AON

A&O SHEARMAN

The Insurability of Cyber Fines

Executive Summary

Cyber incidents are proliferating across every sector and jurisdiction, prompting new regulations aimed at promoting resilience, as well as fines and penalties for companies, executives and board members.

Cyber insurance is a critical pillar of any large organisation's cyber risk management strategy. It not only helps recover financial losses, costs and liabilities following an incident, but also promotes best practice and resilience through the underwriting process. While the overarching goal of cyber insurance is to provide comprehensive protection against the wide range of exposures that can arise from a cyber event, it is equally important to understand the limits of coverage.

Until recently, regulatory obligations for companies impacted by cyber incidents were driven primarily by data protection laws, with some jurisdictions adding narrowly scoped operational resilience requirements. That landscape has shifted significantly and continues to evolve. For example, Europe has introduced major frameworks such as DORA and NIS2, while the UK has recently published the Cyber Security and Resilience Bill.

There are clear trends emerging.

First, the sources of cyber fines have expanded considerably. Beyond data protection enforcement, an increasing body of cyber-specific and sectoral regulations heightens the risk of substantial monetary penalties and introduces non-monetary sanctions such as management bans and operational suspensions.

Second, the insurability of cyber fines remains an uncertain and jurisdiction-specific issue. National laws and public policy dictate whether such penalties can be covered by insurance, with some countries imposing blanket bans. Others allow insurance except in cases of deliberate or reckless misconduct.

Third, enforcement is becoming more assertive. Regulators are not only imposing significant fines but are also scrutinising the adequacy of technical and organisational measures, the timeliness of breach notification and the robustness of incident response.

Recent high-profile cases — ranging from multi-million Euro fines against global technology companies to sector-specific enforcement in healthcare and financial services — underscore the need for a proactive and holistic approach to cyber risk management. How newly implemented regulations will be enforced remains uncertain, as does whether they will lead to a material increase in enforcement activity.

The emergence of collective redress mechanisms and class actions, particularly following the implementation of the EU Representative Actions Directive, adds a further layer of litigation risk. Organisations must now anticipate both regulatory investigations and the possibility of coordinated claims from affected individuals and consumer groups.

Looking ahead, the regulatory environment is expected to become more demanding and fluid. Compliance is a continuous journey. Standards will likely rise over time, requiring sustained attention and adaptation from organisations and their leadership. The EU AI Act, with its stringent cybersecurity requirements for high-risk AI systems and the potential for cumulative penalties alongside the GDPR, exemplifies this direction of travel. New regulations place greater responsibility on boards and senior management, with direct liability and heightened expectations for oversight and investment in cyber resilience.

This survey highlights the importance of understanding local legal nuances, the need for close collaboration among legal, risk and insurance functions and the imperative of staying ahead of regulatory developments. As the threat landscape continues to evolve, so too must strategies for managing legal and financial exposure.

We hope that this report will serve as a practical resource for risk managers, in-house counsel and insurance professionals as they navigate the challenges of cyber risk in an increasingly regulated world.

Charlie Weston-Simons
A&O Shearman

Pablo Constenla
Aon

Table of Contents

What are the Principal Sources of Cyber Fines?

Chapter Summary

Across global jurisdictions, exposure to fines after cyber incidents is being driven by privacy, cybersecurity and sectoral regimes and regulations that are increasingly overlapping.

In the EU, GDPR is the dominant framework, imposing significant administrative fines for data breaches, unauthorised access, and failures in data protection. National laws supplement the GDPR, with local data protection authorities empowered to enforce compliance and impose fines with fines of up to EUR 20M or 4 percent of global turnover for serious cyber breaches.

The NIS2 Directive and its national implementations extend cyber resilience obligations to critical sectors, introducing additional fines for failures in cybersecurity risk management and incident reporting. Sector-specific regulations, such as DORA for financial services and the Cyber Resilience Act for digital products, further expand the landscape of potential fines. This combination of data protection, operational resilience and sector-specific regulations is replicated in the UK.

Outside the EU and UK, countries including South Africa, Saudi Arabia, and Turkey have enacted their own data protection and cybercrime laws, with varying degrees of alignment with the EU and UK standards.

Fines vary both by jurisdiction and by sector. They can be administrative or criminal, with some jurisdictions allowing for personal liability of directors and management. There is an increase in the complexity and severity of cyber fines, driven by both harmonised EU regulations and diverse national approaches.

There is also a trend towards higher maximum penalties, broader sectoral coverage, and the growing importance of non-monetary sanctions such as operational suspensions and management bans. We are also seeing higher ceilings and more granular, technical enforcement, especially for critical sectors and digital infrastructure.

The cyber insurance market has been taking a flexible approach to covering cyber fines, provided that such coverage is legally permissible. Where cyber fines on directors or senior executives are possible (e.g., under NIS2) directors and officers (D&O) liability insurance should respond on a similar basis.

Practical Actions for Organisations to Consider Now

- Monitor regulatory changes: Stay updated on new laws (e.g., Cyber Resilience Act, EU AI Act).
- Establish robust incident response and breach notification procedures.
- Ensure senior management is aware of personal liability risks.
- Conduct a jurisdictional risk mapping exercise: Identify which laws apply to your operations across countries and sectors.
- Appoint a compliance lead: Assign responsibility for monitoring regulatory changes and coordinating responses.
- Regularly review and ensure your compliance with GDPR, NIS2, DORA, and sector-specific regulations.
- Run tabletop exercises: Simulate breach scenarios to test response readiness and regulatory engagement.
- Conduct regular cybersecurity audits and staff training: Demonstrate proactive compliance.
- Maintain up-to-date records of data processing and security measures in case of a regulatory review or investigation.
- Engage with regulators proactively: Build relationships with data protection authorities and cybersecurity agencies to facilitate smoother incident handling.
- Ensure best in class insurance coverage is obtained to cover cyber fines as far as possible.

Belgium

Belgium's data protection and privacy regime is primarily based on EU law, with the national government implementing supplementary legislation.

Data Protection/Privacy Laws and Regulations

GDPR

The EU General Data Protection Regulation (**GDPR**)[1] is directly applicable in Belgium and is the principal legal framework for regulatory fines arising from cyber incidents (Cyber Fines), such as data breaches, unauthorised access and loss of personal data. The GDPR is supplemented by the Belgian Data Protection Act of 30 July 2018 (**Belgian Data Protection Act**), which provides for its national implementation.[2]

The Belgian Data Protection Authority (Autorité de protection des données/ Gegevensbeschermingsautoriteit, BDPA3) is the competent authority responsible for enforcing GDPR compliance and imposing administrative Cyber Fines. These fines are determined on a case-by-case basis and must be effective, proportionate and dissuasive.

The GDPR distinguishes between two tiers of administrative fines, with due regard to the nature, gravity and duration of the infringement:

Tier 1: Up to EUR 10M or 2 percent of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher.[4] These lower Cyber Fines are generally imposed for failures to comply with certain procedural or organisational obligations related to data breaches such as:

- Failure to notify the BDPA of a data breach within 72 hours.
- Failure to communicate a data breach to the affected data subjects.
- Failure to maintain an internal record of data breaches.
- Failure to implement adequate security measures.

Tier 2: Up to EUR 20M or 4 percent of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher.[5] These higher Cyber Fines are generally imposed for more serious, substantive violations that underlie or lead to a data breach, such as breach of the core data protection principles (e.g., integrity, confidentiality), violation of data subjects' rights and unlawful international data transfers.

Although Belgium does not have a formal methodology for calculating fines, the BDPA consistently refers to the European Data Protection Board (EDPB) Guidelines 04/2022.[6] In practice, Cyber Fines imposed by the BDPA have been more modest compared to those imposed by supervisory authorities in certain other EU Member States.

For certain serious breaches, criminal prosecution is possible (albeit exceptional), with maximum fines for legal entities up to EUR 240,000 (for legal entities and/ or individuals).

Eprivacy Directive

The ePrivacy Directive[7] aligns the laws of EU Member States to guarantee a consistent level of protection for the right to privacy and the processing of personal data within the electronic communications sector.

Unlike the GDPR, the ePrivacy Directive does not establish specific administrative Cyber Fines. Instead, it establishes a legal framework that requires each Member State to implement its provisions through national legislation and to determine appropriate fines. Belgium has implemented the requirements of the ePrivacy Directive primarily through the Belgian

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).
2. Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Belgian Data Protection Act).
3. dataprotectionauthority.be/citizen.
4. Article 83(4) GDPR.
5. Article 83(5) GDPR.
6. EDPB Guidelines 4/2022.
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications or ePrivacy Directive).

Act of 13 June 2005 on electronic communications (**Telecommunications Act**), which applies to electronic communication providers.[8]

The Belgian Institute for Postal Services and Telecommunications (*Belgisch Instituut voor Postdiensten en Telecommunicatie, Institut belge des services postaux et des télécommunicationsn, BIPT*)[9] has the power to impose administrative fines for infringements of the Telecommunications Act by electronic communication providers, including those related to data security and data breach notification. The maximum administrative fine is generally up to 1 percent of the turnover generated by telecommunication activities in the preceding accounting year. In certain cases and serious breaches, criminal fines of up to EUR 800,000 may be imposed on legal entities.[10]

Cyber-Specific and Relevant Resilience Laws and Regulations

NIS2 Directive

The NIS2 Directive[11] is the EU's principal legislative instrument for strengthening cybersecurity and resilience across Member States. It applies to entities in critical sectors, such as data centre service providers, cloud computing service providers and providers of public electronic communications networks, provided they meet specific company size requirements and operate or offer services within the EU. The NIS2 framework distinguishes entities in critical sectors between, on the one hand, 'essential' entities and, on the other hand, 'important' entities, with varying degrees of regulatory supervision.

In Belgium, the NIS2 Directive has been transposed into national law through the Belgian NIS2 Act of 26 April 2024 (**NIS2 Act**)[12] and further implemented by the Belgian Royal Decree of 9 June 2024.[13]

The NIS2 Act applies to entities operating in 18 critical sectors, including: Energy, Transport, Banking, Financial market infrastructures, Health, Digital infrastructure, Public administration, Space, Postal and courier services, Manufacture, production and distribution of chemicals, Food production, processing and distribution, Research.

On the basis of the NIS2 Act, the Centre for Cybersecurity Belgium (**CCB**)[14] can impose administrative fines for infringements of the NIS2 Act and, where appropriate, coordinate with the competent sectoral authorities whose jurisdiction corresponds to the activities of the infringing entity. The sectoral authorities can also impose administrative fines upon the CCB's approval thereof. The maximum fines are significant:

- **For important entities:** up to EUR 7M or 1.4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.[15]
- **For essential entities:** up to EUR 10M or 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.[16]

In determining a sanction that is both appropriate and proportionate, the CCB must consider, at a minimum, factors such as the classification of the entity concerned, the seriousness and duration of the infringement, any previous infringements, the material or non-material damage caused and the degree of intent or negligence involved.[17]

In cases of repeated infringements of the same nature within a three-year period, the applicable fine may be doubled. Moreover, directors and members of senior management may be held personally liable where non-compliance is attributable to their actions or omissions.

8. Belgian Act of 13 June 2005 on electronic communications (*Telecommunications Act*).
9. bipt.be.
10. Article 145 Telecommunications Act.
11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).
12. Belgian Act of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2 Act).
13. Belgian Royal Decree of 9 June 2024 implementing the Act of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public safety.
14. ccb.belgium.be.
15. Article 59, 4° NIS2 Act.
16. Article 59, 5° NIS2 Act.
17. Article 54 NIS2 Act.

Cyber Resilience Act

The Cyber Resilience Act (**CRA**)[18] is a directly applicable EU regulation in Belgium. It imposes uniform cybersecurity obligations on manufacturers, importers and distributors of products with digital elements. The CRA complements existing EU cybersecurity legislation, such as the NIS2 Directive and aims to harmonise cybersecurity standards across the EU internal market.

The CRA's implementation is phased, with key requirements entering into force between late 2024 and 2027. Belgium is currently in a transitional phase regarding the implementation of the CRA. Manufacturers will be required to begin reporting vulnerabilities and cybersecurity incidents starting from September 2026. Full compliance with all CRA requirements, including essential cybersecurity obligations for products with digital elements, will become mandatory by December 2027.

In Belgium, the CCB is the designated authority empowered to monitor compliance and impose administrative fines for breaches of the CRA's requirements. The CCB exercises its enforcement powers with due regard to the nature, gravity and duration of any infringement.[19] Failure by manufacturers to comply with the essential cybersecurity requirements of the CRA can result in administrative fines of up to EUR 15M or, if the offender is an undertaking, up to 2.5 percent of its total global annual turnover for the preceding financial year, whichever is higher.[20] For distributors and importers, non-compliance may lead to administrative fines of up to EUR 10M or, if the offender is an undertaking, up to 2 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher.[21]

Cybersecurity Act

The Cybersecurity Act[22] strengthens the mandate of the European Union Agency for Cybersecurity (**ENISA**)[23] and establishes a harmonised EU-wide cybersecurity certification framework for information and communication technology products, services and processes. This framework allows for the issuance of European cybersecurity certificates and conformity statements, ensuring that ICT products, services and processes meet specific security standards.

In Belgium, the Cybersecurity Act has been transposed into national law through the Belgian Act of 20 July 2022[24] and further implemented by the Belgian Royal Decree of 16 October 2022.[25]

The Cybersecurity Act requires Member States to establish a regime of effective, proportionate and dissuasive penalties for infringements.[26] In Belgium, the CCB is mandated as the national cybersecurity certification authority, tasked with monitoring compliance and, where necessary, imposing penalties. Manufacturers or providers of ICT products, services, or processes who fail to meet the self-assessment conformity requirements may face administrative fines of up to EUR 100,000. Similarly, holders of European cybersecurity certificates at the basic assurance level who breach the obligations arising from the corresponding cybersecurity certification scheme may be fined up to EUR 100,000. For certificates issued at the substantial or high assurance levels, administrative fines may reach up to EUR 150,000. Anyone who knowingly provides false or incomplete information, or engages in any other fraudulent act or negligence, can be subject to administrative fines of up to EUR 200,000. [27]

18. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828.
19. The Cyber Resilience Act (CRA) | CCB Safeonweb.
20. Article 64 (2) CRA.
21. Article 64 (3) CRA.
22. Regulation (EU) 2019/ of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
23. enisa.europa.eu.
24. Belgian Act of 20 July 2022 on the certification of cybersecurity of information and communication technology and on the designation of a national cybersecurity certification authority.
25. Royal Decree of 16 October 2022 implementing the Act of 20 July 2022 on the certification of cybersecurity for information and communication technology and on the designation of a national cybersecurity certification authority, and amending the Royal Decree of 10 October 2014 establishing the Centre for Cybersecurity Belgium.
26. Article 65 Cybersecurity Act.
27. Article 23, §2-6 Belgian Act of 20 July 2022.

Sector-Specific Laws and Regulations (e.g., Operational Resilience Rules and Critical Third Parties Regime Which Applies to the Financial Sector in E&W)

DORA

The DORA Regulation[28] establishes comprehensive ICT risk management, incident reporting and digital operational resilience obligations for a broad spectrum of entities in the financial sector. DORA's scope covers more than 20 categories of financial entities, including banks, investment firms, insurance and reinsurance undertakings, credit and payment institutions, crypto-asset service providers. It also extends to third-party service providers that support critical functions for these financial entities.

In Belgium, the enforcement and supervision of DORA are entrusted to the sector's national competent authorities: the National Bank of Belgium (**NBB**) and the Financial Services and Markets Authority (FSMA). These authorities are responsible for monitoring compliance, conducting investigations and imposing sanctions where necessary.

Non-compliance with DORA can result in substantive administrative fines of up to 2 percent of the undertaking's total annual global turnover, or up to 1 percent of its average daily global turnover. Both individuals and companies can be fined up to EUR 1M. Furthermore, critical third-party ICT service providers that support financial entities may face even higher penalties, with fines reaching up to EUR 5M for companies and EUR 500,000 for individuals. Failure to report major ICT-related incidents or cyber threats as required under DORA may result in additional financial sanctions.[29]

CER Directive

The CER Directive[30] aims to strengthen the physical resilience of critical entities that provide essential services in 11 key sectors, such as energy, transport, healthcare and public administration. It introduces obligations for Member States to identify critical entities, assess risks and ensure that these entities implement appropriate resilience measures.

In Belgium, the CER Directive is currently in the process of being transposed into national law. Until the transposition is complete, the security and protection of critical infrastructure continues to be governed by the Belgian Act of 1 July 2011 on the Security and Protection of Critical Infrastructure (in addition to the NIS2 framework, as discussed above).[31] This Act provides for penalties in cases of non-compliance with internal security obligations, including criminal fines up to EUR 192,000 for legal entities.[32]

28. 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 (DORA Regulation).
29. Article 50 DORA.
30. Directive on the resilience of critical entities 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive).
31. Act of 1 July 2011 on the Security and Protection of Critical Infrastructure.
32. Article 26, §1 Act of 1 July 2011 on the Security and Protection of Critical Infrastructure.

Luxembourg

Regulatory exposure in Luxembourg is largely driven by supra-national EU instruments that apply directly or must be transposed into Luxembourg law, supplemented by domestic statutes, regulations and circulars enforced by the competent Luxembourg supervisory authorities. The most relevant sources are detailed below:

- The EU General Data Protection Regulation (Regulation [EU] 2016/679 — **GDPR**) which has direct effect in Luxembourg, which foresees administrative fines of up to the higher of EUR 20M or 4 percent of the preceding year's worldwide annual turnover.
- EU Directive 2022/2555 (**NIS2 Directive**), applicable to entities other than those of the financial sector and which expands the scope of former NIS1 Directive. NIS2 Directive distinguishes between: (a) Essential Entities (**EE**) including energy, finance, health, transport, and (b) Important Entities (**IE**) such as digital providers, postal services, manufacturing. Under NIS2 Directive, fines for IE can reach up to EUR 7M or 1.4 percent of global annual turnover, while for EE, they may go as high as EUR 10M or 2 percent of global turnover. Luxembourg has yet to implement the NIS2 Directive and the draft Bill 8364 (the **Bill**) remains under review. However, the Bill retains the NIS2 ceilings for the fines (Article 26 of the Bill).
- Luxembourg also enforces the Cyber Resilience Act (**CRA**) which imposes initial obligations from September 2026, with full compliance required by December 2027. Non-compliance may result in fines of up to EUR 15M or 2.5 percent of global annual turnover, whichever is higher. The law of 20 December 2024 designated Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (**ILNAS**) as the competent authority.

For entities of the financial sector in Luxembourg, the Digital Operational Resilience Act (Regulation [EU] 2022/2554 — **DORA**) applies since 17 January 2025. Luxembourg had already since January 2024 required financial entities to disclose any cyber incidents. The Law of 1 July 2024 (the **Law of 2024**) designates the Commission de Surveillance du Secteur Financier (**CSSF**), the Commissariat aux Assurances (**CAA**) as the competent authorities. Under Article 20 to 24 of the Law of 2024 the CSSF and the CAA may impose:

- On in-scope financial entities, administrative fines of up to the higher of EUR 5M or 10 percent annual turnover;
- On members of the management body and other responsible individuals, personal fines of up to EUR 5M.

Critical ICT third-party service providers may also be fined by one of the three European Supervisory Authorities, the **Lead Overseer** for periodic penalty payments of up to 1 per cent of their average daily worldwide turnover for each day of non-compliance, in addition to lump-sum fines.

For completeness, the Law of 3 March 2010 clarifies that where a crime or offence is committed in the name of and in the interests of a legal entity by one of its legal bodies or by one or more of its de jure or de facto directors, the legal entity may be held criminally liable. The criminal liability of legal entities does not preclude the criminal liability of natural persons who are perpetrators or accomplices of the same offences. Fines against corporations for offences classified as correctional matters (*matière correctionnelle*) may reach twice the maximum amount applicable to natural persons, as specified in the law governing the offence.

