Law and Technology

David Cowan

Bloomsbury

Contents

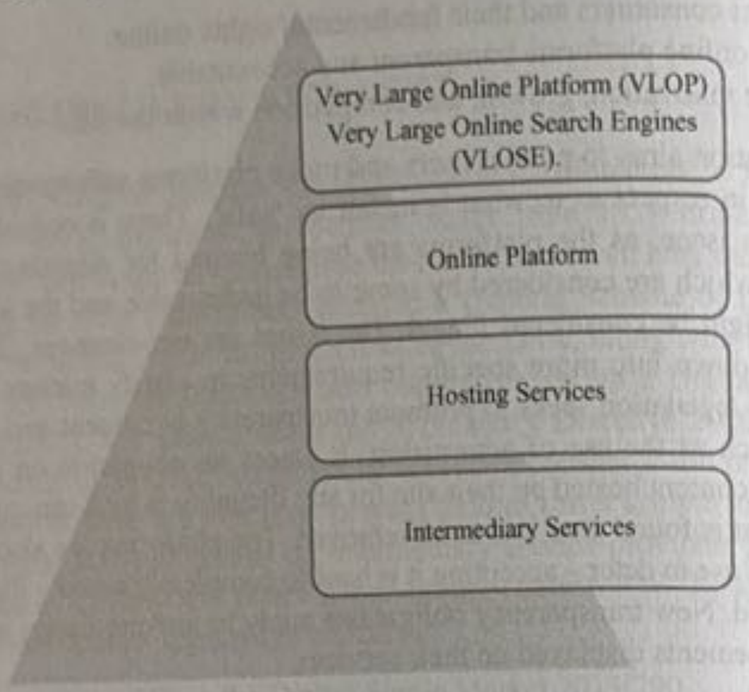
PART II
THE LAW OF TECHNOLOGY

PART III
TECHNOLOGY OF LAW

Table of Cases

The DSA predominantly follows a tiered regulatory system, as illustrated in Fig. 3.4.

Fig. 3.4 DSA regulatory tiers



(a) **Very large online platform:** Very large online platforms (VLOPs) and very large online search engines (VLOSEs) that have at least 45 million average monthly recipients located in the EU. The EU views these platforms as posing 'particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10% of 450 million consumers in Europe'.[35]
(b) **Online platform:** sellers and consumers on social networks, online marketplaces, platforms storing and disseminating information to the public, at the request of service users, as their primary activity (including marketplaces, app stores, collaborative economy platforms and social media platforms).
(c) **Hosting services:** cloud computing and web hosting, which also includes online platforms.
(d) **Intermediary Service Providers:** offering network infrastructure such as internet access providers and domain name registrars, including hosting services. These are the most affected as the bulk of DSA obligations apply to online platforms. There is a need to implement policies, internal processes, and new functionalities.

[35] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

DSA OBLIGATIONS

[3.14] It is fair to say the main targets here are the VLOPs, given their role as powerful channels and distributors of content. They are also scrutinised in terms of competition laws and unfair practices. Unsurprisingly this has met with legal challenge from the VLOPs. The EU set a deadline of 17 February 2023 for all platforms and search engines, irrespective of size, to publish their user numbers, open up their algorithms to the commission and offer approved researchers access to their data. In April the EC presented a list of 19 online companies said to meet the VLOP criteria, 17 of which were designated VLOPs, and the other two very large online search engines (VLOSE). The 19 satisfied the criteria of having 45 million or more average monthly active users in the EU. Of the 19 VLOPs, 16 are US-based, two are Chinese, and only one is based in the European Union. A Center for Strategic and International Studies paper accuses the EU of putting in place 'discriminatory provisions aimed directly at large US platforms'.[36] The DSA specifies four different levels of obligations depending on the type of provider, though it should be noted that this does not apply to small companies and micro-enterprises having less than 50 employees and under €10 million in annual sales. The key requirements for all DSA designated providers are set out in Fig. 3.5. and the EC statement on obligations for VLOPs and VLOSEs is presented in Fig. 3.6.

