

Underwriting aspects

– Current standard wording could possibly not cover key aspects of potential NIS2-related loss (e.g. definition of Privacy Regulation)

– Risk assessment to become more complex?



02

Digital Operational Resilience Act (“DORA”)

Introduction to DORA

Single European regulation on technology resilience applicable to all types of financial institutions.

Regulation arising as a consequence of:

- exposure and dependence of financial institutions on ICT service providers (including cloud services)
- the lack of a harmonised framework for ICT risk management
- the current inadequate regulatory framework for outsourcing in view of the imbalance in the relationship between service providers and financial institutions

The DORA pillars are:

- ICT risk management, ICT incident management, digital operational resilience testing, ICT third-party risk and information sharing

Scope of DORA | 1
(financial institutions)

All types of financial institutions, with due proportionality, including, among others:

- credit institutions
- payment institutions
- electronic money institutions
- investment services companies
- fund management companies
- insurance and reinsurance companies
- insurance intermediaries
- crypto-asset service providers
- credit rating agencies
- crowdfunding services providers

Scope of DORA | 2
(ICT third-party service providers)

ICT third-party service providers in-scope

– Cloud computing service providers
– Software developers
– Software support providers
– Digital service providers
– Data service providers

ICT third-party service providers out of scope

– Suppliers of hardware components
– Telecommunications service providers

Main areas regulated by DORA

- Corporate governance requirements **of financial institutions** in relation to ICT risk (management bodies, governance responsibilities, training)
- ICT risk and incident management requirements **for financial institutions**
- Digital operational resilience testing requirements **for financial institutions**
- Risk management and contractual requirements **for financial institutions**
- Information sharing **between financial institutions**
- Oversight framework for **critical ICT third-party service providers**

Considerations for insurers

Are DORA exposures covered?

- “Traditional” cyber policies are not expressly drafted to address DORA
- Are other policies relevant?

Underwriting aspects

- Alignment with DORA’s requirements?
- Third Party Risk Management

03

European Cyber Resilience Act (“CRA”)

EU Cyber Resilience Act

- Development and implementation of common cybersecurity standards for products with a “digital element” (IoT) in the EU – e.g. baby monitors, vacuum cleaners, Wi-Fi routers and alarm systems. Intended to enhance consumer trust and customer safety
- Entered into force in December 2024 and will apply in full from December 2027
- Whilst NIS 2 targets critical infrastructure and DORA focuses on the financial services sector, the CRA imposes obligations across the connected hardware and software ecosystem, implementing a range of security-related obligations on manufacturers, importers and distributors of covered products. Must be supplied for distribution or use to the EU market
- Does not include product categories with sector-specific legislation – e.g. medical devices, motor vehicles and military hardware
- Manufacturers will be required to provide an EU declaration of conformity with the product (and distributors/importers will be required to confirm this). Includes a cyber risk assessment (including due diligence on TP suppliers) and ongoing management of product vulnerabilities
- Reporting obligations (24 hours) to ENISA and CERT following an exploited vulnerability or security incident.
- Sanctions regime – fines of EUR5 – EUR15m or 1-2.5% of global turnover for non-compliance. Potential for GDPR/DPO fines in addition

04

UK Cyber Regulation

Cyber Security and Resilience Bill | 1

- Introduced to Parliament in 2025, could be law by 2026. Update to UK NIS Regulations
- Part of the UK government's pledge to enhance and strengthen the UK's cybersecurity measures and protect the digital economy in response to recent cyber incidents impacting hospitals, universities, democratic institutions and government departments and State Actors
- Will likely follow a similar approach to EU in NIS2 and Cyber Resilience Act – i.e. to ensure critical infrastructure and digital services are secure
- Stricter security requirements, mandating regular vulnerability assessments, and ensuring robust incident response plans in place
- Greater powers to Regulators alongside enhanced reporting and compliance requirements – focus on intelligence gathering
- Government Consultation on Ransomware – Targeted ban (public sector bodies, local government and operators of CNI); payment prevention; reporting regime

Cyber Security and Resilience Bill | 2

- No mention of AI in Bill BUT: AI Opportunities Action Plan – Intended to establish UK at forefront of AI development and adoption. Diverge from EU regulation (harmonised risk-based) with a “pro-innovation” approach which allows regulators to “promote AI” with a “higher risk tolerance”
- If follows EU legislation, may also impose obligations for the implementation of cyber security measures, and liability for any failings, on senior management
- Subject to the specific contents of the Bill, there will likely be a need for businesses, certainly tech companies and those operating in critical services, to adhere to, and likely invest in, stricter cybersecurity standards
- Requirement for all businesses to consider who they may interact with in their supply chains to determine whether they fall within the scope, even indirectly, of the new stricter cyber security requirements
- Anticipated information sharing will likely increase collective resilience to cyber-attacks, enhanced reporting obligations may well increase the administrative burden on businesses and bring with it additional costs arising from cyber incidents

Considerations for insurers

Increased demand for adequate coverage to be expected

- As with NIS 2 and DORA, will likely result in further uptake in Cyber insurance
- Increased use of risk management services (where offered)

Underwriting aspects

- Need to account for greater level of regulatory scrutiny
- Higher fines and penalties for failure to comply with mandated cybersecurity standards. But, not a Privacy Regulation?
- Potential risk of increased civil litigation
- Improvement in cyber security posture
- Other Insurances (D&O, FI) may also be in scope

05

Class Actions

Class action risk – why is this important?