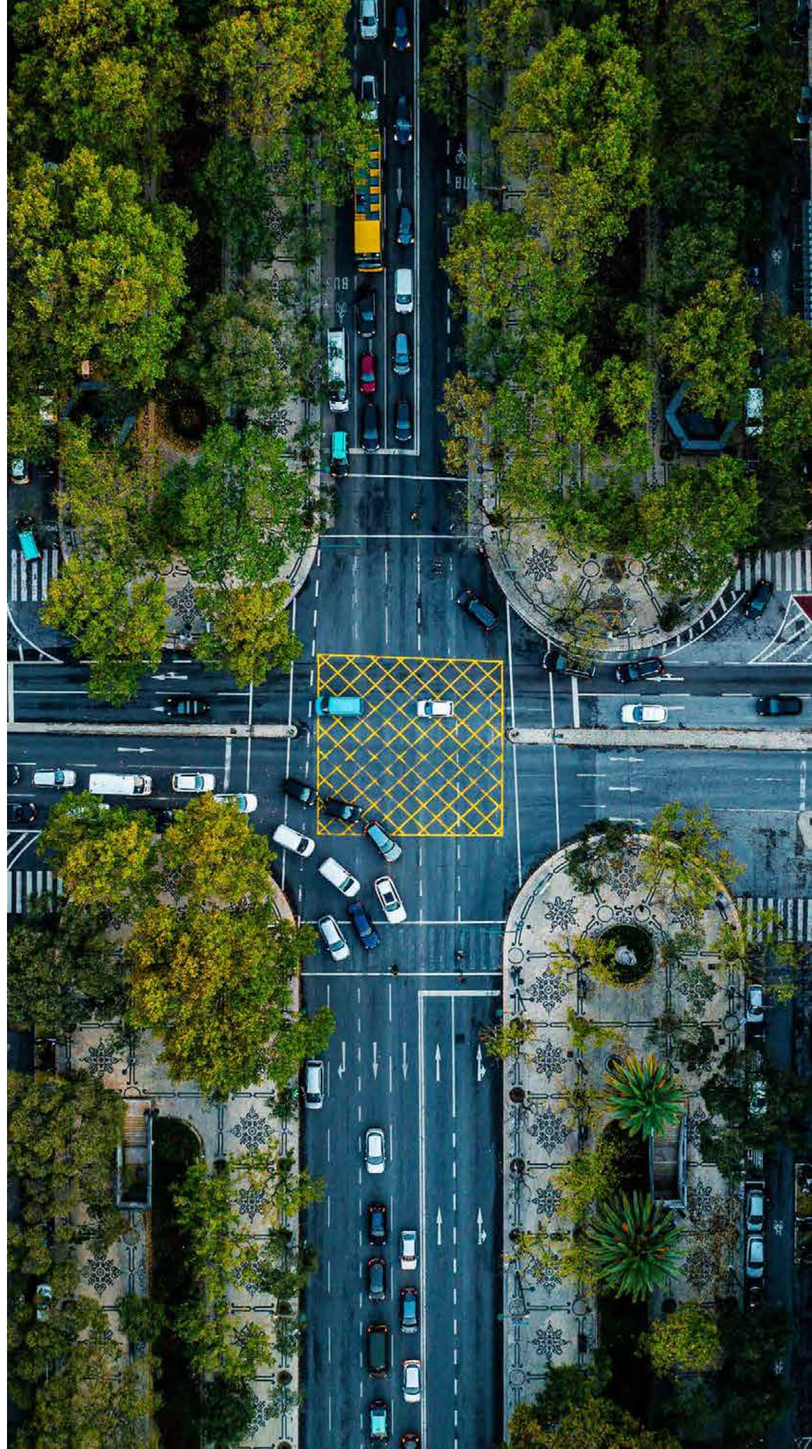
Portugal

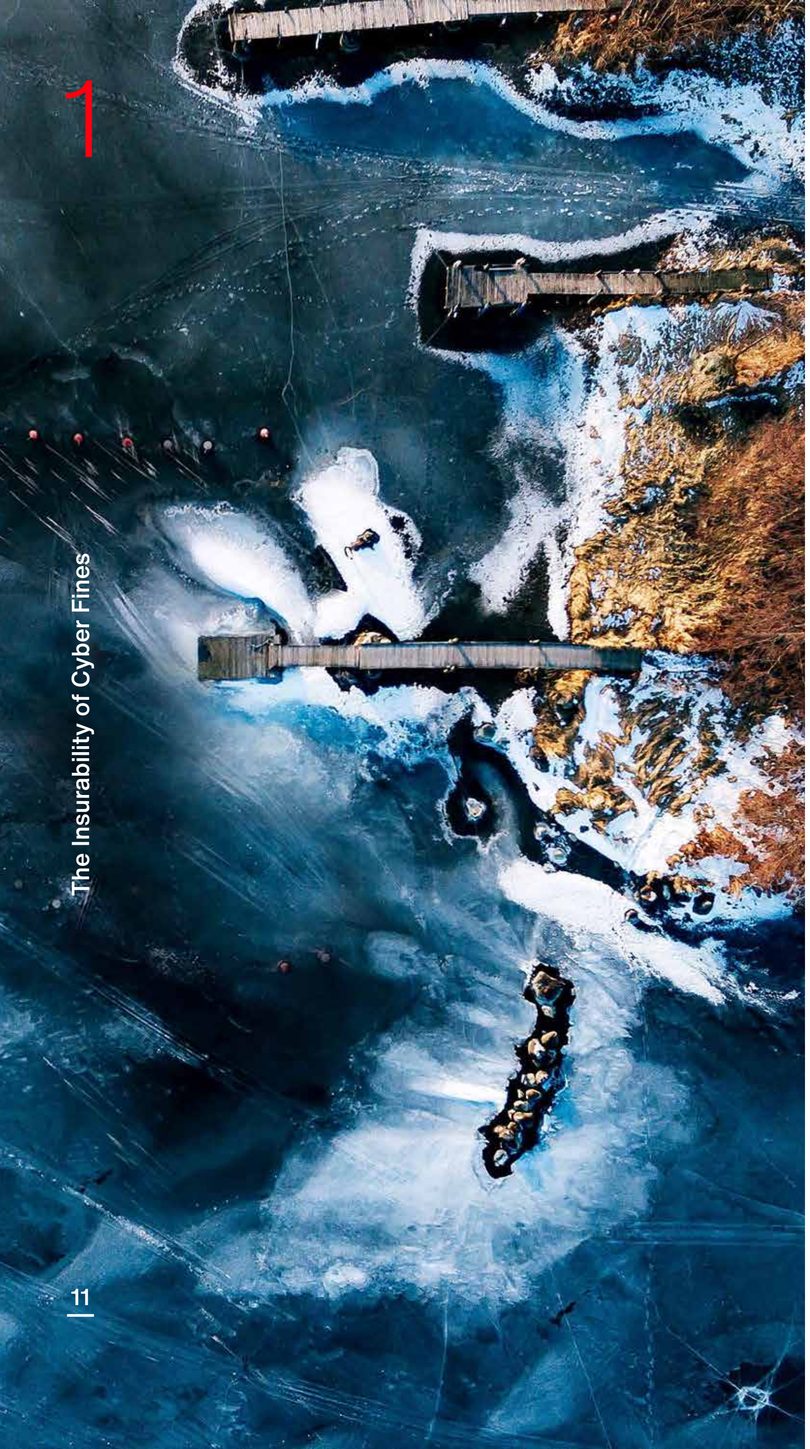
There are several legal instruments that provide for regulatory fines resulting from cyber incidents, as these incidents often involve breaches of multiple legal and regulatory duties. Without aiming to be exhaustive, the most relevant include:

1. The General Data Protection Regulation (**GDPR**) (Regulation [EU] 2016/679), together with Law No. 58/2019, implements it in Portugal; and the ePrivacy Directive (Directive 2002/58/EC) and its transposition through Law No. 41/2004.
2. The NIS2 Directive (Directive [EU] 2022/2555) and Implementing Regulation (EU) 2024/2690, which aims to enhance the security of network and information systems within the EU. In this context anticipating the future landscape of regulatory fines, the Draft Law No.7/XVII must also be taken into account (A draft legislative proposal for NIS2's transposition, having been approved by the Council of Ministers, that is presently under consideration and is expected to receive approval from the Parliament, hereinafter referred to as "Draft Law No. 7/XVII"). Until the transposition of the NIS2 Directive, Law No. 46/2018 of 13 August, which transposed the NIS1 Directive and Decree Law No. 65/2021 of 30 July, which implemented Regulation (EU) 2019/881, remain in force and establish sanctioning mechanisms.

Regarding the resilience of critical sectors such as energy, water and rail transport, Directive (EU) 2022/2557 and Decree Law No. 22/2025, which transposes it, also provide for sanctions in the event of non-compliance.

For the financial sector, Regulation (EU) 2022/2554 (**DORA**), read jointly with Directive (EU) 2022/2556 and Delegated Regulation (EU) 2024/1774, is also worth highlighting. However, Portugal has not yet introduced national legislation to implement DORA, which means there are currently no specific Portuguese sanctions for direct breaches of its obligations, though general sanctions may still apply if instructions from the Bank of Portugal or other supervisory authorities are not followed.





Finland

In Finland, the principal source of Cyber Fines is the Cybersecurity Act (124/2025) which was enacted in connection with the national implementation of the Directive (EU) 2022/2555 (**NIS2 Directive**). Under the Cybersecurity Act, administrative fines may be imposed on entities that intentionally or through gross negligence fail to comply with the cybersecurity risk management obligations set out in the Act. These obligations, which are based on the NIS2 Directive, include implementing cybersecurity risk management measures and reporting incidents to the supervisory authorities. Another key source for Cyber Fines in Finland is the Data Protection Act (1050/2018) is the Finnish supplementing act for the application of the EU General Data Protection Regulation. A cyber incident resulting in a personal data breach may also constitute a violation of data protection laws and result in an administrative fine being imposed by the sanctions board of the Finnish Office of the Data Protection Ombudsman, in accordance with section 24 of the Data Protection Act.

Although the NIS2 Directive does not limit the application of the GDPR and infringements of the Cybersecurity Act that entail a breach of personal data must be notified to the Data Protection Ombudsman, it should be noted that an administrative fine cannot be imposed under both the Cybersecurity Act and the Data Protection Act, if the fine would be based on the same violating conduct.

Regarding financial entities, section 38, subsection 1, subparagraph 12 of the Act on the Financial Supervisory Authority (878/2008) allows the Finnish Financial Supervisory Authority (FIN-FSA) to impose an administrative fine on anyone who wilfully or negligently fails to comply with the obligations of the EU Regulation 2022/2554 on digital operational resilience for the financial sector (**DORA**), such as ICT risk management and ICT related incident reporting.

In the future, the Finnish implementing legislation of the Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (**CRA**), will include a possibility of imposing Cyber Fines for products within its scope. The Finnish supplementing legislation has not yet been enacted, but the draft government proposal for the national act already includes a mention of an administrative fine that can be imposed on the various economic operators, such as manufacturers, importers and distributors, for the non-compliance of CRA obligations. These obligations include conformity with cybersecurity requirements for products and reporting of possible cyber vulnerabilities.

South Africa

Data Protection/Privacy Laws and Regulations

The National Cybersecurity Policy Framework (**NCPF**), the Cybercrimes Act, 2020 and the Protection of Personal Information Act, 2013 (**POPIA**) form a complementary triad regulating South Africa's cybersecurity and data protection/privacy landscape.

The NCPF is a strategic document that outlines the approach to cybersecurity in South Africa and provides the overarching principles and guidelines for securing South Africa's cyberspace. The NCPF outlines national objectives, promotes collaboration across sectors and assigns roles to entities like the State Security Agency for coordinating incident response. It is not a law but a policy framework that guides the development and implementation of cybersecurity measures across government and private sectors and serves as the foundation for developing specific laws, regulations and policies relating to cybersecurity.

The Cybercrimes Act gives effect to key aspects of the NCPF by addressing criminal activities in the digital realm. Its primary objectives are to criminalise a broad range of cyber conduct, establish investigation and prosecution procedures, provide mechanisms for preserving and disclosing electronic evidence and impose related penalties as well as compliance obligations on electronic communications service providers and financial institutions. The Cybercrimes Act is South Africa's first comprehensive legislation aimed at addressing cybercrime.

The concept of "cybercrimes" is dealt with in Chapter 2 of the Act and includes offences related to:

- **Unlawful access** to a computer system or data storage medium (section 2);
- **Unlawful interception** of data (section 3);
- **Unlawful acts in respect of software or hardware tools** for purposes of committing an offence under the Act (section 4);
- **Unlawful interference** with data, a computer programme, a computer data storage medium or a computer system (sections 5 and 6);
- **Unlawful acquisition, possession or use of a password** or similar data for purposes of committing an offence under the Act (section 7);
- **Cyber fraud and extortion**, by using digital means to defraud or extort (section 8 and section 10);
- **Cyber forgery or utterances**, by creating or using false data with the intention to defraud (section 9);
- **Theft of incorporeal property** (section 12);
- **Malicious communications**, this includes sending data messages that incite violence, threaten individuals or disclose intimate images without consent (sections 13 to 16); and
- **Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring another to commit an offence** (section 17).

The penalties for these offences under the Cybercrimes Act include fines, imprisonment, or both, with the severity determined by the nature and seriousness of the specific offence committed (section 19). For example:

- Offences relating to inciting or threatened damage to property or violence through a data message and disclosure of a data message of an intimate image, carry a potential imprisonment term of up to three years.
- Offences such as unlawful access to a computer system carry a potential imprisonment term of up to five years.
- Offences such as those relating to unlawful interception of data carry a potential imprisonment term of up to 10 years.
- Aggravated offences related to restricted computer systems carry a potential imprisonment term of up to 15 years.

For certain offences such as cyber fraud, if the relevant penalty is not specified in any other law, the court has a discretion to impose an appropriate sentence. The value of any potential fine is not referenced in the Cybercrimes Act. Where an imprisonment term is included, the value of such fine will be calculated with reference to such term, in accordance with the Adjustment of Fines Act, 1991. The Adjustment of Fines Act provides a framework for converting imprisonment terms into monetary fines, where the value of the fine is not otherwise provided for. Based on current adjustment amounts, an imprisonment term of one year may be adjusted to a fine of ZAR 40,000.

South Africa does not currently have legislation that specifically addresses cyber incidents without a criminal or malicious element. While the Cybercrimes Act targets unlawful cyber conduct, it does not regulate non-criminal cyber incidents, such as accidental data loss, system outages, or operational disruptions caused by internal failures or third-party service issues.

In such cases, regulatory exposure typically arises under POPIA, which focuses on the protection of personal information. As part of the lawful conditions for processing personal information, POPIA mandates responsible parties (similar to data controllers under the GDPR), to implement and maintain reasonable technical and organisational measures to protect against the loss of, damage to or unauthorised destruction of personal information, as well as unauthorised access to or processing of personal information as well as report security breaches to the Information Regulator (the supervising and enforcement body under the Act) and affected data subjects.

POPIA provides for a number of remedies and penalties aimed at addressing and rectifying the harm caused by a violation of data protection rights and to serve as a deterrent to prevent future violations.

Any person may submit a complaint to the Information Regulator alleging interference with the protection of personal information of a data subject. Such interference typically results from a breach of one or more of the conditions for lawful processing of personal information, failure to report a data breach and/or non-compliance with cross-border transfer restrictions.

Due to the Information Regulator's focus on promoting compliance over imposing punitive measures, one of the primary remedies under POPIA involves the Information Regulator investigating complaints and directing remedial action. Following its investigation, the Information Regulator is empowered to, among others, issue an enforcement notice requiring the responsible party to take or refrain from taking certain steps, or stop processing personal information as specified in the notice, within a specific time-period.

Depending on the specific contravention, which includes non-compliance with an enforcement notice, a person convicted of certain offences under POPIA may be liable to a penalty in the form of fine or imprisonment of up to 10 years, or both (section 107). As above, based on current adjustment amounts, an imprisonment term of 10 years may be adjusted to a fine of ZAR 400,000 in accordance with the Adjustment of Fines Act.

POPIA also makes provision for administrative fines. If a responsible party is alleged to have committed an offence in terms of POPIA, the Information Regulator may issue an infringement notice, which may include imposition of an administrative fine up to ZAR 10M.

In addition to the principles under POPIA relating to processing activities generally, the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (**RICA**) applies to any processing activities which specifically involve the interception or monitoring of communications.

Generally, RICA prohibits the interception of communications except in specific circumstances. This prohibition applies to both **direct communications**, such as face-to-face exchanges and **indirect communications**, which include the transmission of information through electronic means that are not immediately accessible or audible to a third party. Examples of indirect communications include emails, text messages, as well as data transmitted over the Internet and associated records such as browsing activity and search history.

In a business context, interception is permissible in the following circumstances:

- Where the interception is carried out by a party to the communication, for example, recording your own otherwise private telephone conversation (section 4 of RICA);
- With prior written consent from one of the parties to the communication, unless the interception is for the purposes of committing an offence (section 5 of RICA); or
- With regard to indirect communications, where such interception is in course of carrying on of any business, provided certain requirements are met — this is colloquially referred to as the 'business purposes exception' (section 6 of RICA).

The conditions to be met to rely on the business purposes exception are set out in section 6 of RICA, namely:

- The communication must be an indirect communication, transmitted over a telecommunication system;
- The communication must relate to a business transaction, take place in the course of carrying on such business, or otherwise relate to that business;
- The system controller, such as the CEO or equivalent senior official of the business, must consent (express or implied) to the interception;

The purpose of the interception must be to either:

- Monitor or keep a record of indirect communications in order to establish the existence of facts, for purposes of investigating or detecting unauthorised use of the telecommunication system, or to secure or as an inherent part of the effective operation of the telecommunication system; or
- Monitor indirect communications made to a confidential voice-telephony counselling or support service which is free of charge and operated in such a way that users may remain anonymous, if they so choose;
- The telecommunication system concerned must be provided for use in connection with the business (wholly or partly); and
- The system controller must take reasonable steps to inform users, in advance, that their communications may be intercepted when using the telecommunications system.

Any person who intercepts indirect communications in contravention of the aforesaid conditions is guilty of an offence, in terms of section 51 of RICA. Upon conviction, the person responsible may be liable to a fine of up to ZAR 2M, or imprisonment for up to 10 years.

Cyber-Specific and Relevant Resilience Laws and Regulations

South Africa currently lacks comprehensive cybersecurity legislation which unifies and regulates cyber resilience and security across both public and private sectors. A Cybersecurity Bill was initially introduced in 2015 and revised in 2018, aiming to establish a coordinated national framework. Whilst discussions around the Cybersecurity Bill resumed in late 2023, formal adoption remains pending.

Notwithstanding the absence of unified legislation, South Africa has enacted other laws that regulate discrete aspects of cyber conduct. For example, the Electronic Communications and Transactions Act, 2002 (**ECTA**) (which previously dealt with cybercrime) was enacted to provide a legal framework for the facilitation of electronic communications and transactions. One of its key objectives is to prevent the abuse of information systems, such as the Internet.

Although many of its cybercrime provisions have since been superseded by the Cybercrimes Act, ECTA remains relevant and continues to support the broader regulatory environment by promoting secure digital practices and encouraging responsible use of electronic systems in the context of electronic communications and transactions. Notably, ECTA also provides for the appointment of a “cyber inspector” from among the employees of the Department of Communications and Digital Technologies.

The powers of the cyber inspector, as set out in section 81 of ECTA, include the power to monitor and inspect any website or activity on an information system in the public domain. The cyber inspector may also, on request, assist other regulatory authorities, such as the South African Police Service (**SAPS**), with regulatory investigations.

Sector-Specific Laws and Regulations

Section 54 of the Cybercrimes Act imposes specific reporting obligations on electronic communications service providers and financial institutions. Where such entities become aware that their electronic communications service or network has been involved in the commission of a cybercrime under the Cybercrimes Act, they are required to report the offence to the SAPS without undue delay and, where feasible, within 72 hours of becoming aware of the incident. They must also preserve any information that may assist SAPS in investigating the offence. Failure to comply with these obligations constitutes an offence and may result in a fine of up to ZAR 50,000. Notwithstanding such reporting obligation, the Cybercrimes Act does not imposed a duty on service providers or financial institutions to pro actively monitor data or seek out unlawful activity.

While there are certain frameworks and regulatory standards to address cybersecurity risks in specific industries in South Africa, these remain relatively limited. Most existing obligations are derived from general legislation, such as the Cybercrimes Act, POPIA and ECTA — with only a few sectors, like finance and telecommunications, beginning to develop more targeted regulatory requirements.

Financial Sector

In May 2024, the Financial Sector Conduct Authority (responsible for market conduct regulation within South Africa’s financial sector) and the Prudential Authority (responsible for maintaining the safety and soundness of financial institutions) issued a joint standard on cyber security (the **Joint Standard).**

The Joint Standard applies to a wide range of financial institutions in South Africa, including banks, insurers, retirement funds, fund administrators and collective investment scheme managers, as well as their controlling companies. It aims to address the sector’s growing concerns regarding evolving cyber threats and strengthen cyber risk management and resilience across the sector.

Under the Joint Standard, financial institutions are requi red to establish and maintain a cybersecurity framework, including policies and procedures that align with industry standards and best practices. These policies and procedures must be aimed at preventing, detecting, responding to and recovering from, cyber incidents.

The Joint Standard is principle-based, meaning that financial institutions must implement its requirements in a manner relative to their risk appetite, nature, size and complexity. However, it does contain

certain minimum information, security measures and governance expectations, including incident response planning, vulnerability assessments and cybersecurity awareness training.

Unlike the Cybercrimes Act, which criminalises specific cyber offences, the Joint Standard focuses on preventative and resilience-building measures within regulated financial institutions.

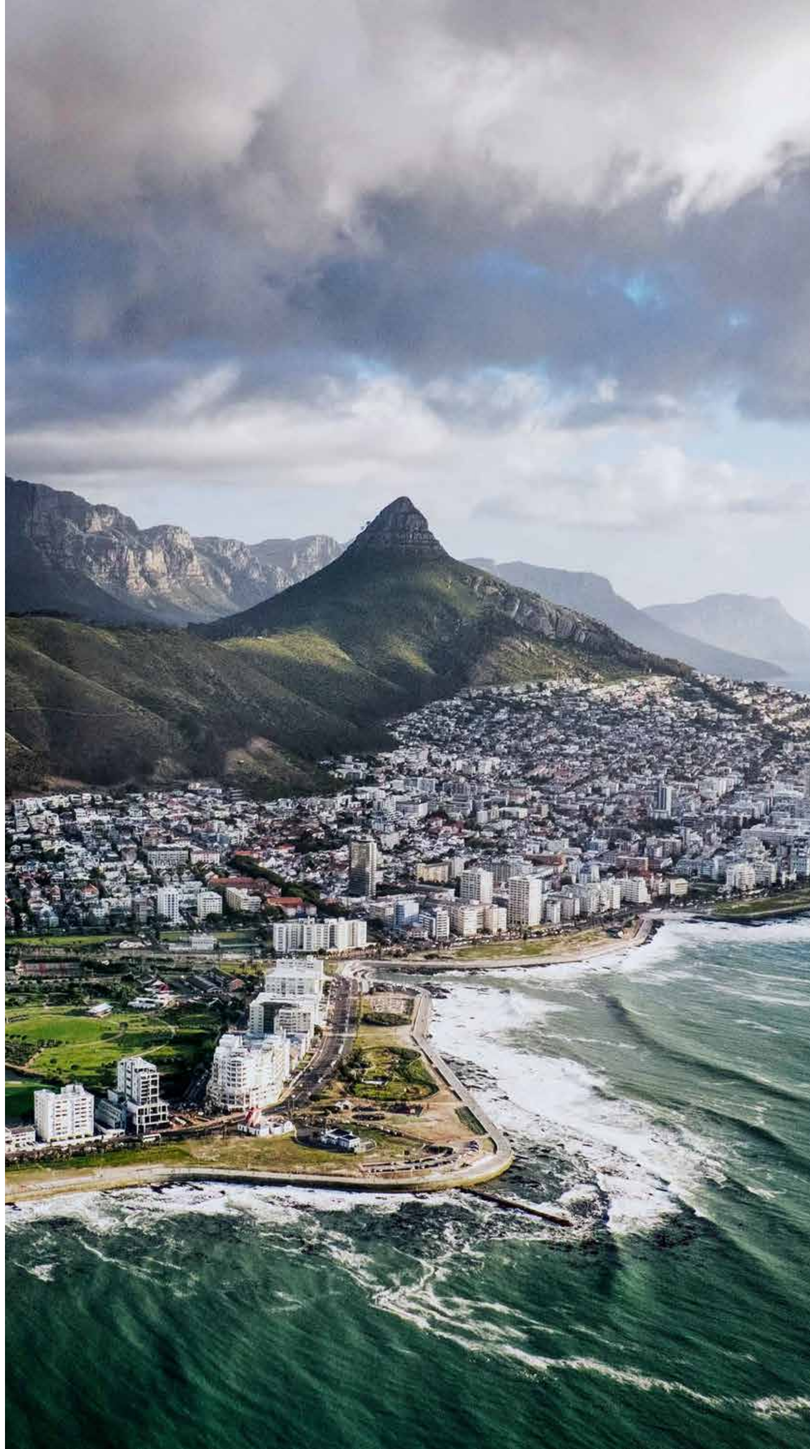
Telecommunications Sector

The Independent Communications Authority of South Africa (**ICASA**) plays a central role in ensuring that telecommunications service providers implement robust network security and data protection measures. These requirements are founded in ECTA and RICA.

While ICASA has not yet issued detailed cybersecurity regulations, in April 2019 it published its findings and position paper following an inquiry into its role and responsibilities in cybersecurity. The paper was the result of a consultative process involving written and oral submissions from stakeholders across the public and private sectors.

ICASA concluded that although its current mandate under ECTA is limited to network reliability and information security, it does have a role to play in the broader cybersecurity landscape. It also emphasised that cybersecurity is a multi-faceted and multi-stakeholder issue and that enabling legislation is required to clarify roles, avoid duplication of efforts and ensure coordinated action. ICASA expressed its intention to collaborate with other government agencies and industry players to strengthen cyber resilience in the communications sector.

Although no further information regarding ICASA's plans have been released, it is expected that future steps may include sector-specific cybersecurity regulations under ECTA.



Italy

Data Protection/Privacy Laws and Regulations and the Italian Data Protection Code (Legislative Decree No. 196/2003)

The GDPR, directly applicable in Italy, is the cornerstone of data protection law. It is supplemented by the Italian Data Protection Code (Legislative Decree No. 196/2003, as amended). The Italian Data Protection Authority ("**Garante per la Protezione dei Dati Personali**" or the "**Garante**") is empowered to impose significant administrative fines for breaches, such as failure to implement adequate security measures, unauthorised data processing, or failure to notify data breaches. Pursuant to Article 83 of the GDPR, fines can reach up to EUR 20M or 4 percent of the annual global turnover, whichever is higher.