Fig. 3.5 Key obligations

Requirement	Actions
The illegal content must be managed and taken down as appropriate.	Implement measures to prevent the spread of illegal content.
	Act quickly and efficiently in dealing with such content cooperation, and deploy tools.
	Illegality defined based on the affected EU Member State law.
The DSA sets out transparency requirements for all DSA designated providers.	Reporting on content moderation and compliance.
	Transparent in reporting volume of complaints.
	Performance metrics and targeting criteria employed.
Additional VLOPs and VLOSEs requirements.	Establish independent compliance function.
	Regular compliance audits.
	Mandatory risk assessment of new features.
	Crisis response mechanism.
	Repository of information of online advertising displayed on their platform.

(continued)

[36] Broadbent, 'The EU Data Act: The Long Arm of European Tech Regulation Continues', Center for Strategic and International Studies in Washington, D.C., June 2023, https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues.

Fig. 3.5 *(Continued)*

Requirement	Actions
EU stipulation of the penalties for non-compliance	EU Member States empowered to appoint a Digital Services Coordinator (DSC) to monitor and enforce compliance within that Member State.
	May impose fines of up to 6% of a provider's global annual turnover or 1% for violating an information obligation.
	Temporary suspension of the provider's services in more severe cases.

Source: European Commission.

Fig. 3.6 Obligations for VLOPs and VLOSEs[37]

EC Statement on obligations for VLOPs and VLOSEs

A platform or a search engine designated as such under DSA needs to:

- establish a point of contact for authorities and users
- report criminal offences
- have user-friendly terms and conditions
- be transparent as regards advertising, recommender systems or content moderation decisions

They also must follow the rules that focus only on VLOPs and VLOSEs due to their size and the potential impact they can have on society. This means that they must identify, analyse and assess systemic risks that are linked to their services. They should look, in particular, to risks related to:

Illegal content

- fundamental rights, such as freedom of expression, media freedom and pluralism, discrimination, consumer protection and children's rights
- public security and electoral processes
- gender-based violence, public health, protection of minors, and mental and physical well-being
- once the risks are identified and reported to the Commission for oversight, VLOPs and VLOSEs are obliged to put measures in place that mitigate these risks. This could mean adapting the design or functioning of their services or changing their recommender systems. They could also consist of reinforcing the platform internally with more resources to better identify systemic risks.

Those designated as VLOPs or VLOSEs will also have to:

- establish an internal compliance function that ensures that the risks identified are mitigated
- be audited by an independent auditor at least once a year and adopt measures that respond to the auditor's recommendations

(continued)

37 https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

Fig. 3.6 *(Continued)*

- share their data with the Commission and national authorities so that they can monitor and assess compliance with the DSA
- allow vetted researchers to access platform data when the research contributes to the detection, identification and understanding of systemic risks in the EU
- provide an option in their recommender systems that is not based on user profiling
- have a publicly available repository of advertisements

Source: European Commission.

DSA ACTIONS BY THE EC

[3.15] The EC was quick to demonstrate its enforcement approach, which led to some pushback from the major platforms. Meta was investigated for various potential violations under the DSA regime.[38] In December 2024, the EC launched a third formal processing against TikTok, following an ongoing investigation in relation to its verification mechanisms and secondly an alleged addictive design, which opened on 19 February 2024 and closed with commitments in August 2024. The EC issued a retention order to TikTok, ordering the platform to freeze and preserve data related to actual or foreseeable systemic risks its service could pose on electoral processes and civic discourse in the EU. This retention order concerns national elections in the European Union between 24 November 2024 and 31 March 2025.[39] In July 2023, internet retailer Amazon launched a legal challenge in an EU court against Brussels designating it as a VLOP. Amazon stated that 'the DSA was designed to address systemic risks posed by very large companies with advertising as their primary revenue and that distribute speech and information'.[40] Amazon also noted that it had already implemented measures to protect customers from illegal products in 2022, independently of EU obligations, at the cost of $1.2 billion. German online fashion retailer Zalando had challenged the designation prior to Amazon. Zalando subsequently challenged a supervisory fee that covers EU regulatory costs of monitoring compliance with DSA rules, one of three entities to do so.[41] VLOPs are obliged to pay the annual charge capped at 0.05 per cent of their annual worldwide net income. There has been much criticism of the DSA, as well as concerns about scoping issues. In respect to content moderation, in November 2023 the platforms disclosed for the first time how

38 European Commission, 'Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act', press release, 30 April 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373.