- Cyber attacks and data breaches on the rise
- Cyber coverage is broad and responds to a variety of civil data litigation claims
- Changes in the law make bringing claims easier and enabling forum shopping
- Claimant law firms and funders are investing
- Strategies for resolution differ depending on jurisdiction, costs recovery rules and claimants' objectives

Globally, 30,000 websites are hacked daily

There are 2,200 data breaches every day

Morrisons
British Airways,
Google …

Litigation in the UK

‘Opt-in’ routes

– Group litigation orders under Section III, Part 19 CPR (common or related issues of fact or law) – *Morrisons Supermarkets/Sharp v Blank/ RBS Rights Issue*

A key rationale for group litigation is to facilitate claims that would otherwise be uneconomic/ impractical to pursue

‘Opt-out claims

– Representative claims under CPR 19.6 (same interest) – *Lloyd v Google*

– Claims for breach of competition law under CRA 2015 – *Merricks v Mastercard*

Recent case law suggests group litigation for cyber data breach claims in the UK will be difficult and uneconomically viable

Mass actions in the EU after Brexit | 1

- Professional claim industry (experienced lawyers, experienced and sophisticated funders)
- The NL is a hub for claimants (European foundation of claim funders, branch offices of US plaintiff firms, etc.)
- Mass actions increase across Europe (see our European Class Action Report)
- GDPR must be in scope of the mass actions according to the Rep Actions Directive
- In international incident multiple class or group actions simultaneously in various jurisdictions
- A number of mass actions are pending in the NL

Europe

Mass actions in the EU after Brexit | 2

Trending issues

- Each jurisdiction has its own issues (experienced courts, resources, language).
- Corporate governance of the claim vehicle
- Conflict of interest between funders and claimants
- Disclosure of funding mechanism/review by the court?
- Cross border approach by claimants (combination of UK/Germany/NL/Ireland claims)
- Combination of claims against Company, D&O, Accountants, Regulator (even POSI) to create a large potential pot of money)
- Specific GDPR issues:
  - can individual claims for compensation of immaterial damage be aggregated?
  - jurisdiction of the national court with a mixture of claimants and foreign defendants?

Europe

Mass actions in the EU after Brexit | 3

Litigation funding

- Each jurisdiction has its own rules (No cure no pay, *pars quota litis*, anything goes)
- Sophisticated funders with expert counsel (both legal and financial)
- Conflict of interest between funders and claimants:
  - who is in charge of the litigation strategy, funders or claimants?
  - likewise, with settlement discussions
- Disclosure of funding mechanism/review by the court?

Europe

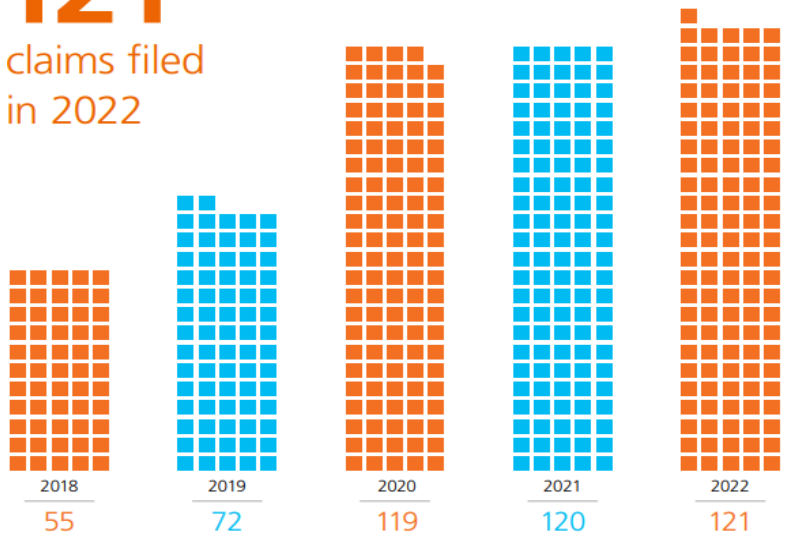
Post-incident

Mass actions on the rise

Overall number of class actions

Europe and the UK continue to see record numbers of class actions being filed. Every year we have analysed has shown a consecutive increase.

121
claims filed
in 2022



With the Representative Actions Directive now being implemented across the EU, we anticipate yet further increases in the years to come.

Europe

Countries with op-out claims

Data breach group actions in Europe

Elements that effect underwriting/claims management

- Forum shopping
- Either one targeted defendant or as many defendants as possible
- Simultaneous mass actions in multiple jurisdictions; differences in approaches and experience by the courts
- Collection of relevant data
- Language and cultural issues
- Variety of rep agents: extremely aggressive vs reasonable/idealistic
- Wide variety of conduct by the Insureds (pro-active vs very defensive)
- New European concepts of liabilities in directives and regulations

Considerations for insurers

Greater reliance on Insurance cover

- Potential for data breach claims to be significant and well funded
- Substantial defence costs and liability exposure
- Longer “tail” to incidents and issues with finality for opt-in litigation

Underwriting aspects

- Understanding exposure to specific jurisdictions and rules of engagement/funding/costs recovery will be key
- Control over conduct of claims may be essential to limit exposure

Final conclusions

The new regulations will likely result in an increased appetite for Cyber insurance

The new regulations focus on operational resilience rather than privacy. Is there a gap in cover?

Consider differences in regulation between EU Member States. Where does the policy holder operate? Will they be subject to different approaches?

Increased focus on supply chain risk part of wider trend and should filter through to underwriting assessments

Does the policy holder know whether they will be in scope? Can they afford to pay for changes required/increased scrutiny?

Watch this space as no one really knows how the implementation will play out!

Questions?

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

Further information can be found at **cms.law**

UK - 708674251.2