Cyber-Specific and Relevant Resilience Laws and Regulations

Network and Information Security 2 (NIS2) Directive and Italian Implementing Legislation

The NIS2 Directive, transposed in Italy by Legislative Decree No. 138/2024, establishes stringent cybersecurity obligations for public and private entities operating in critical sectors.

The National Cybersecurity Agency (Agenzia per la Cybersicurezza Nazionale or **ACN**) is the competent authority for the imposition of administrative sanctions, which may be triggered by:

- Failure to implement appropriate technical and organisational security measures;
- Omission or delay in the notification of significant incidents (notification required within 24/72 hours);
- Non-compliance with registration and data update obligations with the ACN;
- Lack of cooperation with supervisory authorities;
- Direct liability of management bodies.

Sanction amounts: up to EUR 10M or 2 percent of the worldwide annual turnover for "essential entities" and up to EUR 7M or 1.4 percent for "important entities". Accessory sanctions may also be imposed (e.g., temporary disqualification of managers).

Italian Cybersecurity Perimeter (Perimetro di Sicurezza Nazionale Cibernetica)

Law Decree No. 105/2019 and subsequent implementing decrees establish a national cybersecurity perimeter, imposing strict security and notification obligations on entities deemed critical for national security. The ACN can impose significant fines for non-compliance. The penalties vary depending on the violations and in some cases can reach EUR 1.8M. Repeated violations can result in the penalty being increased up to three times the amount of the penalty.

Sector-Specific Laws and Regulations

Financial Sector (Bank of Italy, Consob, IVASS)

Financial institutions are subject to specific operational resilience and cybersecurity requirements under regulations issued by the Bank of Italy, CONSOB (for securities) and IVASS (for insurance). These include obligations to ensure business continuity, manage ICT risks and report incidents. Breaches can result in administrative sanctions, including fines and in severe cases, suspension of activities.

Critical Infrastructure and Essential Services:

Entities operating in sectors such as energy, transport, health and digital infrastructure may be subject to additional sectoral regulations, often aligned with the NIS2 Directive and the national cybersecurity perimeter.

Saudi Arabia

Data Protection/Privacy Laws and Regulations

Under the PDPL's penalty framework (specifically, Articles 35–40 of the law), violations can result in both criminal and administrative sanctions, but the degree of which depends on the type and seriousness of the breach.

Article 35 specifically criminalises the unlawful disclosure or publication of Sensitive Personal Data in violation of the law, when done with the intention of harming the Data Subject or achieving a personal benefit. Under the PDPL (Article 1[11]), Sensitive Data includes personal data revealing "*racial or ethnic origin, religious, intellectual or political belief, data relating to security criminal convictions and offences, biometric or genetic data for the purpose of identifying the person, health data and data indicating that one or both of the individual's parents are unknown.*" Under Article 35, such conduct would be punishable by up to two years' imprisonment and/or a fine of up to SAR 3M. Note also that in cases of recidivism, the court may double the fine (even beyond the statutory maximum), provided it does not exceed twice that limit.

In addition to Article 35 above, Article 36 governs all other breaches of the PDPL or its IRs (not covered by Article 35). Here, the law provides for administrative penalties — either a warning or a fine of up to SAR 5M — imposed by a specialist committee appointed by the president of the competent authority (i.e., the Saudi Data Artificial Intelligent Authority [**SDAIA**]). Again, the fine may be doubled for repeat violations, up to twice the original maximum. In doing so, the committee considers the nature, seriousness and impact of the violation and its decisions can be appealed before the competent court.

The PDPL also includes additional enforcement tools. For example, under Article 38, the competent court (in criminal cases) or the SDAIA penalty committee (in administrative cases) may confiscate any funds obtained through the violation and order publication of a summary of the judgment or decision, this is at the violator's expense (in local newspapers or via other suitable means) and once the decision becomes final. Article 39 further requires Public Entities to discipline any of their employees who breach the PDPL, in accordance with public-sector disciplinary rules. Finally, Article 40 preserves the right of any individual harmed by a PDPL violation to seek proportionate compensation for material or moral damage through the competent court.

In practice, this creates a two-tiered enforcement regime: Article 35 targets deliberate and harmful misuse of sensitive data with potential imprisonment, while Article 36 captures the broader universe of compliance failures through substantial administrative fines. Both can be accompanied by confiscation orders, public naming and civil claims for damages.

This makes the PDPL a central source of Cyber Fines in KSA, particularly in the context of personal data breaches and mishandling.

Cyber-Specific and Relevant Resilience Laws and Regulations

KSA's Anti-Cyber Crime Law of 2007 (Royal Decree M/17, 1428H), as amended in 2017 (**ACCL**) criminalises a broad range of activities as well, involving unauthorised access, hacking, data manipulation, cyber fraud and offences affecting public order, morality, or national security. The ACCL provides for both criminal fines and imprisonment. The penalties are scaled to the severity and nature of the offence. Moreover, note that "Person" under Article 1 includes explicitly both natural and corporate persons. This means that companies can also be fined if an offence is committed for their benefit (although imprisonment applies only to individuals).

For less serious cyber offences, Article 3 imposes up to one year's imprisonment and/or a fine up to SAR 500,000. Covered acts include spying on, intercepting, or receiving data without authorisation (Art. 3[1]), unauthorised access for threats or blackmail (Art. 3[2]), website hacking to alter design or destroy content (Art. 3[3]), invasion of privacy through misuse of camera-equipped devices (Art. 3[4]) and defamation or causing damage via IT means (Art. 3[5]).

More serious conduct falls under Article 4, which provides for up to three years' imprisonment and/or a fine up to SAR 2M. Examples include acquiring property, bonds, or signatures through fraud or false identity (Art. 4[1]) and illegal access to bank, credit, or securities ownership data with intent to obtain data, funds, or services (Art. 4[2]).

Under Article 5, the penalties increase to up to four years' imprisonment and/or SAR 3M in fines. This applies to unauthorised access aimed at cancelling, deleting, destroying, leaking, damaging, altering, or redistributing private data (Art. 5[1]); causing network or system breakdowns, or destroying or leaking programme/data (Art. 5[2]); and obstructing, distorting, or disrupting services (Art. 5[3]).

Article 6 addresses offences impinging on public order, morals, or privacy, prescribing up to five years' imprisonment and/or SAR 3M in fines. This covers producing, transmitting, or storing such material via networks or computers (Art. 6[1]); creating or publishing sites to promote or facilitate human trafficking (Art. 6[2]); promoting pornography or gambling (Art. 6[3]); and facilitating drug-related activities (Art. 6[4]). Courts may also order publication of the conviction at the offender's expense, reflecting the seriousness of these offences (Art. 6, final paragraph).

The most severe penalties appear in Article 7, which targets cybercrimes linked to terrorism or national security. These carry up to ten years' imprisonment and/or SAR 5M in fines. Examples include creating or publicising websites for terrorist organisations to communicate, finance, or share bomb-making methods (Art. 7[1]) and unauthorised access to obtain data threatening the State's security or national economy (Art. 7[2]).

The ACCL also contains aggravating provisions. Article 8 raises the minimum penalty to half the maximum if the crime involves organised crime, abuse of public office, exploitation of minors, or if the offender has prior convictions for similar crimes.

Liability extends beyond direct perpetrators: Article 9 punishes inciters, assistants and collaborators up to the maximum penalty if the crime occurs, or up to half the maximum if it does not. Article 10 criminalises attempts, with up to half the maximum penalty for the intended offence.

There are also leniency measures. Article 11 allows courts to exempt an offender from punishment if they inform authorities before discovery and before harm occurs. Post-offence reporting can also lead to exemption if it results in the arrest of others or seizure of crime tools.

Importantly, Article 13 authorises confiscation of equipment, software, means, or proceeds used in the crime and allows permanent or temporary closure of websites or venues where the offence occurred, if the owner knew of the activity.

The above criminal penalties are distinct from regulatory fines under frameworks like the PDPL. They serve as the primary statutory basis for criminal Cyber Fines in KSA (particularly in cases of hacking, insider data theft and unauthorised disclosures as discussed above, with the potential for both individuals and companies to face substantial financial and operational consequences).

Sector-Specific Laws and Regulations

Communications and IT

The Communications, Space & Technology Commission (**CST**) regulates telecom and ICT service providers under the Telecommunications and Information Technology Act of 2022 (**TITA**), which replaced the older Telecom Act.

Under the TITA, violations are broadly defined under Article 26 to include: operating without a licence (Art. 26[2]); misuse of telecom/ICT services (Art. 26[5]); causing damage to, illegally using, or interrupting networks (Art. 26[7]); breaching competition rules (Art. 26[6]); impeding inspections (Art. 26[4]); providing misleading information to the public or authorities (Art. 26[3]); owning unlicensed telecom/ICT devices (Art. 26[9]); failing to submit required reports (Art. 26[8]); and any other act that violates the Act, bylaws, or CST's regulatory decisions (Art. 26[10]).

Several of these provisions directly link to cybersecurity because of e.g., failure to safeguard network integrity, unauthorised network interference, or non-compliance with mandated security controls.

Article 27 sets a maximum fine of SAR 25M per violation, along with other possible sanctions, including:

- Full or partial suspension of the service subject to the violation (Art. 27[1][b]);
- Temporary prohibition from obtaining or renewing a telecom/ICT licence (Art. 27[1][c]);
- Full or partial blocking of a digital content platform (Art. 27[1][d]).

The law also empowers CST to require the offender to return any proceeds from the violation (after reimbursing affected users) (Art. 27[3]), to order the violation to be ceased, rectified, or eliminated within a set timeframe (Art. 27[4]) and to proportion penalties to the seriousness, effect and repetition of the offence (Art. 27[5]). The Committee considering violations may also order publication of the operative part of its penalty decision electronically or in print at the offender's expense (Art. 27[6]).

Enforcement is handled by the Committee for the Consideration of Violations (Art. 28), appointed by CST's Board and comprising legally and technically qualified members, with decisions subject to appeal before the administrative court.

In addition to these monetary and administrative sanctions, CST retains broad operational powers under other provisions of TITA. For example, it may cancel or suspend licences for failure to remedy violations (Art. 6(1)(a)), revoke licences for changes in technology or market conditions (Art. 6[2]), or block access to services and devices violating technical standards (Art. 13). Under Article 23, service providers are obligated to protect the confidentiality of user information and report data breaches to CST; non-compliance with these duties could trigger Article 26–27 penalties.

In practice, one can argue that enforcement has been to some extent aggressive. For instance, in January 2021, CITC imposed approximately SAR 40M in combined fines on major telecom operators (including STC, Mobily and Zain) for violations such as sending spam messages, using unlicensed frequencies, breaching SIM card rules and failing to comply with user protection directives — offences that, under the current Act, would fall squarely within Articles 26–27. STC alone was fined about SAR 31M in that action. arabnews.com/node/1793596/business-economy. Unfortunately, given that the KSA has no *stare decisis* and there are no published case files available, the information above has been drawn from news sources covering the matter.

Thus, under TITA, the telecom/ICT sector faces sector-specific cyber related penalties of up to SAR 25M per breach, with potential licence suspensions, service blocks and reputational sanctions. These provisions are directly relevant not only to privacy/data breaches but also to network security failures, unlicensed operations and critical infrastructure incidents in communications.

National Cybersecurity Regulations

KSA's National Cybersecurity Authority (**NCA**) also sets mandatory cybersecurity standards — most notably the Essential Cybersecurity Controls (ECC-1:2018) and Cloud Cybersecurity Controls (CCC-1:2020) — for (i) government entities and their companies and (ii) private-sector organisations that own, operate, or host Critical National Infrastructure (**CNI**).

The Critical Systems Cybersecurity Controls (CSCC-1:2019) extend the ECC for "critical systems," with their own scope and compliance sections. NCA also licenses/registers cybersecurity service, solution and product providers (including managed SOC services).

Historically, NCA frameworks lacked explicit statutory penalties; however, Royal Decree No. M/117 (22 Dec 2024) — Legal Powers of the NCA now grants enforcement authority. Defined violations include: providing cybersecurity activities requiring a licence without one (Clause First[1]); non-compliance with NCA policies/standards/controls (First[2]); withholding/misleading information requested by NCA (First[4]); and obstructing inspectors (First[6]). Detected violations are referred to a specialised committee formed by NCA's Board (Second[2]; Fourth[1]).

The committee may impose warnings, temporary licence suspension, licence revocation, service/activity suspension, or fines up to SAR 25M (Fifth[1][a]–[e]) and may order publication of the decision at the violator's expense (Fifth[2]) and require remedy of the violation and deposit of any unlawfully obtained funds into the State treasury (Fifth[3]). In urgent cases, the NCA Governor (or designee) may suspend or terminate violating activities/systems pending committee action (Third[1]–[2]).

These NCA-imposed measures form a new, cross-sector cyber enforcement regime that complements sector regulators and reaches private companies if they are within CNI scope or offer cybersecurity services in the KSA — hence the importance of heeding ECC/CCC/CSCC and applicable licensing/registration requirements.

Financial Sector (Banking/Insurance)

SAMA imposes also cyber and operational-resilience requirements on banks, insurers and payments/fintech firms. The SAMA Cybersecurity Framework applies to all SAMA-regulated entities and requires immediate notification to SAMA of medium/high incidents, "no-objection" before media interactions and a post-incident report after recovery (Sub-domain 3.3.15, items 5–7). SAMA's Business Continuity Management (**BCM**) Framework likewise mandates that "*all disruptive incidents classified as Medium or High*" be reported immediately to SAMA's supervision function, with a post-incident report and coordination on media communications (Section 2.11[1]–[2]).

SAMA's enforcement toolkit is broad. Under the Banking Control Law, if a bank breaches the law or regulations, SAMA (with required approvals) may, among other measures, suspend or remove directors/officers, limit or suspend business, or ultimately revoke the licence (Article 22). Certain contraventions carry fines and even imprisonment as well (Article 23). For insurers, the Cooperative Insurance Companies Control Law authorises SAMA to impose administrative measures (warnings, corrective programmes, suspensions) and fines via Article 19, with statutory penalties up to SAR 2M and potential publication of final decisions under Article 21. For payments and many fintech business models, the Law of Payments and Payment Services (2021) provides explicit administrative penalties: warning, temporary suspension, licence revocation and fines up to SAR 25M (Article 12), with SAMA empowered to classify violations and impose penalties accordingly.

The *net effect* is that while these specific, public "Cyber Fines" for banks are rarely disclosed as such, the legal framework does empower SAMA to sanction cybersecurity and resilience lapses — ranging from mandatory incident reporting and remediation to heavy administrative measures and significant monetary penalties (especially in the payments/fintech space).

Relatedly, the Capital Market Authority has issued its Cybersecurity Guidelines that apply to licensed capital market institutions. Although only a guideline, theoretically CMA could punish non-compliance under the Capital Market Law, which include penalties ranging from a warning and up to imprisonment.

E-Commerce Sector

Online businesses are governed by the E-Commerce Law (2019) (**ECL**) and its Implementing Regulations (**IRs**) under the Ministry of Commerce (**MoC**). Under the Law, service providers may not retain consumers' personal data or electronic communications beyond what the transaction requires; they must protect such data and keep its privacy; and they may not use/disclose it without consent or legal basis. Art. 5(1)–(2). The IRs require notifying the MoC and affected consumers within 3 days of becoming aware of a personal-data breach.

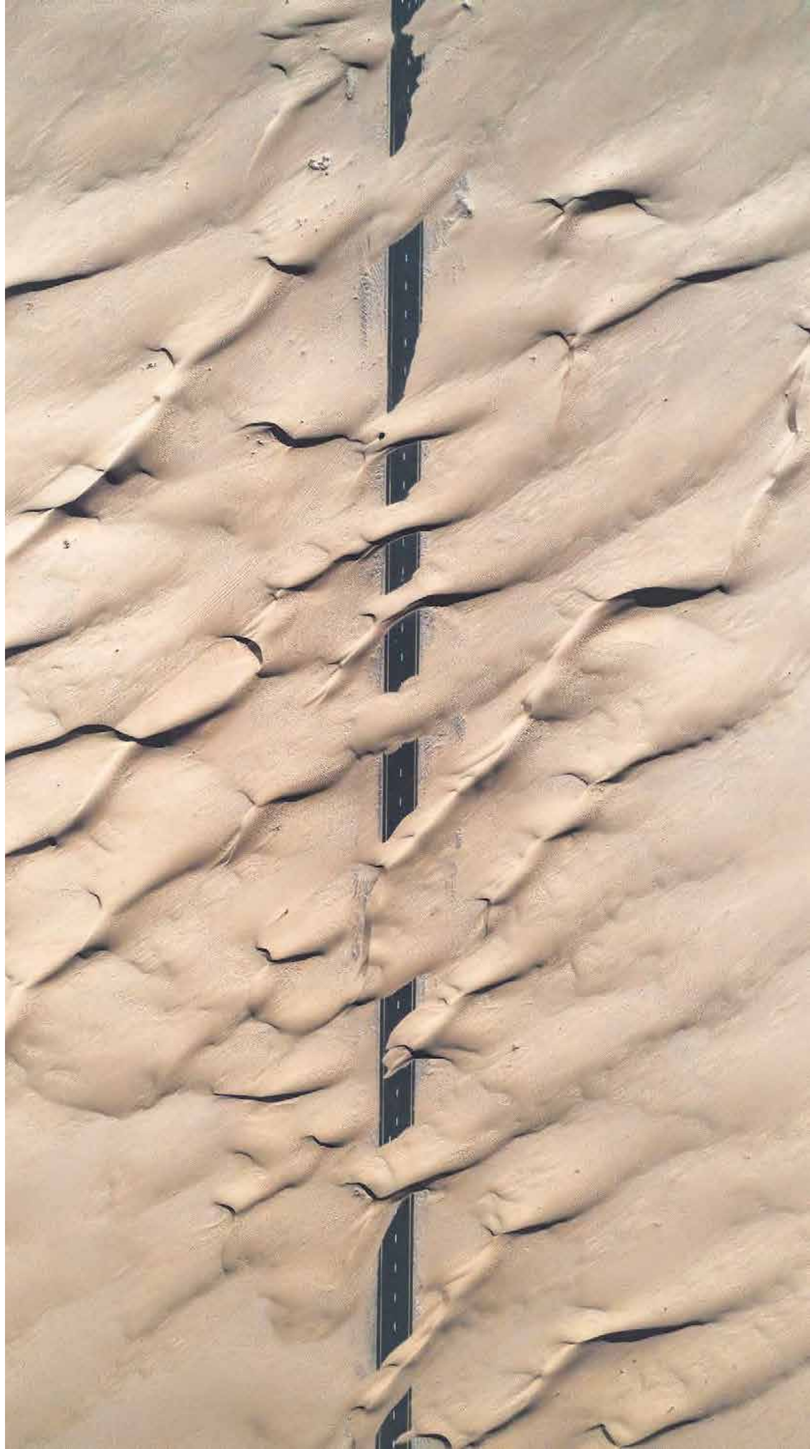
For violations of the ECL/IRs the sanctions are: (a) warning, (b) fine up to SAR 1M, (c) temporary/permanent suspension of e-commerce activity, (d) partial/complete blocking of the e-store (temporary/permanent). Art. 18 of the ECL.

Why this matters for cyber incidents: If a retailer suffers a breach or scam due to non-compliance with these duties, MoC can impose financial penalties (up to SAR 1M) and disruptive measures such as blocking the site — this is on top of any PDPL/NCA exposure discussed above.

Healthcare Sector

Healthcare providers and institutions must protect patient data confidentiality under laws such as the Healthcare Professions Law and ancillary regulations. While these laws (and the Ministry of Health's regulations) don't set very high administrative fines for data breaches, violations can trigger other penalties like professional discipline or facility sanctions. For example, a hospital or clinic that fails to safeguard patient medical records might have its licence to operate suspended or revoked by health authorities, or responsible staff (doctors, administrators) could face disciplinary actions.

The Health Practice Law provides for penalties including warnings, fines (generally and relatively modest amounts) and licence revocation for breaches of patient confidentiality/misuse of health information. In essence, a cyber breach in a hospital could lead to the health regulator stepping in to impose sanctions on the facility or professionals, even if the fines are not as large as in e.g., the PDPL/NCA. But the threat of losing one's medical licence/facility permit is a significant consequence, nonetheless.



Norway

As the Norwegian legal system is dualistic, international legal grounds (e.g., relevant EU-legislation) may only provide basis for Cyber Fines to the extent that they are implemented in Norwegian law.

Below follows a list of the most prominent grounds for Cyber Fines in Norwegian legislation:

The Norwegian Data Protection Act 2018 (Ndpa)

- Incorporates GDPR in Norwegian law (cf. Section 1) — all fines under GDPR apply in Norway.
- Norway-specific regulations of GDPR-fines under the NDPA:
  - Article 83(4) GDPR applies correspondingly to breaches of Articles 10 and 24 GDPR, cf. NDPA Section 26 first paragraph.
  - The Norwegian Data Protection Authority (**DPA**) may impose infringement fines on public authorities and bodies in accordance with the provisions of Article 83 GDPR, cf. Article 83(7) GDPR (cf. NDPA Section 26 second paragraph).

The Norwegian Cyber Security Act 2023 (Please Note That the Act Will Not be in Force Until 1 October 2025)

- Implements EEA NIS1 in Norwegian law and imposes cyber security obligations on undertakings of particular societal significance.
- Max fines of approximately NOK 3.1M or 4 percent of revenue past fiscal year. Currently, there is a proposal to regulate an upper limit for such fines, where it is proposed that the fine may amount to up to 25 times the national insurance basic amount (approx. EUR 275,000) or 4 percent of the total annual turnover in the preceding financial year, whichever amount is higher. However, the fine may not exceed NOK 50M (approx. EUR 4.2M).
- Relevant provisions on infringement fines:
  - The supervisory authority may impose an administrative fine if a provider, or anyone acting on their behalf, intentionally or negligently violates one of the following provisions, cf. Section 17 first paragraph of the Cyber Security Act:
    - Section 7 (security requirements for providers of essential services)
    - Section 8 (notification requirements for providers of essential services)
    - Section 10 (security requirements for providers of digital services)
    - Section 11 (notification requirements for providers of digital services)
    - Section 14 (duty to provide information and access to premises and equipment)

- If the entity liable for the administrative fine is an undertaking that is part of a group of companies, the entity's parent company and the parent company of the group the undertaking belongs to are secondarily liable for the amount, cf. Cyber Security Act Section 17 second paragraph.

The Norwegian Security Act 2018

- Applies to undertakings of importance to national security.
- Infringement fines apply to breaches of provisions that encompass cyber incidents without explicitly referencing them, e.g., data breaches in information systems requiring protection or cryptographic systems intended to safeguard classified information.
- Infringement fines under Section 11-3, which is applicable to intentional or negligent violations of the relevant provisions. Currently, there is a proposal to regulate an upper limit for such fines, where it is proposed that the fine may amount to up to 25 times the national insurance basic amount (approx. EUR 275,000) or 4 percent of the total annual turnover in the preceding financial year, whichever amount is higher.

The Norwegian Electronic Communications Act 2024

- Applies to businesses connected to electronic communication and related equipment, as well as data centre.
- Infringement fines under Section 15-12, including breaches related to e.g., security communications networks and services and notification of security incidents, etc.

The Norwegian Digital Operational Resilience Act 2025 (DORA Act)

- Incorporates Directive (EU) 2022/2554 in Norwegian law.
- Infringement fines up to NOK 50M under Section 4 of the DORA Act, e.g., in case of breaches of the Directive's provisions on response and recovery, management and reporting of ICT-related incidents, etc.