39 European Commission, 'Commission opens formal proceedings against TikTok on election risks under the Digital Services Act', press release, 17 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487.

40 Le Monde, 'Amazon lodges legal challenge to new EU rules on platforms', 13 July 2023, https://www.lemonde.fr/en/economy/article/2023/07/13/amazon-lodges-legal-challenge-to-new-eu-rules-on-platforms_6051118_19.html.

41 Chee, 'Zalando challenges supervisory fee for EU online content rules, third such lawsuit', Reuters, 17 April 2024, https://www.reuters.com/business/retail-consumer/zalando-challenges-supervisory-fee-eu-online-content-rules-2024-04-17/.

many content moderators they have for each official language of the EU. French president Emmanual Macron complained at the 2023 Christchurch Call Summit, aimed at stopping the spread of violent content online (which Meta and Google declined to attend), that the platforms 'simply don't deliver' on handling of hate speech.[42] Content moderation is an issue that erupted again in 2024 following the US presidential election victory of Donald Trump, which is discussed further in Chapter 33.

DIGITAL MARKETS ACT[43]

[3.16] The Digital Markets Act (DMA) regulates online intermediaries, including online app stores, search engines, social media networks. Intermediaries are designated as 'gatekeepers' by introducing specific obligations and prohibitions in relation to business practices. The goal is to ensure a fair digital economy. In force since 1 November 2022, the DMA established new rules to create:

(a) a fair business environment for business users dealing with gatekeepers;
(b) competition in the online platform environment eschewing unfair terms and conditions; and
(c) greater choice and fairer pricing.

The EC has designated the major players as gatekeepers/services; though this has not met with universal acceptance and platforms have appealed[44] (see Fig. 3.7).

Fig. 3.7 Big Tech intermediaries

Online Intermediaries	
Alphabet	Google Play, Google Maps, Google Shopping, Google Search, YouTube, Android, Chrome and Alphabet's online advertising service.
Amazon	(Appealed certain services) Amazon Marketplace and Amazon Advertising.
Apple	AppStore, iOS and Safari.
ByteDance	(Appealed) TikTok.
Meta	(Appealed certain services) Facebook Marketplace, Facebook, Instagram, WhatsApp, Facebook Messenger and Meta Ads.
Microsoft	LinkedIn and Windows PC OS.

42 Politico, 'Macron: Meta, Google 'simply don't deliver' on handling of hate speech', 11November2023,https://www.politico.eu/article/france-macron-meta-google-dont-deliver-hate-speech/.
43 EU Regulation 2022/1925 ([2022] OJ L265/1) of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
44 As of March 2024. The data here is based on a useful breakdown: Herbert Smith Freehills, 'Digital Markets Act – Overview', 13 March 2024, https://www.herbertsmithfreehills.com/notes/crt/2024-03/digital-markets-act-overview.

[3.17] The EC did not designate several core platform services (Gmail, Outlook.com, Samsung Internet Browser, iMessage, Bing, Edge and Microsoft Advertising) since, while they met the thresholds, they were not deemed 'important gateways'. The EC considered notifications from Booking, ByteDance (advertising service) and X and investigated Apple's iPadOS. The EC first flexed their new DMA muscles by taking Apple to task for what they saw as a breach of the Act and competition laws with its App Store marketplace, which sets rules to prevent app makers from alerting users to alternative and cheaper options. The DMA proscribes technology companies blocking app developers from telling users about other options or from directing users to other platforms and promotions outside of an app store. Regulators accepted Apple's pledge to open its 'tap to pay' iPhone payment system to rivals as a way to resolve an antitrust case and head off a fine of up to 10 per cent of its global annual revenue of $383.3 billion.[45] At the outset of the matter, Vestager, as executive vice president in charge of competition policy at the commission, said Apple should have a new slogan: 'act different'.[46]

[3.18] One line of criticism was the concern over the per se rules in arts 5, 6 and 7 forbidding types of conduct without proving harm, which can give rise to false positives or misconduct due to false negatives. This may in turn, as analysis provided to the CMA argues, lead to increased legal risks and spillover for non-gatekeeper platforms.[47] A study from Catalyst Research[48] also raised early concerns that European Small and Medium Enterprises (SMEs) might unwittingly suffer as a consequence of the application of the DMA. Small and medium-sized enterprises represent approximately 90 per cent of all European enterprises and more than half of economic activity in Europe. These enterprises are global users of big tech products and services for simple and practical reasons, the report noted, and these are the connection services that:

> 'DMA could disrupt through forcing the disaggregation of a critically important stack of services offered by large tech companies – e-commerce, digital marketplaces, social media, digital advertising, and business analytics – but they are precisely the affordable yet powerful tools that deliver extraordinary results to small businesses and so their regulation is potentially very harmful.'[49]

The report calls for a different approach to pre-defining and restraining potential troublemakers:

> 'An alternative approach would be to identify "gatekeeper" companies and develop an oversight regime, but impose regulatory prohibitions and obligations on each gatekeeper independently and only after measuring the economic benefits that may be lost as a result. Regulating based on performance instead of arbitrary metrics would create

45 Chan, 'EU accepts Apple pledge to let rivals access "tap to pay" iPhone tech to resolve antitrust case', AP News, 11 July 2024.
46 Taggart, 'Apple "broke EU competition rules"', The Times, Business, 25 June 2024, 34.
47 Paper prepared by King & Spalding LLP for the Computer & Communications Industry Association (CCIA), 'The Digital Markets Act's Per Se Prohibitions Increase Legal Risks for Non-Gatekeeper Platforms', 9 February 2022.
48 Catalysts Research, DCI Digital Markets Act Working Group, 'Misfire: How the Digital Markets Act Will Unwittingly Hurt European Small Businesses', June 2021, https://datacatalyst.org/reports/misfire-how-the-digital-markets-act-will-unwittingly-hurt-european-small-businesses/.
49 Catalysts Research, 'Misfire', 5.

a pathway to success for large and growing companies, while also looking out for Europe's competition and broader economic interests.'

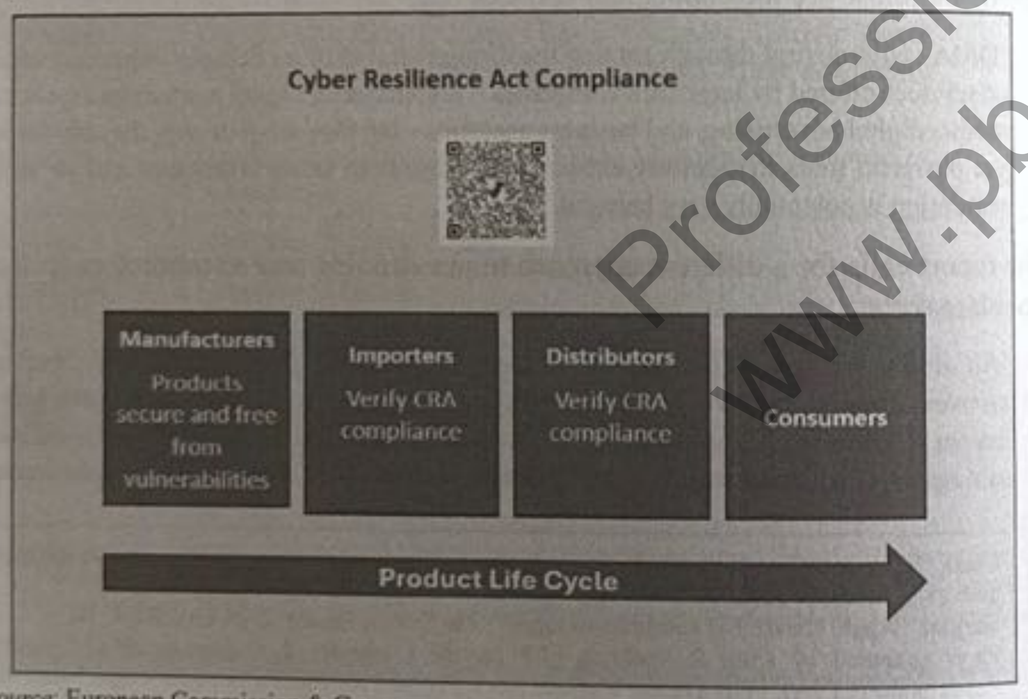
This approach, as the report acknowledges, would be slower, but offering such alternatives may provide for greater regulatory dialogue and more sustainable solutions than the constant hammering out of regulations.