The Norwegian Credit Information Act 2019

The provisions on infringement fines, coercive fines and damages under Articles 82 and 83(5) GDPR and NDPA Sections 26 through 30 apply correspondingly to contraventions of the Act.

Turkey

In principle, we believe that (i) the data protection legislation; (ii) cyber security legislation; and (iii) certain additional sector-specific legislation are relevant in relation to Cyber Fines.

The Law No. 6698 on the Protection of Personal Data (**Data Protection Law**), which governs data protection and privacy, is the main source of Cyber Fines in Türkiye. The following administrative fines are set out under the Data Protection Law (the fine amounts are updated every year — the ranges below reflect the 2025 figures).

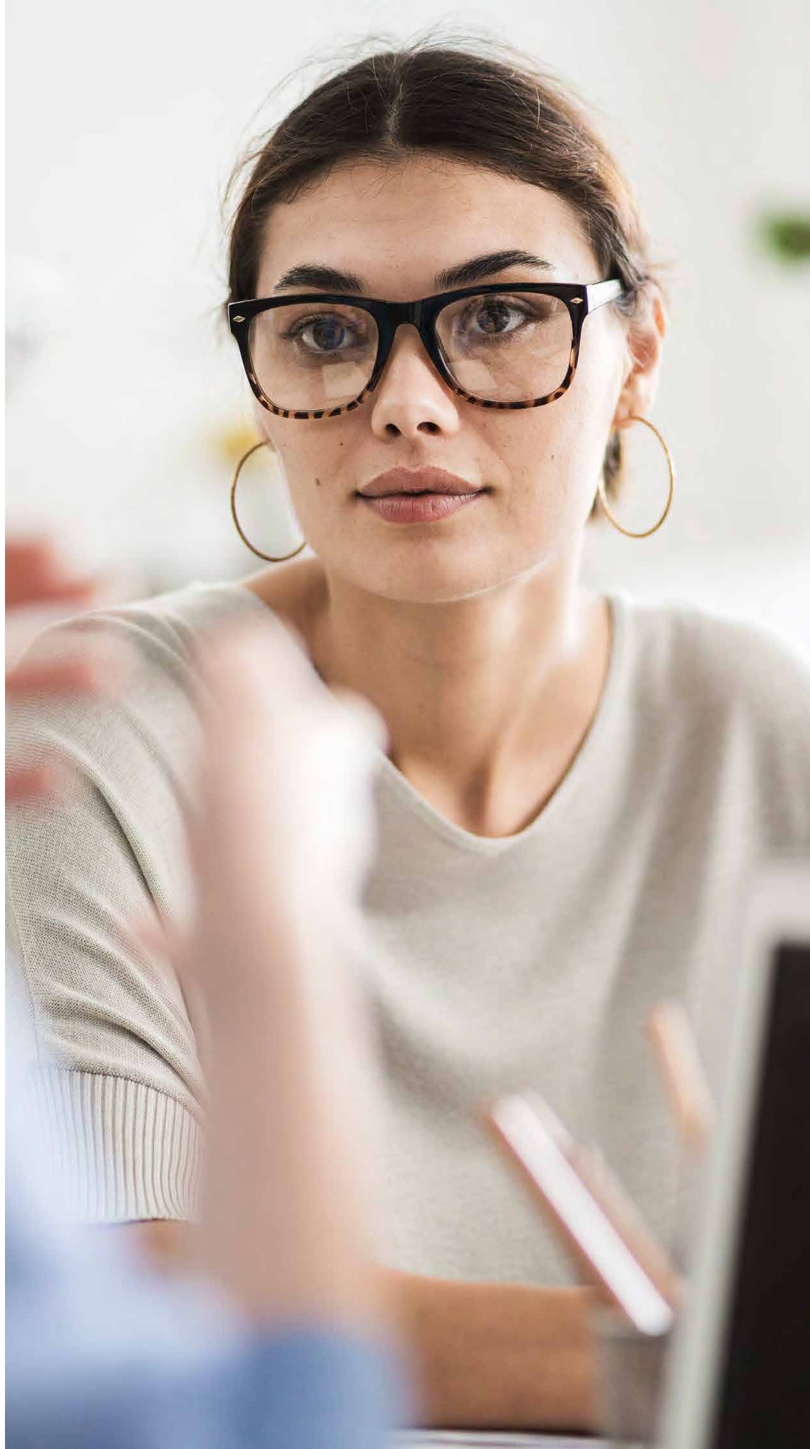
- Failure to comply with the conditions required for **cross-border transfer of personal data** under Article 9 of the Data Protection Law is subject to an administrative fine in the range of TRY 71,965 to TRY 1.4M (approx. USD 1,762 to USD 35,241).
- Failure to comply with the **data controller's obligation to inform the data subject** on data processing as required under Article 10 of the Data Protection Law is subject to an administrative fine in the range of TRY 68,083 to TRY 1.4M (approx. USD 1,667 to USD 33,349).
- Failure to comply with the data controller's obligation to **take all necessary technical and organisation measures or notification obligation in case of data breach** pursuant to Article 12 of the Data Protection Law is subject to an administrative fine in the range of TRY 204,285 to TRY 13.6M (approx. USD 5,001 to USD 333,498).
- Failure to comply with the **procedural obligations regarding Personal Data Protection Board ("Kişisel Verileri Koruma Kurulu") investigations** under Article 15 of the Data Protection Law is subject to an administrative fine in the range of TRY 340,476 to TRY 13.6M (approx. USD 8,366 to USD 333,498).
- Failure to comply with the registry requirement to the Data Controllers' Registry ("VERBIS") under Article 16 of the Data Protection Law is subject to an administrative fine in the range of TRY 272,380 to TRY 13.6M (approx. USD 6,669 to USD 333,498).

Apart from data protection and privacy, cyber specific legislation is very recent in Turkey. In March 2025, the Cybersecurity Law No. 7545 (**Cybersecurity Law**) came into effect. The Cybersecurity Law primarily governs the protection of critical information infrastructure and prevention of cyber incidents in order to protect national cybersecurity. The following administrative fines are set out under the Cybersecurity Law. Please note that since this legislation is very recent, secondary regulations are not established and the enforcement and judicial practice are not clear yet. We believe this is an area that requires monitoring going forward and may be the source of new developments in relation to Cyber Fines.

- **Failure to implement cybersecurity measures or breach of reporting obligations** under Article 7 of the Cybersecurity Law is subject to an administrative fine in the range of TRY 1M to TRY 10M (approx. USD 24,485 to USD 244,851).
- **Failure to take necessary measures to allow inspection** of the relevant equipment, system, software and hardware and keep these in running condition under Article 8 of the Cybersecurity Law is subject to administrative fine in the range of TRY 100,000 to TRY 1M (approx. USD 2,448 to USD 24,485) for real persons and TRY 100,000 (approx. USD 2,448) to up to 5 percent of the gross annual sales revenue for companies.
- **Unauthorised export and control of cybersecurity products** under Article 18 of the Cybersecurity Law is subject to an administrative fine in the range of TRY 10M to TRY 100M (approx. USD 244,851 to USD 2.5M).

Finally, it is possible to come across regulations establishing requirements for the information systems of regulated companies, which also impose administrative fines for non-compliance related to cybersecurity. Please see below examples of such sector-specific regulations.

- **For banks,** the Regulation on Banks' Information Systems and Electronic Banking Services establishes comprehensive requirements for cybersecurity measures, including risk management, information security, system localisation, etc., to ensure continuity of banking operations. Failure to comply with the obligations under this regulation is subject to administrative fines in the range of TRY 377,783 to TRY 3.8M (approx. USD 9,250 to USD 92,502) in accordance with Article 148 of the Banking Law No. 5411 (**Banking Law**).
- **For financial leasing, factoring and financing companies,** the Communiqué on the Management and Auditing of Information Systems of Financial Leasing, Factoring and Financing Companies regulates secure information systems and includes obligations on risk management, access controls, data confidentiality, network security and business continuity. Failure to comply with the obligations under this communiqué is also subject to the same administrative fines under Article 148 of the Banking Law above.
- **For capital markets institutions** (such as stock exchanges, pension funds and public companies) the Communiqué No. VII-128.10 on the Principles and Procedures Regarding Information Systems Management sets out detailed requirements for the secure, sustainable and orderly management of information systems, including obligations on risk management, access controls, data confidentiality, network security and business continuity. Failure to comply with the obligations under this communiqué is subject to administrative fines in the range of TRY 354,761 to TRY 4.4M (approx. USD 8,686 to USD 108,592) in accordance with Article 103 of the Capital Markets Law No. 6362 (**Capital Markets Law**).



Sweden

Data Protection/Privacy Laws and Regulations

According to the EU General Data Protection Regulation, organisations shall implement appropriate technical and organisational measures to ensure the security of personal data, including protection against unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data (Art. 32 GDPR). In the case of a personal data breach, the relevant data protection authority shall be notified within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Art. 33 GDPR). If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, affected data subjects shall also be informed of the breach without undue delay (Art. 34 GDPR). Failure to comply with the security requirements under the GDPR may result in administrative fines up to a maximum of EUR 10M or 2 percent of an undertaking's global annual turnover, whichever is higher.

Cyber-Specific and Relevant Resilience Laws and Regulations

The NIS Directive (Directive [EU] 2016/1148) has been implemented in Swedish law by means of the Act on information security for operators of essential services and digital service providers (2018:1174) (the “NIS Act”). Entities subject to the NIS Act shall take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems they use. The measures shall ensure a level of security of the network and information systems appropriate to the risk. Security incidents shall be reported to the relevant authority. Failure to comply with the NIS Act may result in fines of minimum SEK 5,000 and maximum SEK 10M.

The new NIS2 Directive (Directive [EU] 2022/2555) has not yet been implemented in Sweden. The NIS2 Directive has stricter requirements for operators and aims to achieve a higher level of cybersecurity for the expanded number of sectors that are specified in the NIS2 Directive. Failure to comply with the NIS2 Directive (once implemented in Sweden), may result in fines up to a maximum of EUR 10M or 2 percent of an entity's global annual turnover.

The Cyber Resilience Act (Regulation [EU] 2024/2847) aims to ensure that digital products, including hardware and software, meet minimum cybersecurity requirements. Failure to comply with the Cyber Resilience Act may result in fines up to a maximum of EUR 15M or 2.5 percent of an undertaking's global annual turnover.

Sector-Specific Laws and Regulations

Under the Digital Operational Resilience Act (**DORA**), a harmonised framework has been established for the financial sector, requiring financial entities to maintain sound ICT risk management, report and address major incidents, test digital resilience and manage risks arising from critical third-party ICT providers. The principal regulatory source of fines for cyber incidents derives from the obligation imposed on Member States to establish and enforce penalties for breaches of the regulation. Article 50 requires that Member States lay down the rules on penalties applicable to infringements and ensure that such penalties are “effective, proportionate and dissuasive”.

In Sweden, the Financial Supervisory Authority (*Sw.* Finansinspektionen) (the **SFSA**) is responsible for supervising compliance with DORA and has the authority to impose sanctions in cases of non-compliance. Under the Swedish Supplementary Act (*Sw.* Lag [2024:1278] med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn), the SFSA may issue injunctions, impose administrative fines and in serious cases, caused by intent or gross negligence, prohibit individuals such as board members or CEOs from holding management positions for a period of three to ten years.

Poland

In Poland, financial sanctions for cybersecurity and data-protection failures derive from a layered framework composed of EU regulations that are directly applicable, Polish statutes implementing or complementing those regulations and sector-specific rules enforced by specialised regulators.

Data Protection/Privacy Laws and Regulations

The Regulation (EU) 2016/679 — General Data Protection Regulation, directly binding in Poland since 25 May 2018, remains the single most important source of Cyber Fines. Administrative monetary penalties are imposed by the President of the Personal Data Protection Office (**UODO**) under Articles 83 and 84 GDPR, read together with Chapter 10 of the Polish Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2018, item 1000, as further amended). The GDPR fine ceilings — up to EUR 10M/2 percent of worldwide annual turnover for undertakings or EUR 20M/4 percent of turnover for undertakings, depending on the infringement — apply in full.[33]

The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) is transposed mainly by the Electronic Communication Law of 12 July 2024 (Journal of Laws 2024, item 1221; **ECL**) and the Act on the Provision of Services by Electronic Means of 18 July 2002 (consolidated text: Journal of Laws 2024, item 1513). Those statutes empower the President of the Office of Electronic Communications (**UKE**) to levy penalties of up to 3 percent of the prior year's revenues for violations of confidentiality of communications.[34] The subjective scope of the application of financial penalties is determined by the subjective scope of the obligation to maintain confidentiality. This obligation applies not only to electronic communications service providers but also to entities cooperating in the provision of electronic communications services. Moreover, the electronic communications service provider is liable for breaches of confidentiality committed by entities acting on its behalf. The scope of telecommunications secrecy also includes data about users, although personal data is currently protected separately.

Moreover, under Article 401 of the ECL, an electronic communications service provider is required to implement appropriate technical and organisational protection measures to ensure the security of personal data processing. Regardless of the requirements indicated in the GDPR, the protection measures must ensure at least: (i) that access to personal data is granted only to a person who has been authorised by the data controller; (ii) the protection of stored or transmitted personal data against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage, processing, access, or disclosure; (iii) the implementation of a security policy with respect to the processing of personal data. The electronic communications service provider is also obliged under the ECL to notify the UODO of a data protection breach within 24 hours of its detection and to maintain a register of such breaches.

Failure to comply with these obligations, as well as failure to report a data protection breach, may result in the UODO imposing a fine of up to 3 percent of the penalised entity's revenue earned in the previous calendar year.[35]

Cyber-Specific and Relevant Resilience Laws and Regulations

Cyber specific regulation is currently anchored in the Act of 5 July 2018 on the National Cybersecurity System (consolidated text: Journal of Laws 2024, item 1077; **NCSA**), which transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "first NIS Directive") into Polish law.

33. Art. 86 of the GDPR.
34. Art. 444, 446 of the ECL.
35. Art. 401-404 of the ECL.

A key service operator[36] is subject to fines ranging from PLN 15,000 to PLN 200,000 for violations of their obligations, including, among others, failure to conduct systematic risk assessments or failure to manage the risk of incidents, failure to implement appropriate and proportionate technical and organisational measures in line with the assessed risk and the latest state of knowledge (including failure to continuously monitor systems), failure to report incidents within the statutory deadline (24 hours), or failure to eliminate vulnerabilities in IT systems.[37]

A digital service provider[38] who fails to report a serious incident to the appropriate authorities or does not eliminate vulnerabilities that have led or may lead to a security incident is subject to an administrative fine ranging from PLN 1,000 to PLN 15,000.[39]

Importantly, these fines may also be imposed even if the entity has ceased the violation or remedied the damage caused, if the competent cybersecurity authority determines that the duration, scope, or consequences of the violation justify such a penalty.

If, as a result of an inspection, the competent cybersecurity authority finds that a key service operator or digital service provider persistently violates the provisions of the NCSA, causing: (i) a direct and serious threat to cybersecurity for national defence, state security, public safety and order, or the life and health of people, (ii) a risk of causing serious material damage or significant disruptions in the provision of key services, — the competent cybersecurity authority will impose a fine of up to PLN 1M.[40]

Despite the deadline for implementing the provisions of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (**NIS2 Directive**) having passed, this directive has still not been fully transposed in Poland. Currently, the sixth version of the draft act amending the national cybersecurity system, aimed at transposing the directive into Polish law, is being processed. This draft has still not reached the stage of parliamentary work and is at the stage of inter-ministerial consultations. In practice, the earliest possible date for the national regulations to come into force is at the turn of the third and fourth quarters of 2025.

Once enacted, they will raise potential fines to the higher of EUR 10M or 2 percent (essential entities) / EUR 7M or 1.4 percent (important entities) of annual turnover and will introduce personal liability of management board members for wilful misconduct or gross negligence.

Finally, the Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act, **CRA**), once fully applicable from 11 December 2027, will supplement the above national regulations by imposing security-by-design and vulnerability-management obligations on online platforms and manufacturers of connected products, enforceable through fines of up to 2.5 percent of undertaking's total worldwide annual turnover for the preceding financial year.

36. An operator of an essential service is an entity, which has an organisational unit within the territory of Poland, and in relation to which the competent authority for cybersecurity has issued a decision recognising it as an operator of an essential service. The sectors, subsectors, and types of entities are specified in Annex No. 1 to the NCSA, and include among other energy, transport, financial services, health-related services, digital infrastructure and water supply services sectors.
37. Art. 73 of the NCSA.
38. A provider of a digital service is a legal person or an organisational unit without legal personality that has its registered office or management within the territory of Poland, or a representative with an organisational unit within the territory of Poland, providing a digital service (ie, e-commerce platform, cloud computing services or search engines), with the exception of micro-enterprises and small enterprises.
39. Art. 73 of the NCSA.
40. Art. 73.5 of the NCSA.

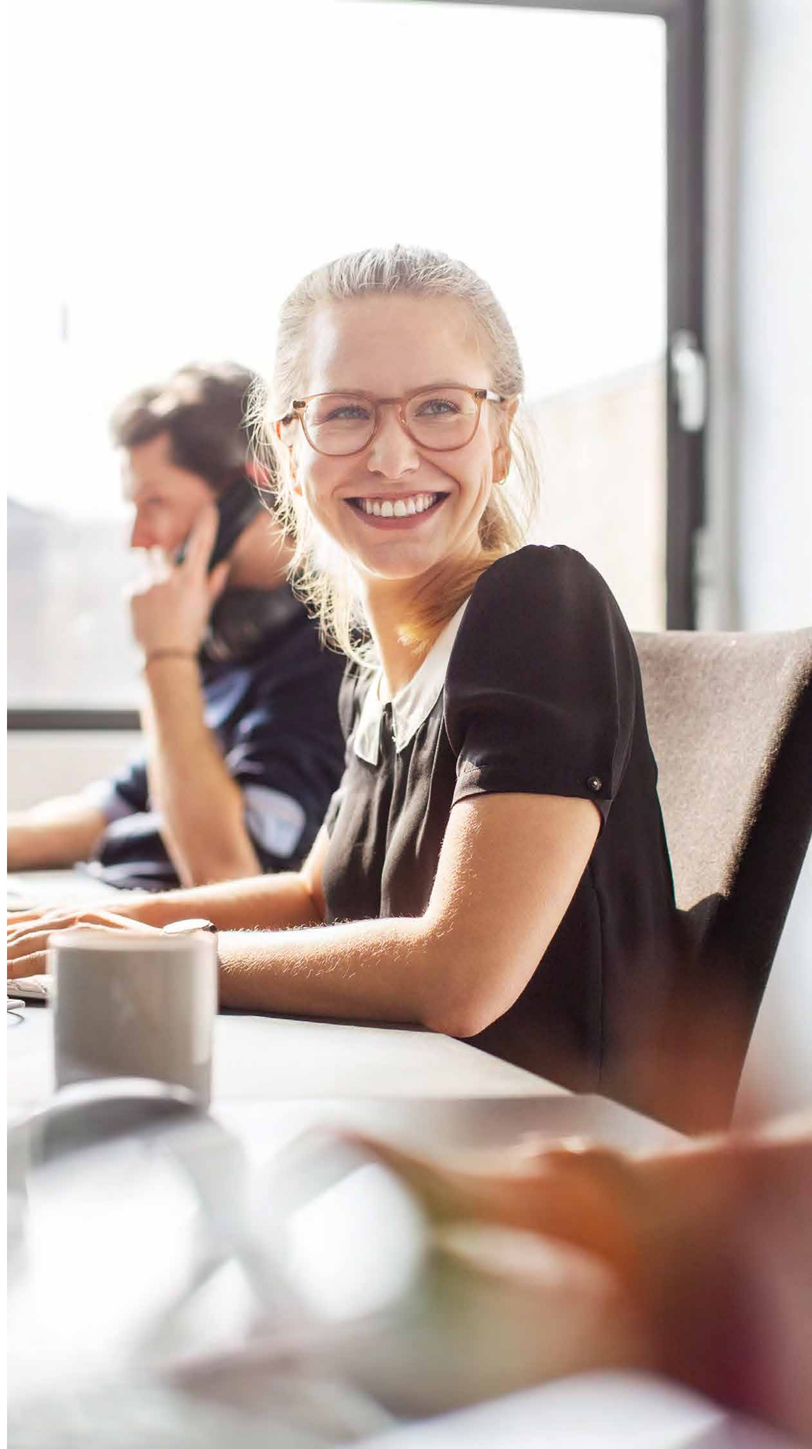
Sector-Specific Laws and Regulations

Sector-Specific Regulations Create Additional Exposure

As of 17 January 2025, 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 (**DORA Regulation**) is applied in Poland. Its aim is to increase the digital operational resilience of financial entities and to regulate the provision of ICT services in the financial market.

Any breach of cyber resilience-related obligations under the DORA Regulation may trigger the sanctions specified in the Polish Act of 21 July 2006 on Financial Market Supervision (consolidated text: Journal of Laws 2025, item 640; **FMSA**). Under the FMSA, the Polish Financial Supervision Authority (**KNF**) can impose a financial penalty up to the following amounts:

- In the case of a legal person or an organisational unit without legal personality: (i) an amount of PLN 20.9M or 10 percent of the total annual revenue and in the case of an insurance undertaking or a reinsurance undertaking — 10 percent of the gross written premium, as shown in the most recent financial statement for the financial year approved by the approving authority; or (ii) twice the amount of the benefits gained or losses avoided as a result of the violation, if it is possible to determine such amounts.
- In the case of a natural person responsible for the violation who, during this period, performed the duties of a member of the management board or another managing body of the financial entity — an amount of PLN 3M.
- In the case of another natural person responsible for the violation — six times the amount of the remuneration received by the penalise person, calculated according to the rules applicable for determining the cash equivalent for unused annual leave.



England and Wales

Regulatory fines for cyber incidents in England and Wales largely stem from a few key regimes and regulators. The most significant sources of exposure include data protection and e-privacy, network and information systems obligations, financial services regulation and telecoms security.

The Information Commissioner's Office (ICO) is the primary enforcer where personal data is involved. Under UK GDPR and the Data Protection Act 2018, fines on organisations which process personal data can reach up to the greater of GBP 17.5M or 4 percent of the undertaking's global annual turnover for serious failures. Providers of public electronic communications networks and services are subject to a separate regime which is also supervised by the ICO, the Privacy and Electronic Communications Regulations 2002 (PECR) which — like the UK GDPR — imposes specific obligations to ensure the security of services. Until mid-2025, monetary penalties under PECR were capped at GBP 500,000. However, the Data (Use and Access) Act 2025 has now brought maximum penalties for PECR infringements into line with the UK GDPR.

Beyond data protection, the Network and Information Systems (NIS) Regulations 2018 impose cybersecurity and incident reporting obligations on operators of essential services — such as energy, transport, water, health and certain digital infrastructure — as well as on relevant digital service providers, including online marketplaces, search engines and cloud services. Competent authorities (and the ICO for digital providers) can levy fines of up to GBP 17M for non-compliance.

The NIS Regulations are set to be replaced by the Cyber Security and Resilience Act, which is currently progressing through Parliament as a Bill. The new Act will extend coverage to a broader range of sectors and organisations and, under the current draft, enforcement will sit with various regulators who will have authority to impose fines in some situations of up to the greater of GBP 17M and 4 percent of the undertaking's global annual turnover.

Ireland

Data Protection/Privacy Laws and Regulations

GDPR

As you know, the GDPR is an EU regulation which sets out the rules to protect natural persons regarding the processing of their personal data. Under the GDPR, personal data must be processed lawfully, fairly and in a transparent manner. It must be collected for a specific purpose and the collected data must be limited to what is necessary. It should be kept up to date and accurate, with a limitation period on its storage. It should be processed in a way that ensures appropriate security.