CYBER RESILIENCE ACT[50]

[3.19] Published on 15 September 2022, the Cyber Resilience Act (CRA) entered into force on 10 December 2024. The main obligations introduced by the CRA will apply from 11 December 2027. The CRA establishes cybersecurity requirements for products with digital elements. Its focus is on countering cyberthreats, and it has two main objectives: to create conditions for the development of secure digital products, and to create conditions allowing users to take cybersecurity into account when selecting or using products with digital elements. The CRA will guarantee:

- harmonised rules when bringing to market products or software with a digital component;
- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain; and
- an obligation to provide duty of care for the entire lifecycle of such products.

Fig. 3.8 CRA Compliance



Source: European Commission & Cowan.

50 European Commission, 'Cyber Resilience Act', 10 December 2024, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[3.20] The regulation applies to all products connected directly or indirectly to another device or network. However, there are specified exclusions such as open-source software or services already covered by existing rules, such as medical devices, aviation and cars. Manufacturers of digital devices will have to place compliant products on the EU market by 2027, and must meet several obligations, including:

- Essential cybersecurity requirements, applicable to all products with digital elements.
- Vulnerability handling requirements.
- Extra requirements for 'critical' products.
- Conformity requirements for manufacturers of products in scope.
- Reporting obligations.

The Regulation was announced in the 2020 EU Cybersecurity Strategy, and complements other legislation in this area, specifically the NIS2 Framework. Criticism has come from the open-source community,[51] since it may place greater responsibility for compliance on open-source developers, and as a result commercial software sold in the EU market using open-source component may require the developers to be accountable for its security. Providers and publishers of software are also concerned that the 24-hour window to disclose vulnerabilities to regulators does not provide enough leeway to deal with security vulnerabilities in secrecy until a proper fix can be applied and deployed.

THE DATA ACT[52]

[3.21] The Regulation on harmonised rules on fair access to and use of data is generally called the Data Act. Adopted by the European Commission on 23 February 2022, the Data Act entered into force on 11 January 2024, applicable in September 2025. The Data Act focuses on data generated by Internet of Things (IoT) devices. It aims to create a single data market in which data is more accessible and can be shared without legal obstacles among European businesses and the public sector. In particular, it aims to enable consumers and businesses to take full advantage of the digital data they create when using IoT devices. The EU states the benefits of the Act as:

(a) *Accessibility and transparency*: Products and services must be designed in a way that makes data accessible to users by default. Users also need to be provided with certain transparency information around data before purchase.
(b) *Data portability*: Users of products are granted a right to request that data holders make all data generated by products available to third parties of their choice.

51 Domas, 'The Cyber Resilience Act: What It Means For Open Source', Forbes Technology Council, 10 September 2024, https://www.forbes.com/councils/forbestechcouncil/2024/09/10/the-cyber-resilience-act-what-it-means-for-open-source/.

52 European Commission, 'Data Act', 10 October 2024 https://digital-strategy.ec.europa.eu/en/policies/data-act. For an EC explainer, see https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained.

(c) *Data-sharing agreements with small and medium-size enterprises (SMEs)*: The Data Act includes protections for SMEs against unfair contract clauses included in data-sharing agreements with more powerful market players.
(d) *Switching cloud services*: Cloud services providers must remove obstacles that restrict customers from entering into contracts with new providers and porting over data, applications, and other digital assets to the new provider.
(e) *Rules for international transfer of non-personal data*: The Data Act proposes new restrictions, similar to those found in the General Data Protection Regulation and Schrems, applicable to international transfers of non-personal data held in the EU.
(f) *Exclusion for database rights*: The Data Act specifies that the database right created by the EU Database Directive does not apply to databases containing data from, or generated by, the use of a connected device.

Fig. 3.9 The Data Act

The Data Act: Today and Tomorrow

Cheaper prices for aftermarket services and reparation of their connected objects – Three EC example scenarios.

Problem: A factory robot breaks down.

Today: Only the manufacturer can access the data, leaving no alternative for the company but to call them for repairing.

Tomorrow: The user could request that a repair service that may be cheaper also gets access to the data.

New opportunities to use services relying on access to this data

Problem: A farmer has equipment from different manufacturers (tractor, automatic irrigation system).

Today: Farmer cannot outsource the data analytics of its different equipment: the data is locked with each manufacturer.

Tomorrow: Farmer could receive customised advice from a company gathering data from the different equipment.

Better access to data collected or produced by a device.

Problem: A bar owner wants to serve better coffee, and the coffeemaker company wants to improve its product.

(continued)

Fig. 3.9 *(Continued)*

Today: Only the company can access the data produced by the machine to design the next generation of coffeemakers, but the bar owner cannot access information such as the quantity and temperature of water or coffee strength.

Tomorrow: Both parties can access all data collected by the machine.

Source: European Commission & Cowan.

DATA GOVERNANCE ACT – REGULATION ((EU) REGULATION 2022/865)

[3.22] In force since 23 June 2022, the DGA created a framework for making available public-sector data, setting out the role of data intermediaries, facilitates data-sharing and encouraging 'data altruism' on the part of individuals and private sector entities. The DGA aims to improve data-sharing across sectors and EU countries, particularly by facilitating wider reuse of data held by public sector bodies. For example, it contemplates supporting data-driven innovation using health data, mobility data, environmental data, agricultural data, and public administration data. To achieve this aim, it introduces four types of measures:

(a) Facilitating the reuse of public sector data that is not currently accessible to third parties.
(b) Ensuring trust in data intermediaries.
(c) Supporting individuals and businesses in making their data available for the benefit of society.
(d) Facilitating data-sharing across sectors and borders, and ensuring the right data is found for the right purpose.

NIS2 FRAMEWORK[53]

[3.23] The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU.[54] The stated aims of NIS2 are to ensure:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority;
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States; and

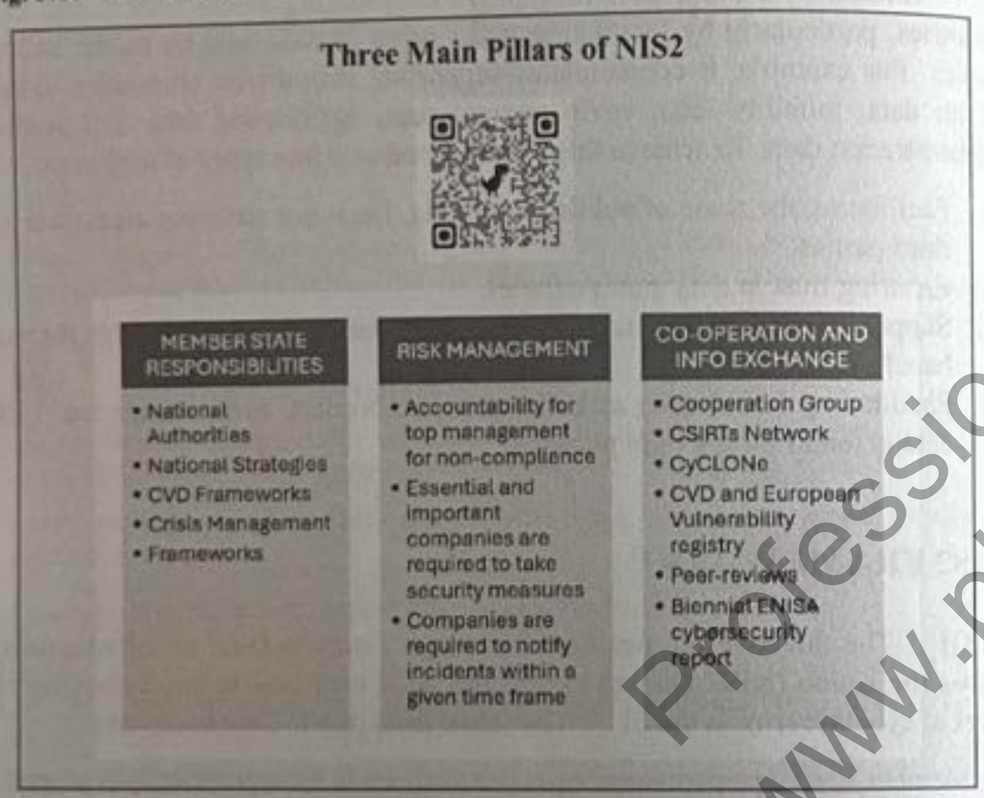
53 European Commission, 'Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)', 21 November 2024, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
54 The National Security Centre for Ireland offers a comprehensive guide: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf.

- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

NIS2 was developed to deal with differences in the application of NIS1 across Member States. Vandezande provides a useful scorecard on NIS2:

> 'Overall, the NIS2 framework can be hailed as a welcome update to the existing framework. It maintains the general approach of the NIS Directive and specifically focuses on tightening the points where its predecessor was underperforming. In removing the substantial discretion left to the Member States under the NIS Directive, NIS2 should succeed in providing a more level playing field across the EU in this matter. At the same time, NIS2 continues the approach of not being too forceful in some matters, and it will need to be seen whether its renewed approach leads to better results than its predecessor.'[55]

Fig. 3.10 Three Pillars



Source: European Commission & Cowan.

However, other incentives might increase the uptake, and the regulator should ensure that while addressing sector-specific legislation, fragmentation does not result with different sectors deploying different solutions.

[55] Vandezande, 'Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor' (2024) 52 Comp Law & Security Rev, 105890.

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)[56]

[3.24] The Digital Operational Resilience Act (DORA) established a harmonised regulatory framework to strengthen information and communication technology (ICT) security of financial organisations. DORA entered into force on 16 January 2023 with application from 17 January 2025. McCarthy notes:

> 'Even though the EU's DORA is an immense initiative by any measure of a legislative effort to regulate for cyber-risks in finance, it is but part of the progress towards international standards for testing of cyber-risks and for reporting of cyber incidents and cyber-attacks. The aspirations in standard-setting can be plain to see. Yet, it can be more difficult to precisely delineate what coordinated testing and reporting frameworks should look like and how these frameworks are to function.'[57]

His comment highlights a common theme in regulation, namely the need for a dialectical process of improvement and feedback, plus a certain flexibility to how efforts are to be coordinated.

Fig. 3.11 DORA Framework

The DORA Six-Pack

ICT risk management	Principles and requirements on ICT risk management framework.
ICT third-party risk management	Monitoring third-party risk providers. Key contractual provisions.
Digital operational resilience testing	Basic and advanced testing.
ICT-related incidents	General requirements. Reporting of major ICT-related incidents to competent authorities.
Information sharing	Exchange of information and intelligence on cyber threats.
Oversight of critical third-party providers	Oversight framework for critical ICT third-party providers.

Source: ESMA & Cowan.

[3.25] The European Supervisory Authorities (ESAs) – The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) – are

[56] ESMA, 'Digital Operational Resilience Act (DORA)', https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora.

[57] McCarthy, 'Cyber-Risks in Modern Finance: Building Operational and Regulatory Resilience' (2023) 38(7) JIBLR, 233.

tasked with developing technical standards for implementation of the DORA framework.[58] The first batch of policy mandates were published on 19 June 2023 and the second batch 8 December 2023, covering:

- Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents.
- Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) on content, timelines and templates on incident reporting.
- RTS on threat-led penetration testing (TLPT).
- RTS on subcontracting of critical or important functions.
- Guidelines on oversight cooperation between ESAs and competent authorities.
- RTS on oversight harmonisation.