The GDPR sets out these obligations on data controllers, who determine the purposes and method of processing personal data and data processors, who process personal data. Any entities operating within or from Ireland who process or control the method of processing data must comply with the GDPR obligations as any breach of these obligations may result in fines or other remedial measures. The GDPR also has provisions with extra-territorial effect.

Article 83 of the GDPR sets out the administrative fines that may be imposed by a Member State's national supervisory authority with penalty amounts up to EUR 10M or 2 percent of total worldwide annual turnover of the preceding financial year, whichever is higher.

For more serious violations, fines may be imposed of up to EUR 20M or 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The Irish Data Protection Commission (**DPC**), which is the supervisory authority for the GDPR in Ireland, has imposed fines for breaches of the GDPR such as the most recent fine against Meta for EUR 251M stemming from a personal data breach. This breach is discussed in further detail below.

Data Protection Act 2018 (DPA 2018)

The DPA 2018 was enacted to establish the DPC and to give effect to certain provisions of the GDPR which are to be implemented at a national level. The DPC is the national independent supervisory authority in Ireland. The DPC is responsible for the protection of individuals' fundamental right to have their personal data protected and it may impose the administrative fines set out under the GDPR for any infringement of those rights.

Data Protection Act 1988 and 2003

The Data Protection Acts of 1988 and 2003 are national legislation on data protection that have generally been replaced by the GDPR and the DPA 2018. However, in circumstances where the GDPR does not apply, such as where the data protection complaint or potential data infringement occurred before the GDPR's applicable date of 25 May 2018, then the provisions of the 1988 and 2003 Acts may apply instead.

Under the 1988 and 2003 Acts, a data controller or processor guilty of an offence under the Act shall be liable on summary conviction of a fine not exceeding EUR 3,000 or on conviction on indictment to a fine not exceeding EUR 10,000.

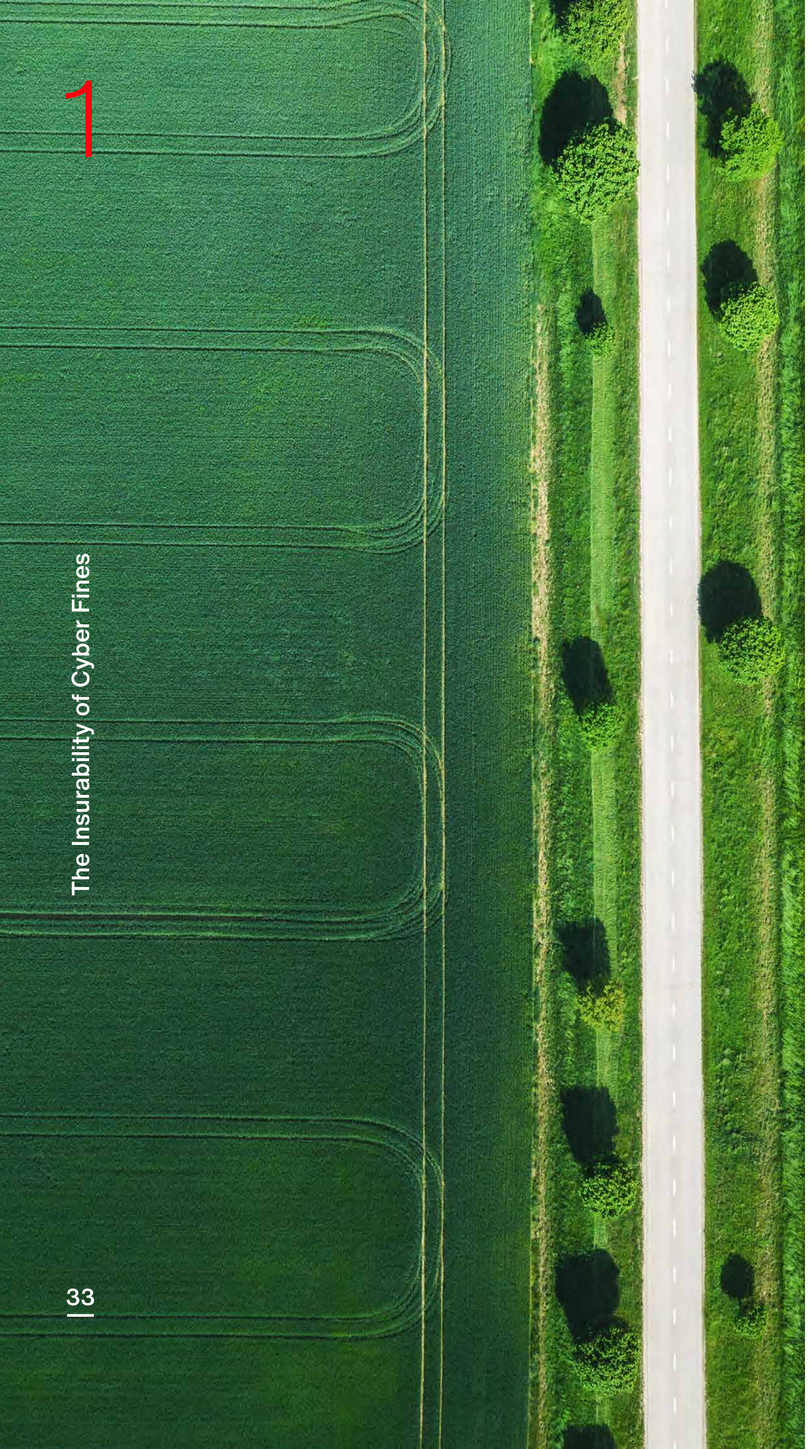
Eprivacy Regulations 2011

The ePrivacy Regulations transpose the European ePrivacy Directive 2002/58/EC as amended by 2009/126/EC into Irish law. It protects the confidentiality of electronic communications and regulates electronic direct marketing. Fines can be imposed for breaches of these regulations; in the case of a natural person, up to EUR 50,000 and, in the case of a body corporate, up to EUR 250,000.

Cyber-Specific and Relevant Resilience Laws and Regulations

Network and Information Security Directive EU 2022/2555 (NIS2)

NIS2 is the most recent directive introduced by the European Union to address the cybersecurity of essential and important entities in certain sectors across EU Member States. NIS2 is set to be transposed in Ireland under the National Cyber Security Bill, which has yet to be enacted and which will establish the National Cyber Security Centre as the Irish national authority.



NIS2 applies to certain entities in critical sectors such as energy, banking, transport and health. It introduces risk management and incident reporting requirements on these entities. NIS2 categorises any in-scope entities as either essential or important entities depending on several factors including the sector in which they operate or how critical the services they provide are.

In-scope entities are obligated under NIS2 to comply with certain requirements including taking appropriate measures to manage any risks posed by their supply chains, systems security and incident handling. If any cyber incident occurs, then this may indicate that the in-scope entity has not taken adequate measures to secure their systems or supply chains in line with these obligations.

This directive also provides enforcement powers to national authorities to impose both remedial measures and administrative fines for any non-compliance with NIS2. The possible fines under NIS2 depend on whether the entity being fined is deemed essential or important. For essential entities a maximum fine of at least EUR 10M or up to 2 percent of the total worldwide annual turnover from the preceding financial year, whichever is higher, may apply for any non-compliance. For entities considered important under the directive, a maximum fine of at least EUR 7M or 1.4 percent of the total worldwide annual turnover from the preceding financial year may be imposed for any non-compliance.

Digital Operational Resilience Act (DORA)

DORA includes a regulation and a directive on digital operational resilience for the financial sector. DORA came into force in January 2022 and took effect on 17 January 2025.

DORA establishes a common set of rules and standards for financial institutions in managing, testing, reporting and mitigating digital operational or ICT risk, as well as monitoring the use of third-party service providers with the aim of enhancing the cyber resilience of these financial institutions. Financial institutions who operate within Ireland must ensure that the service providers who they contract with comply with their DORA obligations by amending any existing contractual agreements to include certain provisions such as audit or subcontracting provisions.

A cyber incident may be a breach under DORA as it may indicate that the ICT systems in use are not sufficiently secure or that they have not been sufficiently tested. Additionally, subsequent to a cyber breach, a financial entity who fails to report where required to do so may be in a breach of their DORA obligations.

DORA provides to the European Supervisory Authorities the power to impose administrative fines on any legal or natural persons found to be in violation of the requirements under DORA. In Ireland the national authority with the power to regulate and investigate DORA entities is the Central Bank of Ireland (**CBI**). DORA requires that a Member State lay down rules

establishing the administrative fines that a financial institution or person can face for non-compliance. In Ireland the Central Bank Act 1942 was amended to enable the CBI to apply its existing administrative fines regime to any financial institution who has failed to comply with any DORA requirements. This means that the CBI may impose a fine for breaches of DORA of up to EUR 10M or 10 percent of the financial institution's annual turnover for the preceding financial year.

Additionally, DORA extends personal liability to the members of the board of directors of financial entities. The CBI has the power to impose administrative sanctions on members of the financial institution's management body. These sanctions include fines of up to EUR 1M.

EU (Resilience of Critical Entities) Regulations 2024

These regulations transposed the EU Directive 2022/2557 (Critical Entities Resilience Directive) and relate to the resilience of essential services. The regulations came into effect on 17 October 2024. They apply to the sectors of energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space and large-scale food production, processing and distribution. Competent authorities are designated for each of the 11 sectors. Offences under the regulations may incur fines of up to EUR 500,000 in the case of a person other than an individual.

Cyber Resilience Act

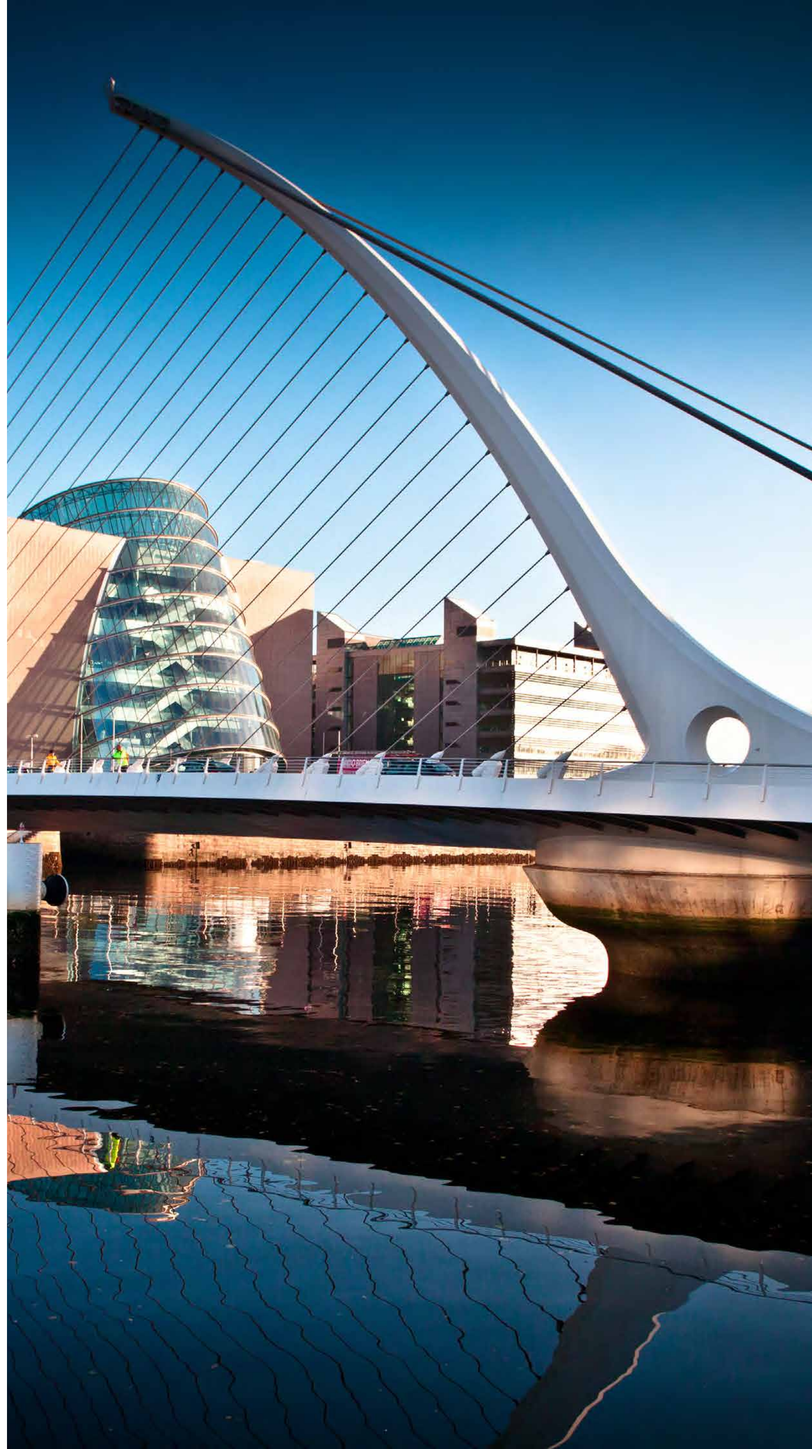
The Cyber Resilience Act (**CRA**) came into force on 10 December 2024 and it aims to enhance cybersecurity standards of products that have a digital component. Member States have been provided a three-year grace period to put compliant products on the EU market and the Act will commence in full from 11 December 2027. However, certain provisions come into effect sooner than this. Under the CRA, the European Commission, the European Union Agency for Cybersecurity (ENISA) and national market surveillance authorities have enforcement powers, however the CRA gives Member States a degree of discretion regarding the method for imposing fines, although it does set the maximum levels to be imposed. Failure to comply with essential cybersecurity requirements, conformity assessments and reporting obligations may incur a maximum fine of up to EUR 15M or 2.5 percent of annual global turnover, whichever is higher.

Regulation (EU) 2024/1689 (the AI Act)

This regulation lays down harmonised rules on artificial intelligence (**AI**). This is discussed in more detail below.

UAE

The principal sources of Cyber Fines in the UAE depend on the entity's location (onshore or in a financial free zone) and the relevant regulator. This is because the UAE has a multi-layered regulatory



framework, with distinct legal regimes for onshore UAE and the financial freezones: (a) Dubai International Financial Centre (**DIFC**); and (b) the Abu Dhabi Global Market (**ADGM**). Each regime imposes its own requirements and potential penalties for cyber incidents, which we have outlined below.

Onshore UAE

UAE Central Bank (CBUAE)

Under the CBUAE's purview, there are two pieces of legislation under which cyber incidents/breaches are relevant. These include the Federal Law No 14 of 2018 regarding the Central Bank and Organisation of Financial Institutions and Activities (as amended) (the **Banking Law**) and the Consumer Protection Regulations (C 8/2020) (**CPRs**).

The Banking Law requires the "immediate reporting" of the occurrence of any material or crucial developments which may impact a CBUAE licensed financial entity's (**LFI**) activities, structure, or overall position. The Banking Law does not include any de minimus limits for which a report must be made, so a strict technical interpretation of the requirements suggests that any breach (however small) would trigger a notification requirement to the CBUAE. In practice, this means an LFI, and as outlined in the Banking Law, its legal representatives, compliance officers and auditors (collectively, the **Relevant Persons**) would need to report to the CBUAE regarding any breach of the confidentiality provisions of the Banking Law, including any cybersecurity breaches. The Relevant Persons will not be considered to have "breached any of the obligations imposed thereon" in case of "filing a report as per provisions of this article or providing information or opinion to the Central Bank if they are acting in good faith". Please note that the interpretation of this exception remains unclear and we have not identified any commentary on its interpretation. However, if the LFI is found to have breached the Banking Law, the CBUAE may impose a fine of up to AED 200M in addition to applying other sanctions/restrictions.

The LFI must also not dismiss any of the Relevant Persons' obligations without approval from the CBUAE.

Under the CPRs, the LFI is required to notify the CBUAE of "all significant breaches" of consumer data and information. The notifications must be made "without undue delay". Violating the CPRs may result in sanctions and penalties deemed appropriate by the CBUAE, but the specific amount has not been outlined with the CPRs.

UAE Data Office

The UAE personal data protection law, Federal Decree Law No 45 of 2021 Regarding the Protection of Personal Data (the **PDPL**), is not currently in force. The effective period for the PDPL will commence six months after the Executive Regulations are implemented. While the PDPL contains obligations on data controllers regarding the security of personal data, further detail on the liability of entities for breaches of data protection is expected to be provided within the Executive Regulations.

Other Sectors

If a cyber incident occurs which impacts a patient's medical or other personal data, under Federal Law No 2 of 2019 Concerning the Use of Information and Communications Technology in Health Fields (the **ICT Healthcare Law**), the relevant federal or local government health authority may issue a fine of up to AED 1M, depending on the severity of the incident. Healthcare authorities such as the Dubai Health Authority (**DHA**) or Abu Dhabi Department of Health (**DoH**) may also have specific obligations under respective policies, standards and guidelines issued from time to time, which may include notification obligations to the DHA and DoH and data subjects in certain circumstances.

Financial Free Zones

DIFC

Under the DIFC General Rules (**Gen Rules**), a licensed entity in the DIFC must notify the Dubai Financial Services Authority (**DFSA**) of any material cyber incidents and make a submission using the appropriate form available on the DFSA electronic portal. A cyber incident is defined in the Gen Rules as an "incident arising from the malicious use of information or communication technology" that "adversely affects" a DIFC licensed entity's use of ICT assets. The DIFC licensed entity must notify the DFSA as soon as reasonably practicable, and in any event, no later than 72 hours after it becomes aware, or has information which reasonably suggests a material cyber incident has occurred. The Gen Rules do not set out the fine relating to a breach of this notification requirement. However, under the Regulatory Law DIFC Law No 1 of 2004, if the DFSA considers that a person has contravened any legislation administered by the DFSA, the DFSA may exercise one or more powers including fining a licensed entity the amount it considers appropriate in respect of the relevant contravention.

To the extent that cyber incidents affect personal data relating to data subjects governed by the DIFC Data Protection Law 2020 (the **DIFC DPL**), additional regulatory fines may apply. Under the DIFC DPL, there are requirements to notify the DIFC Commissioner of any personal data breaches. Failure to report a cyber incident that also affects personal data may result in a fine of USD 50,000. In addition, the DIFC Commissioner may issue a general fine of an unlimited amount against data controllers and processors after taking into account the seriousness of the contravention and risk of actual harm to data subjects.

ADGM

Within the ADGM, there is no specific provisions dealing with cyber incidents. However, under the ADGM Data Protection Regulations 2021 (as amended) (**DPRs**), to the extent a cyber incident affects personal data, and would be deemed a personal data breach i.e., a "breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data", the ADGM entity must, without undue delay, and no later than 72 hours after having become aware of the incident, notify the Office of Data Protection, unless the breach is unlikely to result in a risk to the rights of natural persons. The ADGM DPRs do not specifically state the regulatory fines for cyber incidents/personal data breaches of this nature. However, the Office of Data Protection has the statutory authority, where there has been a breach of the DPRs or a direction issued by the Office of Dara Protection, to issue a fine not exceeding USD 28M.

Germany

Data Protection/Privacy Laws and Regulations

GDPR

The GDPR provides for regulatory fines (Article 83 GDPR).

Cyber incidents may give rise to GDPR fines in three scenarios:

- GDPR violations that contributed to or caused the incident, e.g., excessive storage of data in violation of the principle of data minimisation (Article 5[1][c] GDPR), breach of data security rules (Articles 5[1][f], 32 GDPR) or no / insufficient employee training and policies (Article 24 GDPR). Under Section 42 German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)
- Breach of post-incident notification obligations under Articles 33, 34 GDPR.
- Breach of information requests from DPAs (Article 58[1] GDPR) or mitigation measures ordered by DPAs (Article 58[2] GDPR).
- GDPR violations did not contribute to a cyber incident but are discovered by authorities while investigating the incident. Not common, German DPAs typically stick to investigating the root cause of the incident and the mitigation measures taken.

These violations of the GDPR are subject to effective, proportionate and dissuasive regulatory fines (Article 83[1] GDPR):

- Violations of the principles of data minimisation, integrity and confidentiality are punishable by a fine of up to EUR 20M or up to 4 percent of global annual turnover, whichever is higher (Art. 83[5][a] GDPR).
- Violations of the notification obligations are subject to fines of up to EUR 10M or up to 2 percent of global annual turnover, whichever is higher (Art. 83[4][a] GDPR).
- Insufficient technical and organisational measures are not subject to fines individually, but will increase the amount of all other fines, whichever is higher (Art. 83[2][2][d] GDPR).
- Non-compliance with information requests is punishable with fines of up to EUR 20M or up to 4 percent of global annual turnover, whichever is higher (Art. 83[5][e] GDPR).

If the Data Protection Authority ordered the implementation of specific measures pursuant to Art. 58(2) GDPR, non-compliance is punishable with fines of up to EUR 20M or up to 4 percent of global annual turnover, whichever is higher (Art. 83[6] GDPR).

BSIG

The BSIG (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, Act on the Federal Office for Information Security) provides for fines for operators of critical infrastructure.

Critical infrastructure are designated facilities in critical sectors (e.g., energy, IT and telecommunications, transport and traffic, finance and insurance) which are of great importance to the functioning of the community (Sec. 2[10] BSIG).

Operators of critical infrastructure must:

- Implement sufficient IT security measures (Sec. 8a BSIG).
- Notify the BSI about cyber incidents (Sec. 8b[4], 8c[7], [8] BSIG).
- Cooperate with the BSI to resolve incidents (Sec. 8b[6] BSIG).
- Minimise repercussions of cyber incidents (Sec. 8c BSIG).
- Comply with the EU Cybersecurity Act (Regulation [EU] 2019/881)

The BSI may impose regulatory fines for violations of these duties:

- Insufficient IT security measures are subject to fines of up to EUR 1M (Sec. 14[5][1], [2][1][2] BSIG).
- Failure to cooperate in resolving incidents is subject to fines of up to EUR 2M (Sec. 14[5][1][1], [2][1][c] BSIG).
- Failure to comply with the EU Cybersecurity Act is subject to fines of up to EUR 500,000 (Sec. 14[5][2] BSIG).

Sector-Specific Laws and Regulations

Providers of telecommunication services (including telephone, internet, messengers) are subject to the TKG (*Telekommunikationsgesetz*, Telecommunications Act). The *Bundesnetzagentur* (Federal Network Agency) may impose fines for, i.a., violations of notification duties (Sec. 168, 169 TKG) of up to EUR 100,000 (Sec. 228[1][40], [7][4] TKG).

The KWG (*Kreditwesengesetz*, German Banking Act) contains special cyber security requirements for the banking sector (Sec. 25a, 56[2][3] KWG), further specified in the BaFin (*Bundesanstalt für Finanzdienstleistungsausicht*, Federal Financial Supervisory Authority) guidance MARisk (*Mindestanforderungen zum Risikomanagement*, Minimum Requirements for Risk Management). Non-compliance with BaFin orders is subject to administrative fines of up to EUR 5M (Sec. 56[2][3][f], [6][1], 25a[2][2] KWG).

The BaFin competencies will be extended significantly during the implementation of the NIS2 Directive (EU) 2022/25555, scheduled for late 2025. Of particular importance are administrative fines for lack of risk management measures (Sec. 30 BSIG-new) and more specific notification duties (Sec. 32 BSIG-new) with increased fines of up to EUR10M (Sec. 65(5)(1)(a) BSIG-new).