The ESAs have also published an Introductory Note providing an overview of the consultation papers, with a public consultation on the second batch of policy mandates completed in March 2024 and legal instruments finalised by the ESAs and submitted to the European Commission in July 2024.

ONLINE SAFETY AND MEDIA REGULATION ACT 2022 (OSMR)

[3.26] The OSMR has similar aims to the UK Online Safety Bill and was signed into law in Ireland on 10 December 2022 and commenced on 15 March 2023. This Act established the Media Commission to oversee the regulatory framework established by the OSMR. The Online Safety Framework in Ireland, which has three main parts:

(a) Online Safety and Media Regulation Act, the basis for the Media Commission's Online Safety Code;
(b) EU Digital Services Act, which became fully applicable on 17 February 2024; and
(c) EU Terrorist Content Online Regulation, the Media Commission being the competent authority since November 2023.[59]

The OSMR regulates 'relevant online services' designated by the Media Commission as well as entities that provide on-demand and broadcast media services, and such entities need to comply with the Media Commission's online safety codes. The OSMR requires on-demand service providers to register with the Media Commission and such providers must comply with obligations in

[58] ESMA, 'ESAs launch joint consultation on second batch of policy mandates under the Digital Operational Resilience Act', 8 December 2023, https://www.esma.europa.eu/press-news/esma-news/esas-launch-joint-consultation-second-batch-policy-mandates-under-digital.

[59] Opening Statement from Niamh Hodnett, Online Safety Commissioner at Coimisiún na Meán, 2 February 2024, https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_children_equality_disability_integration_and_youth/submissions/2024/2024-02-20_opening-statement-niamh-hodnett-online-safety-commissioner-coimisiun-na-mean_en.pdf.

respect to harmful online content. The providers should not make such content available and undertake to protect users, particularly children, from content deemed harmful. While the OSMR establishes a lot of territory, to some extent this is shifting ground. The notion of what is harmful will always be contested at the edges, but the difficulty for those subject to the Act is meeting the ongoing revision of codes set by the Media Commission. Future codes will have to take into account the emergence of new content generated by AI, and the Online Safety Commissioner has already raised concerns in respect to the protection of children in the use of AI. Although highlighting both the positives and negatives of AI, the Media Commissioner has put the platforms on alert that they are on the front line of protecting children in particular, noting 'growing concerns' of manipulation of imagery through deepfakes and AI-generated child sex abuse material.

COOKIES

[3.27] In April 2020, the Data Protection Commission provided guidance on cookies for Ireland.[60] The use of cookies and similar technologies on a website normally requires user consent.[61] This consent, under the General Data Protection Regulation (GDPR), must be a clear and affirmative act, freely given, specific, informed, and unambiguous. This does not apply where the cookie or other technology is strictly necessary to provide a service explicitly requested by the user, such as the need for cookies to provide the user with access and website functionality.[62] Users must be provided with easily accessible, 'clear and comprehensive' information on 'the technology used by the website to collect personal data, and the purpose for which the collected data will be used'.[63] In 2023, the European Data Protection Board (EDPB) published guidance on cookies and similar technologies in 2023, based on the findings of a cookie banner taskforce, and have made a 'cookie pledge' to simplify cookie banners.[64] The EDPB has also discussed the 'pay or ok' consent model, with guidance to follow. Several EU data protection supervisory authorities have also issued guidance on cookies. In 2024, the Spanish SA published guidance on analytics cookies, and in the previous year the Austrian SA published FAQs on cookies and data protection and the Belgian SA published a checklist.[65]

[60] DPC, 'Guidance note on Cookies and Other Tracking Technologies', April 2020 https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf.

[61] Regulation 5(3) of the ePrivacy Regulations.

[62] Regulation 5(5) of the ePrivacy Regulations.

[63] DPC guidance: https://www.dataprotection.ie/en/dpc-guidance/guidance-cookies-and-other-tracking-technologies.

[64] See https://www.covingtonblogs.com/2024/01/14/eu-supervisory-authorities-publish-new-guidance-on-cookies/.

[65] Belgian SA Cookies Checklist (in French): https://www.autoriteprotectiondonnees.be/publications/checklist-cookies.pdf.