Spain

Data Protection/Privacy Laws and Regulations (e.g., the Data Protection Act 2018, UK GDPR and the Implementing Legislation Under the Eprivacy Directive [PECR] in E&W)

The overarching source of monetary exposure following a cyber incident is primarily linked to both the EU General Data Protection Regulation (**GDPR**) and Spain's Organic Law 3/2018 on Data Protection and Digital Rights (**LOPDGDD**). The Spanish Data Protection Agency (**AEPD**) can impose administrative fines at the GDPR's higher tier, up to the greater of EUR 20M or 4 percent of worldwide annual turnover for core infringements and at the lower tier for other obligations, together with corrective orders including orders to comply, warnings and processing bans.

Spanish procedural and classification rules under the LOPDGDD complement those EU ceilings and provide for publication of sanctions above certain thresholds. In practice, sanctions following cyber incidents which qualify as personal data breaches frequently rest on the principle of confidentiality under Article 5(1)(f) GDPR and on Article 32 (*security of processing*), coupled in some cases with Articles 25 (*data protection by design and by default*), 33 (*notification to the supervisory authority*) and 34 (*communication to the data subject*) when processing design defaults and notification shortcomings are identified.

Information society services regulation under the ePrivacy Directive and Spanish Law 34/2002, of July 11, on Information Society Services and Electronic Commerce (**LSSI**) is a second vector of administrative exposure that often arises either alongside or following incident investigations. The LSSI provides for monetary sanctions up to EUR 600,000 for very serious infringements and lower caps for serious and minor infringements, accompanied by publication and, for repeated very serious infringements a temporary prohibition to operate may also be imposed. Daily coercive fines to compel compliance with provisional measures are also contemplated.

Cyber-Specific and Relevant Resilience Laws and Regulations (e.g., NIS, PSTIA and Possibly, in the Near Futuree the Cybersecurity and Resilience Bill in E&W)

Spain's current cybersecurity-supervision baseline is the NIS1 framework established by Royal Decree-law 12/2018 and further developed by Royal Decree 43/2021, which applies to operators of essential services and to certain digital service providers. It imposes measures and incident-notification obligations and includes a sanctions scale that reaches up to EUR 1M for very serious infringements, with publication in specified cases. Infringements include failure to notify incidents, failure to adopt required security measures, obstruction of audits and provision of false information. Under this framework incidents shall be notified to the relevant CSIRT through the online process centralised under the National Platform for Notification and Monitoring of Cyber Incidents.

Spain has not yet completed transposition of the NIS2 Directive. The Council of Ministers approved a Draft Law on Coordination and Governance of Cybersecurity in January 2025 to transpose NIS2, but until entry into force of the new law the NIS1-based regime remains applicable. Upon its successful transposition, NIS2 will expand scope and raise ceilings, with essential entities facing fines up to the higher of EUR 10M or 2 percent of worldwide turnover and important entities up to the higher of EUR 7M or 1.4 percent, together with broadened supervisory tools, binding instructions, public disclosures and management accountability measures.

Sector-Specific Laws and Regulations (e.g., Operational Resilience Rules and Critical Third Parties Regime Which Applies to the Financial Sector in E&W)

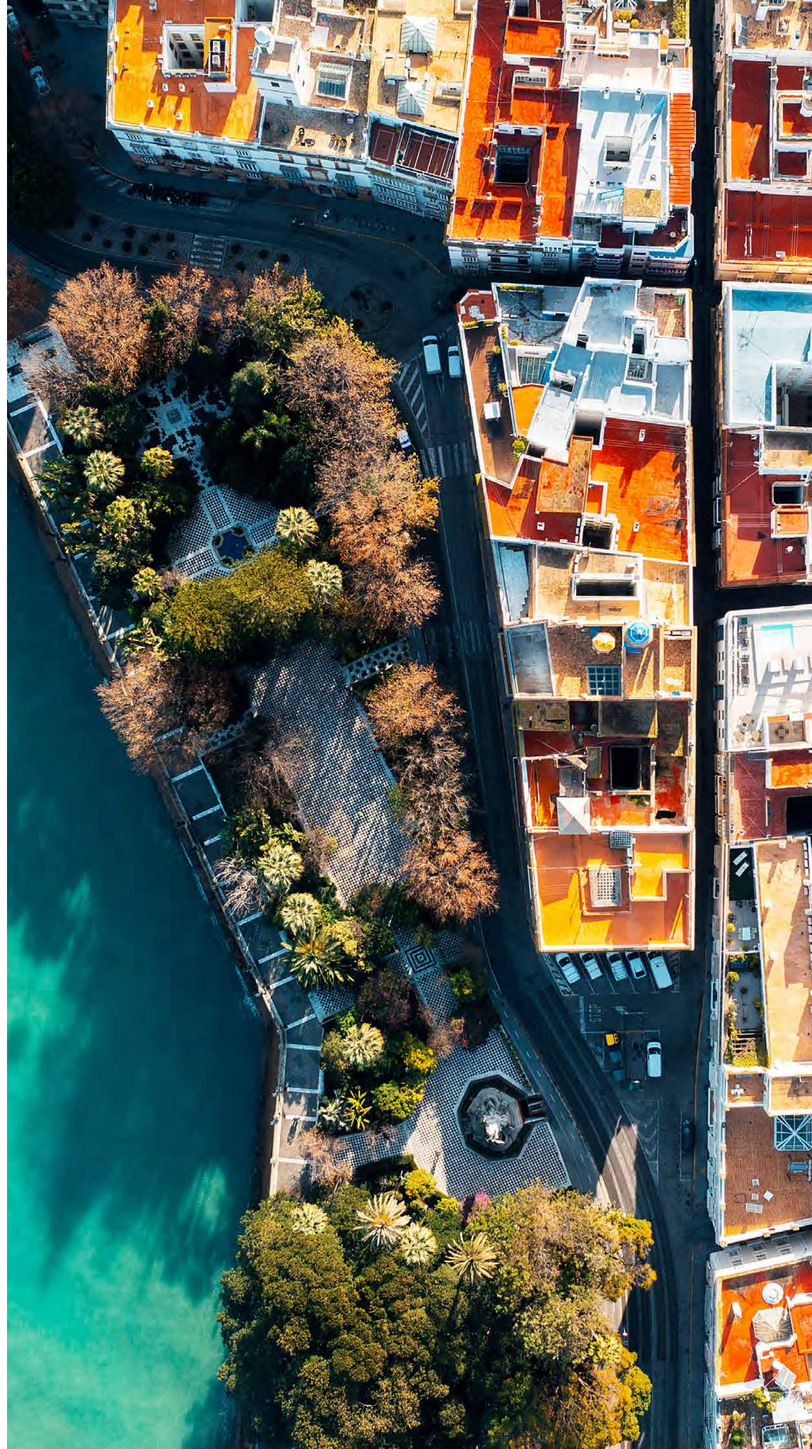
Financial-sector entities face an additional layer under the Digital Operational Resilience Act (**DORA**), which began applying across the EU since 17 January 2025. DORA sets directly applicable obligations for ICT risk management, major-incident reporting, testing, governance and third-party oversight, and creates EU-level oversight for certain critical ICT third-party providers.

Although DORA is directly applicable, national sanctioning and supervisory allocation are established by Member State law. In Spain, the Council of Ministers approved in December 2024 the Draft Law on the Digitalisation and Modernisation of the Financial Sector (**DORA Draft Law**) to articulate the Spanish sanctioning framework and designate competent authorities for DORA supervision. Sectoral supervisors including the Bank of Spain, the National Stock Market Commission (**CNMV**) and the General Directorate of Insurance and Pension Funds (**DGSFP**) are expected to be empowered to impose both monetary fines and non-monetary measures for breaches of DORA.

In terms of fines, the DORA Draft Law points towards fines of up to EUR 5M or 5 percent of annual turnover for legal persons, while natural persons (i.e., individuals in management roles) may be fined up to EUR 1M or five times the benefit gained. However, the specific Spanish fine scales for DORA breaches are still to be confirmed upon the definitive enactment of the final law.

Sector-specific cybersecurity and operational security obligations also feature in telecommunications and public-sector contexts. Telecommunications providers are subject to statutory duties, including security and incident-notification duties to the Ministry of Economic Affairs and Digital Transformation, under the General Telecommunications Law. In the public sector, the National Security Scheme (**ENS**) imposes technical security baselines and incident reporting, enforced through administrative powers.

Critical infrastructure sectors such as energy, water, transport and health are subject to the NIS/NIS2 regime and, where applicable, sectoral regulators. Lastly, please note that, even though the Critical Entities Resilience Directive (**CER**) imposes substantial incident reporting obligations, Spain has not yet transposed CER into national legislation; and the currently applicable critical entities regulations, namely Law 8/2011 and Royal Decree, do not impose any incident notification requirements.



Netherlands

The principal sources of regulatory fines, specifically Cyber Fines, in the Netherlands are the following:

General Data Protection Regulation (GDPR)[41]

GDPR requires appropriate security for the processing of personal data under Article 32. Non-compliance with Article 32 GDPR can result in fines up to EUR 10M or 2 percent of the global annual turnover, whichever is higher.[42] In addition, Article 5(1)(f) requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"). Non-compliance with Article 5(1)(f) GDPR can result in fines up to EUR 20M or 4 percent of the global annual turnover, whichever is higher.[43]

Network and Information Systems Security Act (Wbni)

The Wbni imposes cybersecurity obligations on operators of essential services (e.g., energy, water, transport and finance) and digital service providers. Insurers or insurance intermediaries do not qualify as operators of essential services or digital service providers.[44] The obligations under this act include:

- Taking measures to manage the risk to network security;
- Taking measures to prevent incidents and to limit their consequences, and;
- Notify the minister/designated authorities about an incident or breach with significant consequences.[45] Fines can be up to EUR 5M.[46]

The Wbni will be replaced by the Cybersecurity Act (implementing the NIS2 Directive). The draft bill was published in June 2025. The Dutch government aims for the Cybersecurity Act to enter into force in Q2 2026. Under the Cybersecurity Act, essential and important entities must:

- Take appropriate and proportionate measures to manage the risks of the security of their network and information systems;
- Take measures to prevent incidents or limit their consequences, and;
- Report any significant incident.[47] Fines can reach EUR 10M or 2 percent of the global annual turnover.[48] We again assume that insurers and insurance intermediaries will fall outside the scope of the Cybersecurity Act.

Dutch Telecommunications Act (Not Relevant for Insurers and Intermediaries)

The Dutch Telecommunications Act imposes obligations concerning cybersecurity and breach notifications on telecom providers. Fines for violations can be up to EUR 900.000, or 1 percent of the annual turnover.[49] This act does apply to insurers and insurance intermediaries.

DORA

DORA sets out requirements for ICT risk management, incident reporting, digital operational resilience testing and third-party risk management for financial entities and their ICT service providers. Fines for violations can reach EUR 10M, or 10 percent of the annual turnover, whichever is higher.[50]

EU AI Act

The *EU AI Act will be discussed under Question 7.*

41. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
42. Artt. 32 and. 83 GDPR.
43. Artt. 5(1)(f) and. 83 GDPR.
44. Since they are not mentioned under art. 2 Decree on Security Network and Information Systems.
45. Artt. 7, 8 and 10 Wbni.
46. Art. 29 Wbni.
47. Artt. 21 and 25 Draft Cybersecurity Act.
48. Art. 80 Draft Cybersecurity Act. Note: this is the regime for essential entities. Digital service providers qualify as important entities and can be subject to a EUR 7M fine or 1.4 percent of the global annual turnover (Art. 87 Draft Cybersecurity Act).
49. Art. 15.4 Telecommunicatiewet.
50. Art. 50 DORA and Art. 1:81(3) Wet op financieel toezicht (Wft).

France

Data Protection/Privacy Laws and Regulations

The GDPR (Reg. [EU] 2016/679) and French Data Protection Law (Loi Informatique et Libertés, n° 78-17) impose duties of security of processing (Art. 32 of GDPR), breach notification (Arts. 33–34 of GDPR) and a core security principle (Art. 5 of GDPR). In France, the CNIL, which investigates and can impose administrative fines and corrective measures under the French Data Protection law, has made cybersecurity a key focus of its 2025-2028 strategic plan. Recent CNIL practice often couples Art. 32 with transparency/minimisation violations.

Cyber-Specific and Relevant Resilience Laws and Regulations

France maintains a cyber-specific regime under Law No. 2018-133 of 26 February 2018 on various provisions adapting to European Union law in the field of security (only available in French), transposing the first Directive NIS. This law provides for fines, in particular when organisations (i) fail to implement required security measures within the period set in a formal notice, (ii) fail to notify the French National Cybersecurity Agency (the **ANSSI**) of significant incidents and/or (iii) obstruct inspection operations.

The NIS2 (Directive [EU] 2022/2555): expanded security/risk management and incident reporting duties for essential and important entities, plus broad supervisory powers (audits, binding instructions, orders). However, French transposing law is not enacted yet. France is transposing NIS2 via the Bill on critical infrastructure resilience and cybersecurity enhancement, adopted by the French Senate on 12 March 2025 and pending before the National Assembly. ANSSI is expected to play a central role.

Sector-Specific Laws and Regulations

The Financial sector is subject to DORA (Reg. [EU] 2022/2554), which has applied since 17 January 2025 and is supervised in France by the ACPR and AMF. Failures in ICT risk management, incident reporting, testing, or third party risk can trigger administrative measures under sectoral law.

Switzerland

The Federal Act on Data Protection (**FADP**) with its implementing Ordinance (Data Protection Ordinance; **DPO**) constitutes the principal legal framework for data protection and privacy in Switzerland. It applies to the processing of personal data of natural persons by private persons and federal bodies. The revised FADP came into force on 1 September 2023 after a comprehensive revision to bring the legislation in line with the European General Data Protection Regulation (**GDPR**).

The FADP does not specifically provide for fines in case of cyber incidents (not even if the reporting obligation is not adhered to). However, on complaint, a fine not exceeding CHF 250,000 may be imposed on private persons who wilfully fail to comply with the minimum requirements for data security stipulated by the Federal Council.[51] In this regard, the FADP requires the controller and the processor to guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures.[52]

The DPO further specifies what such relevant technical and organisational measures may be.[53] Moreover, any private person who willfully fails to comply with a ruling issued by the Federal Data Protection and Information Commissioner (**FDPIC**) (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter; **EDÖB**) or a decision of the appeal courts that refers to this penalty may be liable to a fine not exceeding CHF 250,000. Therefore, if the FDPIC issues a ruling in connection with a cyberattack (e.g., orders the controller to inform data subjects of a data breach) and such ruling is not complied with, a fine may be imposed.

The FDPIC generally is the competent authority responsible for enforcing compliance with the FADP and its Ordinance. However, the prosecution and the adjudication of criminal acts (including the imposition of fines) is a matter for the cantons, in particular the cantonal prosecution authorities. The FDPIC may only file a complaint with the competent prosecution authority and exercise the rights of a private claimant in these proceedings.

Fines in accordance with the FADP are imposed ad personam, meaning that they are imposed on the natural person responsible for data protection and not a company. The economic circumstances of the person concerned are taken into account when determining the amount of the fine. Only if a fine not exceeding CHF 50,000 is under consideration and if the identification of the perpetrators requires measures that would be disproportionate in view of the potential penalty, the authority may decide not to pursue these persons but instead to order the company to pay the fine.[54]

51. Article 61 lit. c FADP.
52. Article 8 para. 1 and 3 FADP.
53. Article 3 DPO.
54. Article 64 para. 2 FADP in connection with Article 6 and 7 of the Federal Act on Administrative Criminal Law (ACLA).

Since the revised FADP came into force in September 2023, only a handful of data protection related fines have been imposed in Switzerland. Such fines have stayed rather low (i.e., below CHF 1,000) and were mostly not related to cyber incidents.

Cyber-Specific and Relevant Resilience Laws and Regulations

The Federal Information Security Act (**ISA**) and its related Ordinances (Information Security Ordinance, ISO; Ordinance on Personnel Security Screening, PSSO; Ordinance on the Industrial Security Procedure, ISPO; and Ordinance on the Federal Identity Management Systems and Directory Services, IAMO) provide the legal cyber security framework for public institutions in Switzerland. It applies generally to so-called obligated authorities and organisations who in turn must ensure that the requirements and measures imposed in the ISA are laid down in the relevant agreements and contracts with third parties.

The provisions on notification of cyberattacks additionally also apply directly to providers of critical infrastructure such as public authorities and organisations, higher education institutions, companies active in the areas of energy supply, healthcare facilities, news agencies of national importance, providers of cloud computing, search engines, digital security and trust services and data centre.

The ISA aims to ensure the secure processing of information for which the Federal government is responsible and the secure use of federal IT resources as well as to increase Switzerland's resilience to cyber threats.[55] In this regard, it imposes cyber security obligations on obligated authorities and organisations[56] and implements a notification obligation in case of cyber security incidents to the National Cyber Security Centre (**NCSC**).[57]

As is the case with the FADP, the ISA also does not specifically provide for fines in case of cyber incidents. However, as of 1 October 2025, anyone who deliberately fails to comply with a final decision issued by the NCSC with reference to this penalty or with a decision of the appeal courts may be punished with a fine of up to CHF 100,000.[58] Such decision may occur if there are indications of a breach of the reporting obligation where the NCSC informs the respective obligated authority or organisation and sets a reasonable deadline for it to comply with the reporting obligation. If the obligated authority or organisation fails to comply with its obligations within this period, the NCSC may issue a ruling, setting a new deadline and referring to the penalty set out in the ISA.[59]

Fines are again imposed ad personam and the economic circumstances of the person concerned are taken into account when determining the amount of the fine. Only if a fine not exceeding CHF 20,000 is under consideration and if the identification of the perpetrators requires measures that would be disproportionate in view of the potential penalty, the authority may decide not to pursue these persons but instead to order the company to pay the fine.[60] The prosecution and adjudication of a violation of an NCSC order is a matter for the cantons, in particular the cantonal prosecution authorities.

Since the provisions implementing these fines were only adopted as of 1 October 2025, no such fines have been issued yet.

Sector-Specific Laws and Regulations (e.g., Operational Resilience Rules and Critical Third Parties Regime Which Applies to the Financial Sector in E&W)

In addition to the fines set out in the FADP as well as the ISA, various sector specific laws and regulations provide for fines in relation to cyber incidents, such as i.e.:

55. Article 1 ISA.
56. Article 6 ISA.
57. Articles 74a et seqq. ISA.
58. Article 74h ISA.
59. Article 74g ISA.
60. Article 74h para. 2 and 3 ISA in connection with Article 6 ACLA.

Financial Services Sector

The Federal Act on the Swiss Financial Market Supervisory Authority (**FINMASA**) is applicable to persons and entities that under the financial market acts require to be licensed, recognised, or registered by the Financial Market Supervisory Authority (**FINMA**) and collective capital investments under the Collective Investment Schemes Act that have been or must be licensed or approved (so-called "supervised persons and entities"). It provides for a regulatory reporting obligation for supervised persons and entities and the audit companies that conduct audits of them regarding any incident that is of substantial importance to the supervision (which includes cyber security incidents).[61]

This reporting obligation is connected to potential criminal sanctions for failing to report. Accordingly, any person who as an agent willfully and seriously violates the supervisory provisions by falsely stating essential information in the report or withholding essential information or failing to make a mandatory report to FINMA is liable to a custodial sentence of up to three years or to a monetary penalty. Where the offender acts negligently, he or she is liable to a fine of up to CHF 250,000.[62] Moreover, any person who willfully fails to comply with a legally enforceable ruling issued by FINMA containing notice of this penalty or with a decision of the appeal courts is liable to a fine of up to CHF 100,000.[63]

With its Guidances 05/2020 as well as 03/24, FINMA specifically reminded all supervised institutions of their legal requirement to immediately report any incident that is of substantial importance to the supervision.

Telecommunications Sector

The Telecommunications Act (TCA) and the respective Ordinance on Telecommunications Services (OTS) regulate the transmission of information by means of telecommunications techniques, including the transmission of radio and television programme services. They implement a comprehensive legal framework for the provision of telecommunications services in Switzerland, including respective registration and licensing requirements for certain telecommunication services providers.

The TCA and OTS require telecommunication service providers to take action against unauthorised manipulation of telecommunication installations by telecommunications transmissions and provide for specific security measures applicable to the various telecommunication services providers.[64] Moreover, the telecommunications legislation sets out that telecommunications service providers must immediately report faults in telecommunications installations and services that could affect at least 10,000 customers to the National Emergency Operations Centre and provide information on the faults on a publicly accessible website.[65]

Any person who installs or operates telecommunications installations that do not comply with the regulations in force is liable to a fine not exceeding CHF 100,000, in case of negligence not exceeding CHF 50,000.[66] Moreover, failure to comply with a provision of the telecommunications legislation, a treaty or international agreement on the subject or a violation of a decision taken on the basis of such provisions and notified to such person with an indication of these penalties may be punishable with a fine not exceeding CHF 5,000.[67] Any such fines are imposed ad personam.

The enforcement and supervision of the telecommunications legislation is entrusted to both the Federal Office of Communications (**OFCOM**) as well as the Federal Communications Commission (**ComCom**). Offences set out by the TCA should by law be prosecuted and adjudicated by the Federal Department of the Environment, Transport, Energy and Communications

61. Article 29 para. 2 FINMASA.
62. Article 46 FINMASA.
63. Article 48 FINMASA.
64. Article 48a TCA.
65. Article 95 para. 1 OTS.
66. Article 52 para. 1 lit. e and para. 2 TCA.
67. Article 53 TCA.

(**DETEC**). However, DETEC has delegated the prosecution, adjudication as well as the enforcement of decisions to OFCOM in accordance with the TCA.[68]

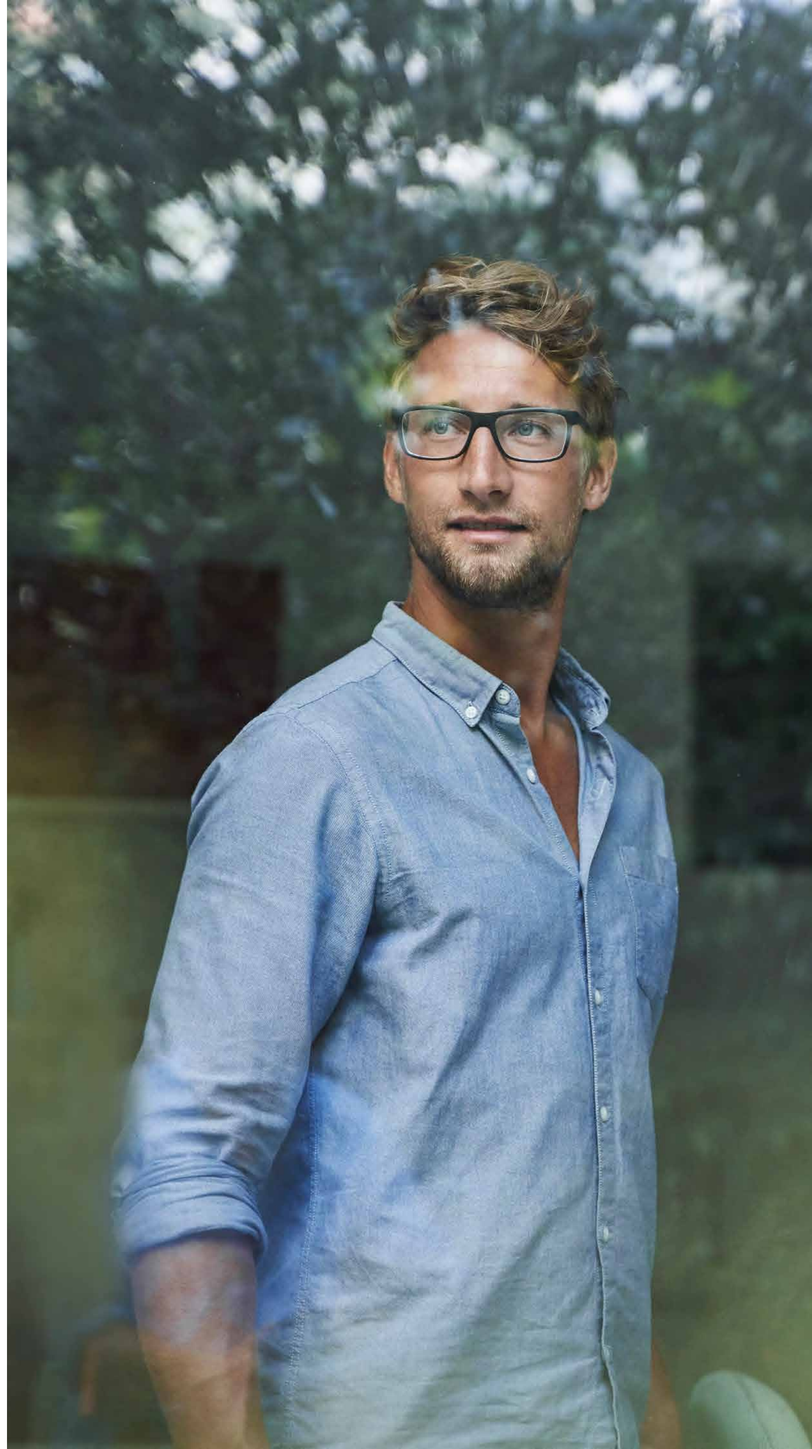
Nuclear Energy Sector

The Nuclear Energy Act (**NEA**) and its related Ordinance (**NEO**) require security measures to be taken in order to prevent any interference with the safety of nuclear installations and nuclear materials through unauthorised acts or the theft of nuclear materials.[69] Any events that may occur in connection with the condition and operation of a nuclear installation and that impair or may impair safety or constitute sabotage or attempted sabotage, extortion, accidents, damage to or failure of security equipment and systems that last longer than 24 hours, malicious acts in and in the vicinity of the nuclear installation that are attributable to, or indicate, unauthorised interference, or any other malicious acts and findings that impair or may impair security, must be reported to the Swiss Federal Nuclear Safety Inspectorate (**ENSI**).[70]

ENSI acts as supervisory authority with regard to nuclear safety and security. The Swiss Federal Office of Energy acts as supervisory authority for other areas of enforcement of the NEA.[71]

The NEA provides that contraventions to the NEA are punishable with fines. Accordingly, any person who willfully refuses to provide information, submit documentation or permit access to business premises or inspection of documentation, or gives false information in this regard, fails to comply with a reporting obligation, an auditing and accounting obligation or an obligation to keep records in accordance with the NEA, or infringes an implementing Ordinance, infringes in any other way a provision of the NEA or of an implementing regulation if the contravention thereof is declared to be an offence, or of a ruling issued with a reference to this penalty, where no unlawful conduct is involved that constitutes another criminal offence, may be liable to a fine not exceeding CHF 100,000. Attempts and aiding and abetting are also considered to be offences and are subject to the same penalties. Negligence reduces the maximum fine to CHF 40,000.[72] Fines are generally issued ad personam.

Such contraventions to the NEA are prosecuted and adjudicated by the Federal Office of Energy subject to the provisions of the Federal Act on Administrative Criminal Law (**ACLA**).



68. Article 55 TCA in connection with Article 1 of the Ordinance of the DETEC on the delegation of powers to impose penalties for violations of the Telecommunications Act
69. Article 5 para. 3 NEA
70. Article 22 para. 2 lit. f NEA in connection with and Article 38 para. 3 NEO.
71. Article 6 NEO.
72. Article 93 NEA.

2

Are Cyber Fines Insurable?

Chapter Summary

The insurability of cyber fines is highly jurisdiction-dependent. The landscape is marked by legal uncertainty and significant variations.

Across markets, insurers routinely cover defence, investigation, notification, PR, business-interruption and restoration costs and civil fines to the extent that they are insurable by law.

In most EU countries and the UK, criminal fines and administrative fines with a punitive or deterrent purpose are not insurable. This reflects public policy concerns that insurance should not undermine the deterrent effect of regulatory enforcement. Payouts for fines which do not fall foul of these concerns and policy exclusions for intentional or grossly negligent acts, are rare and subject to judicial interpretation.

Outside the EU, approaches vary: South Africa and Saudi Arabia rely on common law and regulatory approval, with similar exclusions for wilful misconduct.

Across the board, it is critically important to take account of nuances in local law and policy wordings, and to appreciate the limits on coverage for this type of exposure.

Practical Actions for Organisations to Consider Now

- Review your cyber insurance policies for exclusions related to fines and definitions of insurable events.
- Consider other insurance policies that might offer the correct level of coverage, such as D&O or professional indemnity.
- Ensure your insurance is expanded to ensure the broadest possible coverage — including no territorial limits, but worldwide cover.
- Consult legal counsel to clarify insurability in relevant jurisdictions.
- Train leadership on insurance limitations: ensure executives understand what is and isn't covered to avoid assumptions during crises.
- Quantify your organisation's risk profile, considering your sector, industry and risk exposure.
- Prepare a claims protocol to ensure the right process is followed and decisions made in the event of an incident.

Belgium

As a principle, criminal fines are not insurable under Belgian law.

Administrative fines will likewise not be insurable if the administrative sanction is to be considered of a criminal nature within the meaning of Article 6 of the European Convention of Human Rights. Following the well-known Engel criteria, the assessment of the criminal character of an administrative fine will be made on the following criteria:

- The legal classification of the offence under national law;
- The very nature of the offence, and;
- The severity of the penalty that the person concerned risks incurring (with the second and third criteria being alternative criteria).

The existence of a criminal character of an administrative fine will require a case-by-case assessment. However, generally speaking, most Cyber Fines are likely to be considered of a criminal nature, therefore not be insurable under Belgian law (at least not to benefit the person convicted as the offender).

In addition, and even where Cyber Fines do not qualify as criminal fines, insurers will often refuse coverage on the basis that the person insured intentionally caused the loss.[73]

Luxembourg

Under Luxembourg law, fines imposed by public authorities, are generally uninsurable. Article 97 of the Law of 27 July 1997 on the insurance contract (the **Law of 1997**) prohibits insurance coverage for criminal fines and penal settlements and Luxembourg courts extend this prohibition to administrative fines that are punitive or criminal in nature. Any contractual provision to the contrary is void under Article 6 of the Civil Code as contrary to public policy. While some international insurers may offer coverage for fines "to the extent insurable," in practice, Luxembourg could prevent indemnification for such fines. Local insurers typically exclude coverage for fines altogether, limiting policies to legal defence costs, notification expenses, third-party liability and first-party losses such as business interruption and incident response.

Portugal

Covering any fines through insurance is expressly forbidden under Portuguese law. In fact, Article 14 of the Portuguese Legal Framework for Insurance Contracts (approved by Decree-Law 72/2008, of 16 April, as amended) provides that entering into an insurance contract which cover risks of criminal liability, administrative/regulatory liability and disciplinary liability is forbidden. Fines being sanctioning (and not compensatory) measures arising out of criminal or administrative/regulatory liability, their coverage through insurance contracts is forbidden and any insurance contracts containing such clauses will be deemed null and void. Consistently, such contracts will not be enforceable in Portuguese courts.

It should be also noted that, according to the above mentioned Legal Framework for Insurance Contracts, the coverage of fines through insurance leads to the respective insurance contract not being valid or enforceable in Portugal (i.e., in Portuguese courts) even if the insurance contract is subject to a law other than Portuguese law.

Finland

Cyber Fines are not insurable in Finland. Although most insurance companies offer cyber insurance policies, Cyber Fines are not covered by them. This is due to the concept of “good insurance practice”1, which insurance companies in Finland are obliged to adhere to pursuant to section 30 of the Insurance Distribution Act (234/2018). The concept requires insurance activities to be not only legal, but also ethically sound, fair and just.2

Chapter 25, section 1, subsection 1 of the Insurance Companies Act (521/2008) states that the FIN-FSA is responsible for supervising that insurance companies comply with the legislation governing insurance activities and good insurance practice.

73. Article 62 of the Belgian Insurance Act.

The FIN-FSA has published an official interpretation of the insurability of administrative fines and penalty payments. According to the interpretation, the FIN-FSA considers insuring against any administrative and criminal fines to be contrary to good insurance practice: insuring against the risk of administrative or criminal fines might encourage non-compliance with regulatory obligations and that such insurance would conflict with generally accepted social values. Therefore, providing insurance against Cyber Fines is prohibited in Finland as it is contrary to the concept of good insurance practice.

Consequently, it is not possible to recover Cyber Fines under an insurance policy in Finland. However, existing cyber insurance policies provided by insurance companies operating in Finland may cover compensation for financial losses caused by business interruption in case of a cyber incident, liability for damages to third parties, as well as the costs arising from the investigation of cyber incidents. In summary, Cyber insurance policies are obtainable, but being indemnified against Cyber Fines under such policies is not possible.

South Africa

Cyber Fines may be either criminal or administrative in nature and arise pursuant to culpable conduct or omissions.

The insurability of criminal and administrative fines, including those arising from cyber incidents, is not specifically regulated by statute in South Africa. In the absence of express regulation, the issue is to be determined in accordance with common law principles and public policy considerations.

As such, any determination by a court will likely involve a balance between the principle of freedom of contract (*pacta sunt servanda*) on the one hand, and on the other hand, the principles that one cannot pursue legal action based on their own illegal acts (*ex turpi causa non oritur actio*) and nobody may take advantage of their own wrong (*nemo ex suo delicto meliorem suam conditionem facere potest*).

With regard to criminal fines: As a matter of public policy and by virtue of the common law principles noted above, criminal misconduct is generally not insurable in South Africa.

With regard to administrative fines: This is not settled law but — in our view — a court is likely to make a similar determination as would be the case with criminal fines, on similar grounds, i.e., that it would be contrary to public policy and would reduce the intended punitive and/or deterrent effect.

Our view is supported by the approach taken in, for example, section 78(2) of the Companies Act, 2008, which explicitly prohibits attempts to absolve or indemnify directors for fines and penalties arising from wilful misconduct, wilful breach of trust, reckless conduct or fraudulent actions, reinforcing the broader public policy stance against insuring punitive liabilities.

Notwithstanding the above, it should be noted that whilst cybercrimes under the Cybercrimes Act address specific acts of misconduct, the scope of POPIA is broader than misconduct, and violations (and therefore fines) could be triggered by non-compliance with statutory obligations outside of a specific security compromise or other incident.

Whilst the local insurance market does allow for some expansion of cover to address specific instances of non-compliance under POPIA, such cover would not generally extend to any acts of misconduct.

Italy

Article 12 of the Italian Legislative Decree No. 209 of 2005 (the “Private Insurance Code”)

The provision prohibits insurance policies that are intended to transfer the risk of payment of administrative sanctions. In case of breach this prohibition, the insurance contract is null. The nullity at hand can be exercised only by the policyholder and the by the insured (insured and policyholder may be the same person or two different persons; e.g., this happens in case the insurance is a contract in favour of a third party). This is an exception to the general rule that nullity can be exercised by whoever interested.

The prohibition is interpreted in the sense that it regards the direct insurance of the sanction, ie, the risk that the wrongdoer is sanctioned. Instead, it is generally admitted the insurance of the risk that a person different from the wrongdoer — in accordance with a specific civil obligation — shall hold the latter harmless from the monetary consequences of the sanction. Therefore, the insurance of the indirect risk of sanction is deemed admitted. This type of insurance is indeed provided for by Regulation of ISVAP (*Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo* — the Italian Private Insurance Regulator — then replaced by IVASS *Istituto per la Vigilanza sulle Assicurazioni, the Italian Insurance Regultor*) No. 29 of 16 March 2009 (which is the Regulation on the classification of insurance risks).

The rationale is avoiding that the insurance contract may deprive of effects the administrative sanctions, allocating on the insurers the detrimental consequences of the administrative sanctioning.

Article 1900 of the Italian Civil Code

The provision states that insurers are not required to indemnify losses caused by the insurer's wilful misconduct or gross negligence, unless the policy expressly covers gross negligence.

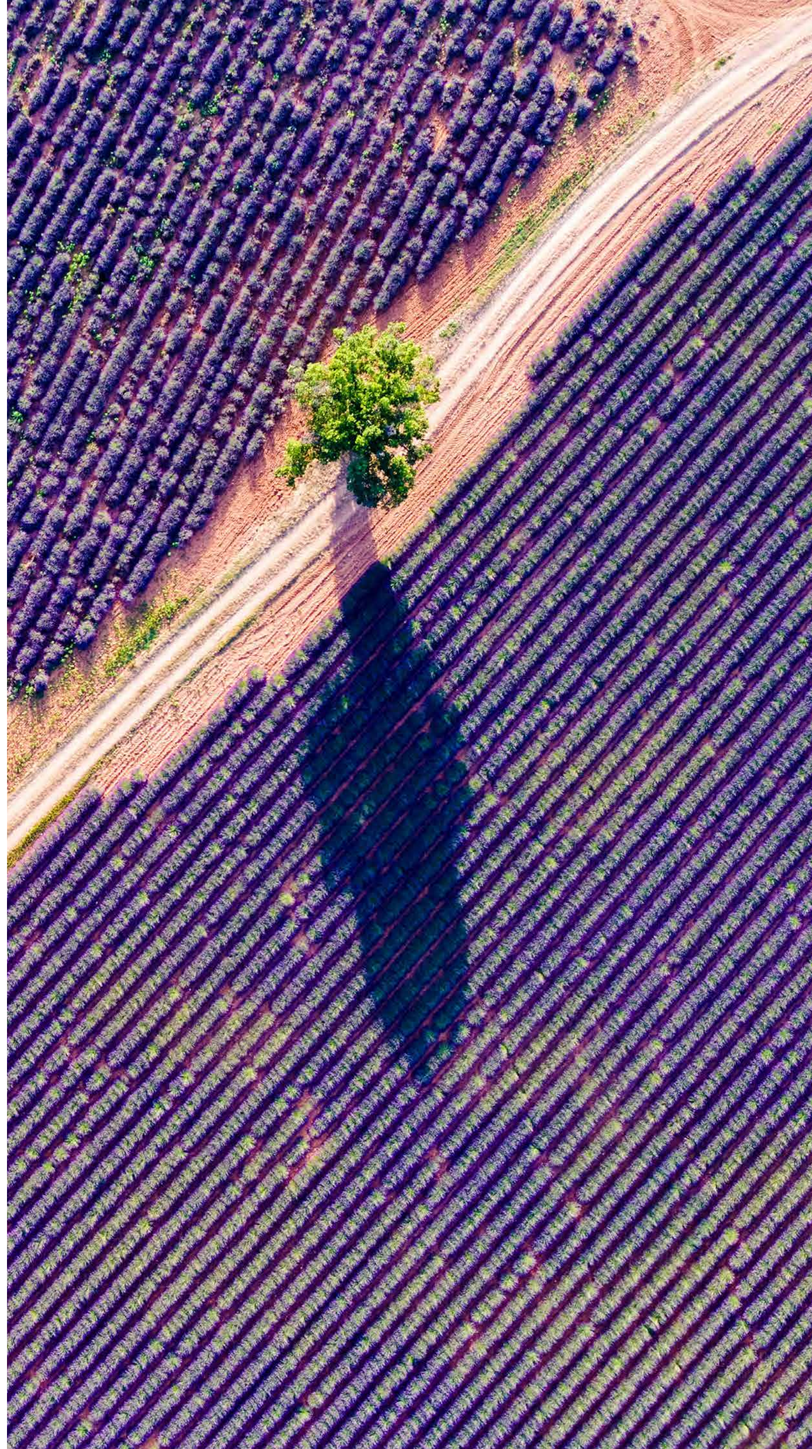
IVASS' (the Italian Insurance Supervisory and Regulatory Authority) Report on Cyber Insurance Policies of October 2023

The report indicated cyber sanctions within the policy exclusion of coverage clauses.

The above remarks do not appear applicable to the financial losses connected with the issuance of a cyber fine (e.g., the above considerations do not seem to apply to the legal costs for defending against the issuance of the sanction) which losses might instead be deemed insurable.

Therefore, it shall be deemed that cyber sanctions cannot be ensured indirectly. It is reasonable to believe that the insurance policy cannot ensure the wrongdoer from the risk of being sanctioned but it can insure third parties to the wrongdoer from the risk of having to hold the wrongdoers harmless from cyber sanctions.

Therefore, while cyber sanctions are generally deemed not directly insurable, it is possible to ensure the civil obligation to hold the sanctioned person harmless from cyber sanctions.



Saudi Arabia

KSA insurance operates under a co-operative model supervised by the Insurance Authority (**IA**) and insurers' products and wordings require SAMA approval and must satisfy core principles like insurable interest and compliance with law/public policy. While there is no blanket statutory prohibition on insuring administrative "regulatory fines" per se, permissibility turns eventually on SAMA's product approval and policy wording (and exclusions for illegality/wilful acts). In practice, some specialty lines (e.g., D&O/PI) may extend to certain regulatory penalties where not contrary to law/public policy, while many standard policies expressly exclude fines/penalties from coverage.

SAMA's Rules of Insurance Products Approval (**RIPA**) and its Implementing Regulations (**IRs**) require prior approval (or file-and-use) before marketing/sale and specify the policy must include coverage description/limits, exclusions, terms/conditions, etc. SAMA may require amendments or suspend marketing if a product conflicts with the Law/Regulations. The IRs of the law state the policy is based on the application and, when completing it, the insured must have insurable interest; also that "*Insurance provided must not violate any rules, regulations and directives.*" (IRs Art. 55(1), (4).)

Market Practice — Standard Exclusions for Fines:

- **Unified Compulsory Motor Policy:** exclusions include "*fines, financial penalties or bails ... imposed on the insured/driver.*" For more info, see Entire Section | SAMA Rulebook.
- **Standard Medical Malpractice Policy:** exclusions include "*any fines, penalties, punitive or exemplary damages*" and "dishonest, fraudulent or criminal acts." For more info, see Entire Section | SAMA Rulebook.

What This Means?

KSA law does not expressly outlaw insurance for "regulatory fines," but any such cover must (i) pass SAMA product approval, (ii) satisfy insurable-interest and legality/public-policy limits and (iii) navigate common exclusions (e.g., willful/criminal acts). Practically, you will see fine coverage excluded in many standard policies, with any affirmative coverage appearing (if at all) in specialty wordings (D&O/PI) vetted by SAMA.

While one may obtain a policy that includes cover for fines, there are important limitations on whether a particular fine will actually be indemnified. KSA rules and regulations will generally not allow insurance to cover deliberate/criminal acts of the insured. For example, if a fine results from intentional wrongdoing, fraud, or willful violation of the law by the insured entity, an insurer would deny coverage on public policy grounds (and policy exclusions).

In practice, the distinction can be summarised as: (a) Obtaining a cyber insurance policy that covers fines — generally allowed if the policy is approved by SAMA. Insurers craft such policies with the necessary exclusions (for fraud, willful breach of law, etc.) to ensure they are not covering uninsurable scenarios. (b) Being indemnified under that policy for a specific fine — this will depend on the facts of the incident and policy terms. We are not aware of KSA statutes that automatically voids coverage of fines, but KSA public policy as stated (and standard policy clauses, as seen above) would prevent indemnification of non-insurable risks (e.g., malicious or intentional acts).

Norway

The answer is not necessarily clear cut, however it is assumed that GDPR-fines and other administrative fines may be insurable, whereas criminal fines and administrative fines with a clear punitive element are likely not insurable. Under Norwegian law, most Cyber Fines are administrative rather than criminal sanctions.

Norwegian law prohibits insurance policies covering criminal fines under the Norwegian Insurance Activities Act 2005, Section 7-1, second paragraph. This prohibition does not, however, encompass regulatory fines. There are, nevertheless, rules in Norwegian contract law that may potentially void insurance agreements covering administrative fines for breaches or non-compliance with the law.

Most topical is NL 5-1-2, which invalidates contracts that are against "law or public decency". A contract is, however, not automatically voided if it is "against the law" — it depends on a individual assessment of whether the considerations the law is founded on warrant invalidity. The provision in NL 5-1-2 also encompasses a requirement that an insurance policy may only insure a "legal interest" — an insurance policy covering an interest that is not "legal", is "against the law or public decency" under NL 5-1-2. The term "legal interest" cannot be construed literally in this connection. Whether an insurance interest is "legal" depends on the following factors (expressed in preparatory works):

- The character of the illegal circumstance;
- The connection between the illegal circumstance and the insured interest; and
- The culpability of the insured person / entity.

The case law relevant to these factors does not explicitly concern insurance policies established intentionally to cover regulatory fines. In a case by the Norwegian Financial Services Complaints Board, it is held that breaches of regulatory laws cannot be considered as "grossly unlawful interests", which might be construed in favor of the insurability of regulatory fines. Moreover, the second and third factor are arguably not particularly apt when undertakings offer insurance policies covering regulatory fines.

In summary, the state of the law on this matter is somewhat unclear. However, a distinction must be made between fines with a clear penal purpose and fines of a more regulatory nature. In the case of the latter, parallels can be drawn to other liability insurances, e.g., covering damages claims against employees or board members. In any event, it is unlikely that the question will be resolved in case law, as insurance firms are not incentivised to attempt to void their own insurance policies. Common practice appears to be offering insurance policies covering regulatory fines "to the extent permitted under Norwegian law" (or similar clauses).

The insurability of Cyber Fines will thus depend on an individual assessment of the legislative intent behind the legal basis of the fine, along with other circumstances. As previously mentioned, it has been argued that GDPR-fines are insurable in Norway. This argument appears to be well founded, as Norwegian law makers consciously decided to abolish criminal punishment for data protection contraventions when enacting the Norwegian Data Protection Act.

Turkey

Under Turkish law, there is no express legislation that permits or prohibits the insurability of Cyber Fines. We have also not identified any court decisions assessing the current legal framework in this regard. However, there are differing doctrinal views on the insurability of Cyber Fines. Certain scholars believe that, in the absence of an explicit legal prohibition, such coverage should be permissible. On the other hand, some scholars assess the matter in the context of mandatory provisions of law and public policy.

According to Article 27 of the Turkish Code of Obligations, contracts that are contrary to the mandatory provisions of the law and public order are deemed null and void. Furthermore, Article 1404 of the Turkish Commercial Code states that "*no insurance may cover any loss arising from an act of the policyholder or the insured that is contrary to the mandatory provisions of the law, morality public order, or personal rights*." According to a view, this provision emphasises that the punitive function of administrative fines should prevail, therefore, such fines are not insurable under Turkish law. Nevertheless, in practice, we see insurance companies including the risk of such fines within the scope of their coverage in Türkiye. In the examples that we have come across, the coverage is mostly related to administrative fines in relation to data protection.

Sweden

Under Chapter 4, Section 3 of the Swedish Insurance Business Act (2010:2043) (Sw. försäkringsrörelselagen), an insurance undertaking must conduct its business in accordance with good insurance standards. In a supervisory statement, 2023:1 Insurance against fines and administrative fines, the SFSA has clarified that providing insurance coverage for fines, corporate penalties, or administrative sanctions is not consistent with good insurance standards. According to the Supervisory Statement, this applies to both Swedish insurance undertakings and foreign insurers operating in Sweden.

It can however be noted that EEA insurers conducting business in Sweden on a freedom of services basis are not subject to the Swedish requirement of good insurance standard. Thus, there is no explicit legal basis for enforcing the position against an EEA insurer that does not conduct business in Sweden through a secondary establishment. Further, the statement does not apply to insurance companies from third countries that do not conduct business in Sweden, but only passively provide insurance at the customer's initiative. The supervisory statement also does not cover marine insurance.

While the position formally concerns the provision of insurance, the statement implies that insurance covering administrative sanctions is without legal effect. If the insurance contract is invalid, this means that a policyholder who has purchased such coverage would be unable to have a claim for indemnification adjudicated in court.

Poland

The insurability of Cyber Fines in Poland remains unclear. Polish law contains no express statutory prohibition on transferring the economic burden of administrative fines to an insurer. Under Art. 822.1 of the Civil Code (consolidated text: Journal of Laws 2025, item 1017) an insurer may indemnify the policyholder for a "pecuniary loss arising from an accident". Cyber Fines qualify as a pecuniary loss in general. Nevertheless, following legal constraints apply.

Firstly, Article 827.1 of the Civil Code explicitly excludes insurance coverage for damages caused intentionally or as a result of gross negligence. It does not prohibit coverage for consequences of ordinary negligence or no-fault situations. The exclusion of coverage for intentional acts or gross negligence applies not only to the policyholder but also to persons for whom the policyholder is responsible (e.g., employees, management). Many administrative fines are imposed for intentional or grossly negligent conduct, which would fall outside the scope of insurability.

Most administrative fines for cyber incidents (e.g., under GDPR) are imposed for breaches that are at least grossly negligent and often for intentional or systemic failures to comply with legal obligations. Thus, if a cyber fine is imposed due to intentional or grossly negligent conduct, insurance coverage for that fine will be automatically excluded by law — even if the policy includes a “to the extent insurable by law” clause.

Secondly, the Civil Code (Art. 353^1) allows parties to shape contractual relations freely, provided that the object of the contract is not contrary to law, the nature of the legal relationship or the principles of social coexistence (zasady współżycia społecznego, Polish public-policy equivalent). Even if a policy were to purport to cover such fines, Polish courts may refuse to enforce indemnification for administrative penalties on the grounds of public policy, especially where the penalty is intended to punish or deter unlawful conduct. Where an administrative fine serves a strictly punitive, deterrent purpose, indemnification may be viewed as undermining that purpose and therefore contrary to public policy. This is rooted in the public policy objective of ensuring that sanctions retain their deterrent effect and are not neutralised by insurance. If the fine is compensatory (i.e., intended to cover actual harm or loss rather than to punish), there is a greater likelihood that coverage would not be contrary to public policy.

Taking out a policy that nominally covers Cyber Fines is not itself prohibited; nonetheless, enforceability of the indemnity clause is judicially untested in Poland and may be struck down under Article 3531 in connection with Article 58 of the Civil Code, if a court concludes that paying the fine frustrates its punitive purpose.

In practice, therefore, cyber insurance policies issued on the Polish market normally contain a clause granting cover for fines "to the extent insurable by law". This means the insurer may agree to provide coverage, but only for those fines which are not expressly prohibited from being insured under applicable law. Even if a policy is obtained, actual indemnification will depend on the nature of the fine and the circumstances of the breach. If the fine is imposed for intentional or grossly negligent conduct, or if the law or public policy prohibits indemnification, the insurer will not be able to pay out. The practical effect is that coverage for Cyber Fines will often be illusory in Poland, except perhaps for certain administrative fines imposed for minor, non-intentional breaches where public policy concerns are less acute.

England and Wales

Under English law, with one notable exception it is currently uncertain whether Cyber Fines are insurable. The exception is FCA fines, which regulated entities are expressly prohibited from insuring against. As the UK GDPR, DPA 2018, PECR and NIS Regulations are silent on this issue, the insurability of Cyber Fines turns on the application of the ex turpi causa doctrine which prevents a party being indemnified for a loss which results from its own wrongdoing. However, such cases as there are in this area (none of which relate to Cyber Fines) indicate that the question in each case will be whether the underlying conduct has sufficient "moral turpitude" for the doctrine to apply.

As a result, most commentators (including us) take the view that it is necessary to evaluate the underlying conduct which gave rise to the Cyber Fine. Until clear guidance is provided by the English Courts, it seems more arguable that a Cyber Fine is insurable where the conduct is innocent or negligent and less arguable where the conduct is deliberate or reckless. Either way, there is no legal difficulty with the way in which cyber insurance policies provide coverage for Cyber Fines "to the extent insurable by law."

Ireland

The position in Ireland on the insurability of Cyber Fines is not currently set out in legislation or settled in case law.

While there is no general prohibition on insurance re such fines, it is worth noting the legal doctrine of *ex turpi causa*, which prevents an individual or company from pursuing a legal action if it arises in connection with the wrongdoings of that individual or company. If the purpose of a regulatory fine is to be dissuasive, but is also indemnifiable, then the public policy reasons behind the fine may be nullified.

However, the position is less clear when it comes to administrative fines. Insurance providers may offer cyber insurance, but these policies are generally caveated that the cover is "only to the extent insurable by law" i.e., the legal costs, other costs and liabilities following a data breach can be insured, but not the fine itself.

The Irish courts have not yet considered the doctrine of *ex turpi causa* in the context of the insurability of Cyber Fines. However, in the case of *Quinn v Irish Bank Resolution Corporation Limited* [2015] IESC 29, the Supreme Court noted that "*in a highly regulated age... a more nuanced approach is to be preferred*" in the context of the application of the doctrine. The court noted that there is the potential for injustice if the courts were to apply the doctrine where there is a breach of a regulatory regime. The court also suggested that it may need to assess the public policy underpinning each statutory provision (i.e., the relevant cybersecurity legislation imposing such fines) and whether such public policy would be undermined by allowing enforceability of such contracts.

UAE

The UAE laws addressed in Question 1 above do not specifically prohibit or limit insuring against Cyber Fines under an insurance policy. Based on market research, we have seen that cyber insurance providers do insure against regulatory fines.

Germany

Insurance contracts in Germany are governed by the VVG (*Versicherungsvertragsgesetz*, Insurance Contract Act). The VVG does not contain explicit limits on insurability. However, insurance contracts may be legally void if they offend common decency (Sec. 138[1] BGB, *Bürgerliches Gesetzbuch*, Germal Civil Code). The interpretation of the general clause Sec. 138(1) BGB is subject to extensive and often contradictory case law.

The current case law and relevant literature give the following outlines:

- **Cyber Risks**, meaning disadvantageous economic consequences of cyber incidents, are generally insurable in Germany. Although cyber risks are the number one concern for companies in Germany, the market is still relatively young and sparse, but becoming increasingly popular.
- **Cyber Fines** serve a punitive purpose. The transfer of economic risk to an insurer would lessen their efficiency and coercive effect and unduly relieve the tortfeasor. Such insurances therefore offend common decency and are legally void as per Sec. 138(1) BGB).

The available case law revolves around antitrust cases, which require a wilful cooperation to harm competition. The assessment of common decency may be different for negligent Cyber Fines. Until clear guidance arrives, companies should consider Cyber Fines uninsurable.

Different rules may apply to D&O insurances against Cyber Fines in the context of recourse. After a company incurred a fine, they will regularly seek damages and recourse from their managers. Whether such recourse is insurable, is not yet clarified. We could not identify relevant case law to the contrary.

Please note that the admissibility of recourse is disputed. The German legislator initially intended to exclude such recourse in Sec. 38(2) NIS2-UmsG but later removed the relevant passage. The BGH (*Bundesgerichtshof*, German Federal Supreme Court) recently referred the question to the CJEU. It considered the effectiveness of EU antitrust law impeded if companies could infringe antitrust law and then refer to their managers' D&O insurances.[74] A decision is expected in 2026, at the earliest.

Limiting the policy to cover fines "to the legally admissible extent" is common practice in Germany, but leads to open and longwinded lawsuits between insurers and insured person.

The limitations set out above do not prevent insurers form covering ancillary cost, e.g., for defence against GDPR fines, reputational damages or legal counsel related to the incident.

74. German Federal Court of Justice refers question of manager liability for cartel fines to CJEU | Gleiss Lutz.

Spain

Spanish insurance contract law and supervisory policy operate together to render administrative monetary sanctions non-insurable in practice. The Spanish Insurance Contract Act (**SICA**) bars indemnity where the loss was caused by the insured's bad faith (Article 19 SICA) and, in the legal-expense line of business, expressly excludes payment of fines and expenses arising from sanctions imposed by administrative or judicial authorities (Article 76 b) SICA). Although the latter exclusion is specific to legal-expense insurance, it highlights a legislative reluctance to construe public-law sanctions as an insurable loss.

More importantly, the Spanish insurance supervisor (**DGSFP**) has long held the view that indemnifying administrative or criminal sanctions is contrary to public order insofar as it would undermine their punitive and deterrent functions. That position, although set out in a 2008 consultation, eventually translated into how insurance products have been designed and how supervisory expectations were shaped across lines of business.

Spanish courts have confirmed in adjacent contexts that certain sanction-like liabilities assigned personally by statute are non-transferable and non-insurable. Although there is no Supreme Court judgment squarely on GDPR/NIS/DORA fine indemnity, the combined effect of the statutory bad-faith bar, the legal-expense exclusion and the supervisor's public-order doctrine means that administrative fines imposed by Spanish authorities are generally treated as non-insurable, irrespective of whether the infringement is characterised as negligent rather than intentional.

Please also note the distinction between (a) obtaining a cyber insurance policy which covers Cyber Fines to the extent that they are insurable and (b) being indemnified under such a policy. Using E&W as an example, this is a relevant distinction because, whereas (a) is permitted, in certain cases there are prohibitions against indemnification, as well as relevant principles that can render contractual provisions void or unenforceable.

Spanish cyber insurance policies frequently include language that purports to cover "*regulatory fines and penalties to the extent legally insurable*," often alongside exclusions for criminal fines and deliberate or fraudulent acts. However, there is a crucial distinction between the ability to purchase such a policy and the ability to be indemnified for a particular sanction.

While it is permissible and commonplace to subscribe to a policy referencing coverage for insurable fines, the enforceability of indemnification for administrative fines imposed by Spanish authorities will depend on the nature and origin of the sanction, the specific policy wording and, most importantly, the application of Spanish public order principles.

Given the historical position of the DGSFP coupled with statutory exclusions, indemnity for most administrative fines (such as those under the GDPR, LSSI, or NIS/NIS2) are likely at risk of being denied or voided as contrary to public order, irrespective of whether the policy may include a coverage grant.

For illustration purposes, in practice, insurers who operate in Spain would normally cover legal defence costs, investigation expenses, notification costs and compliance remediation measures, but resist indemnifying the fines themselves. Even where an insurer were to pay a non-insurable fine voluntarily, it could end up subject to supervisory scrutiny. It is therefore important for policyholders to understand that while purchasing a policy with "*fines where insurable*" language is possible, the actual likelihood of being indemnified against administrative sanctions is unlikely.

Careful characterisation of the liability would also be required, as not all public-law monetary exposures are considered "*fines*", although the prevailing legal and regulatory framework points to the fact that the financial burden of punitive administrative sanctions, as a general rule, cannot be transferred over to insurers.

Netherlands

In the Netherlands, Cyber Fines can be insured because they are administrative fines. Most (Dutch) cybersecurity insurance policies include wording such as: "*administrative fines are covered, insofar they are insurable*".[75] In particular, cyber insurance and directors' and officers' liability insurance covers administrative fines. Usually, this coverage applies only if such insurance is permitted by court or by legislation. There remains legal uncertainty in the Netherlands as to whether insuring administrative fines is allowed.

In principle, fines are not insurable if doing so would violate public order or morality, within the meaning of Article 3:40 of the Dutch Civil Code (**DCC**). The prevailing view is that insurance for punitive fines but also traffic fine is in breach of Article 3:40 of the DCC. Whether insuring fines contravenes public order or morality must be assessed case by case. Unlike punitive fines, administrative fines (e.g., under a cyber security) are not, in principle, considered contrary to public order of morality.[76] Nevertheless, some Dutch scholars question the insurability of an administrative fines imposed by the Dutch DPA, arguing these fines are punitive in nature[77] and should therefore be treated as punitive fines, making coverage incompatible with Article 3:40 DCC — or at least excluded for serious infringements. Even so, the Dutch market practice shows many insurers still over cover Cyber Fines.[78] We therefore conclude that Cyber Fines are insurable under Dutch law, unless and until case law or legislation provides otherwise.

Although a Cyber Fine might be insurable, indemnification it is prohibited where the insured acted with intent or gross negligence.[79] Here, intent must be understood as intent as purpose or intent as awareness of certainty. [80] The Dutch Supreme Court considers indemnification in cases of intent or gross negligence contrary to the public order and morality.[81]

France

Relevant Legal or Regulatory Prohibitions or Limitations on Insuring Against or Recovering Cyber Fines Under an Insurance Policy

French statutory law and case law neither prohibit nor clearly delimit the insurability of Cyber Fines. However:

- Legal scholarship and policy bodies (notably the High Committee for Financial Markets of Paris [HCJP]) predominantly and explicitly take the view that cyber related financial penalties (especially CNIL fines, including penalty payment) are assimilated to criminal penalties and are therefore uninsurable, as this would generally be against public order, but also since, under the GDPR, fines imposed should be "dissuasive", which would not truly be the case of an insurable fine, and;
- The French Prudential Supervision and Resolution Authority (ACPR) recently issued a press release stating that all administrative pecuniary sanctions are uninsurable, and that any clause purporting to cover such fines would be void "subject to the discretion of the courts" — although the legal force and normative scope of that statement remains debated.

The above mentioned HCJP report suggested inserting a new paragraph V into Article 21 of the French Data Protection Law, prohibiting, for the sake of clarity, the insurability of financial penalties provided for by this law or the GDPR.

A report of the French Treasury from September 2022 on the development of cyber insurance further suggested to include in the French Insurance Code a general principle of non-insurability of administrative fines (through an amendment of Article L. 113-1).

75. N.M. Brouwer, De Cyberverzekering vanuit civielrechtelijk perspectief, p. 102.
76. N.M. Brouwer, De Cyberverzekering vanuit civielrechtelijk perspectief, p. 103.
77. J.K. Stam & W.C.T. Weterings, '(On)verzekerbaarheid van boetes', AV&S 2022/3, par. 4.3.2.
78. N.M. Brouwer, De Cyberverzekering vanuit civielrechtelijk perspectief, p. 103; J.K. Stam & W.C.T. Weterings, '(On)verzekerbaarheid van boetes', AV&S 2022/33, par. 4.3.2.
79. Art. 7:952 DCC.
80. HR 30 May 1975, ECLI:NL:HR:1975:AC5594.
81. Idem.

In light of the foregoing, it can be concluded with reasonable certainty that Cyber Fines are not insurable (it being specified that defence costs and, more generally, experts' fees incurred by the insured party or required in the context of a CNIL investigation could in principle be insurable).

Distinction Between Cyber Insurance Covering and Effective Indemnification

Although insurance policies often state that administrative sanctions are covered “to the extent insurable”, French statutory and case law does not allow a clear delineation between insurable and non-insurable sanctions.

At this stage, there seems to be a blanket prohibition on the insurability of administrative monetary penalties, including Cyber Fines (see above), while non-monetary sanctions — such as corrective measures — may be insurable (see response to Question 4).

Switzerland

Under Swiss law, the subject matter of an insurance may only be an insurable interest of the policy holder or of a third party.[82] As a principle, criminal fines or any fines with a punitive nature are not insurable under Swiss law as they are not considered to be compensable damages. The Federal Supreme Court of Switzerland has held that a contractual agreement that obliges a third party to pay a criminal fine in whole or in part is unlawful under Swiss law and therefore void.[83]

In this regard, the Federal Supreme Court has also held that it does not distinguish whether a third party covers such fines directly or indemnifies for such fines.[84] Some legal scholars are even of the opinion that payment of a fine by a third party qualifies as assisting an offender in the sense of the Swiss Criminal Code (SCC), which is however negated by prevailing doctrine.[85]

82. Article 16 para. 1 Insurance Policies Act.
83. Article 20 para. 1 Code of Obligations; decision of the Swiss Federal Supreme Court 134 III 59.
84. Decision of the Swiss Federal Supreme Court 5A_378/2015 dated 15 March 2016.
85. Article 305 SCC.

3

Have There Been any Recent, Noteworthy Cyber Fines?

Chapter Summary

Recent years have seen examples of significant fines being imposed for cyber incidents. We have also seen the increasing assertiveness of regulators, the use of both monetary and non-monetary sanctions and the trend towards publicising enforcement actions to enhance deterrence. There has also been a growing focus on sector-specific enforcement, particularly in financial services and healthcare.

Data protection authorities have imposed multi-million Euro fines on major technology, energy and financial companies for failures in data security, breach notification and organisational measures.

Many have been initiated through enforcement of GDPR. Notable cases include Meta's EUR 251M fine in Ireland, Enel Energia's EUR 79.1M penalty in Italy, significant sanctions against energy and telecoms firms in Spain and France and Capita's GBP 14M fine in the UK, reduced from an initial GBP 45M.

Outside the EU, South Africa's Information Regulator has begun imposing fines for non-compliance with data protection obligations, while Saudi Arabia's telecom regulator has levied substantial penalties for network security failures.

The fines levied are often linked to failures in access controls, breach notification, inadequate security measures, or repeat offences.

The pattern is consistent: authorities test for foundational controls, timely and complete notifications and security/design by default. There is an expectation that new frameworks such as NIS2, DORA and the AI Act will drive further increases in both the frequency and severity of cyber fines.

Practical Actions for Organisations to Consider Now

- Create a breach casebook: Compile summaries of major fines and enforcement actions that others have experienced to inform your internal risk assessments and identify common compliance failures in your sector.
- Benchmark your organisation's security controls against those cited in enforcement cases.
- Review your breach notification protocols: ensure you can meet the 72-hour GDPR deadlines with automated alerts and escalation paths.
- Conduct post-mortems on incidents: analyse internal breaches and near misses to identify gaps in your controls.
- Use case studies as training material: incorporate real-world cases into staff awareness programmes.

Belgium

To date, only a very limited number of Cyber Fines have been imposed in Belgium, and only by the BDPA under the GDPR. To our knowledge, no noteworthy Cyber Fines have been imposed yet under cyber-specific or sector-specific laws and regulations, such as the NIS2 Act or DORA.

In a decision dated 26 April 2021, the BDPA imposed an administrative fine of EUR100,000 on a financial institution for failing to implement proper access controls and logging mechanisms. The case involved unauthorised access to sensitive financial data in the Central Credit Register operated by the Belgian National Bank. The institution allowed multiple managers to access the system using a shared password, without any logging to track individual access. This was deemed a blatant violation of Article 32 of the GDPR, which requires appropriate technical and organisational measures to ensure data security. In determining the amount of the administrative fine, the BDPA considered not only the undertaking's turnover but a series of aggravating circumstances: the intrinsically sensitive nature of the financial data, the lengthy duration of the unlawful processing, the frequency of the illegitimate access events, the institution's minimal remedial action following discovery of the breach, and the significant likelihood of continued unlawful processing had the complaint not been lodged.[86]

In a decision dated 17 December 2024, the BDPA imposed an administrative fine of EUR200,000 on a Belgian hospital following a serious cybersecurity incident.[87] In 2021, the hospital experienced a ransomware attack that disrupted essential medical services and compromised the personal data of approximately 300,000 individuals. This incident marked the hospital's second major breach, following a similar attack in 2019. After investigating the cyber incident, the BDPA found that the hospital had failed to implement sufficient cybersecurity and data protection measures. The fine was determined based on the severity, duration, and impact of the violations, as well as the hospital's efforts to mitigate harm. The BDPA emphasised that organisations must conduct thorough data protection impact assessments (**DPIA**), maintain a coherent and up-to-date information security policy, and implement robust technical security measures such as staff training, effective logging, regular cybersecurity audits, and strong authentication protocols. This case underscores the BDPA's readiness to sanction organisations for inadequate cybersecurity and highlights the active duty to adopt preventive, sector-specific security measures under the GDPR. Although the EUR200,000 Cyber Fine is one of the highest to be imposed in Belgium, it remains relatively low compared to the maximum fines that can be imposed under the GDPR.

86. gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-56-2021.pdf.
87. autoriteprotectiondonnees.be/publications/beslissing-ten-gronde-nr.-166-2024.pdf.

Luxembourg

In Luxembourg, recent cyber related fines have predominantly originated from data protection breaches under the GDPR. Based on Luxembourg's data protection authority's (the **CNPD**) annual reports and individual decisions published on its official website, the CNPD does not issue a high volume of fines under the GDPR, often opting instead for other corrective measures. Most of the decisions are not related to data breach or cyber incident, but to general data protection compliance.

The *Institut Luxembourgeois de Régulation* (**ILR**) can fine operators of essential services and digital service providers for breaches under the NIS2 framework but has yet to publish any monetary sanctions. The CSSF can also imposes administrative penalties for financial entities under DORA. The CSSF has indicated informally that enforcement will begin in 2026.

Portugal

The most prominent fine in recent years was imposed on Portugal's National Institute of Statistics (INE), which received a EUR4.3M penalty from the CNPD for multiple GDPR violations. Although these breaches were related to inadequate storage and handling of personal data during the national census (rather than a typical "cyber incident" like hacking or ransomware) the case remains one of the most high-profile privacy and data protection sanctions seen in Portugal in recent years.

The lack of high-profile cases is largely due to delays of the Portuguese legislator in implementing the European legislative package. Indeed, all current regulations and sanctioning frameworks remain substantially limited when compared to those set out in the new instruments.

For example, the maximum penalties provided under Law 46/2018, which transposed the first NIS Directive (NIS1), are capped at EUR50,000, a figure dramatically lower than the sanctioning thresholds now set by NIS2. The latter, following a similar system to the one established by the GDPR, provides for maximum fines of EUR10M or 2 percent of the total worldwide annual turnover of the preceding financial year of the undertaking, whichever is higher.

Looking ahead, the regulatory landscape is set to shift considerably, as new frameworks come into force. The combination of updated national laws transposing NIS2 (such as Draft Law No. 7/XVII), alongside DORA, the Cyber Resilience Act, and the GDPR, is expected to create a significantly more robust enforcement environment for both cybersecurity and privacy compliance.

Finland

To date, there has only been one notable Cyber Fine in Finland relating to a data breach. In summary, the case involved Vastaamo, a psychotherapy centre whose patient record database was attacked and the data was downloaded. The hacker then used these records to extort Bitcoin from Vastaamo and, subsequently, from individual patients before leaking the data online.

The Data Protection Ombudsman imposed an administrative fine of EUR608,000 on Vastaamo for violating the GDPR's requirements, as it found that the company had neglected its duties relating to the secure processing of personal data and failed to report the data breach. However, the decision has been appealed and is not yet final. Criminal proceedings relating to the case are also still ongoing.

In addition to the Vastaamo case, a few other major cyber incidents have received news coverage in Finland. For example, Finland's largest cyber incident occurred in spring 2024 when the City of Helsinki Education Division was targeted in a data breach, resulting in the exposure of the personal data of around 300,000 individuals, including school children.

This case was significant because an independent investigation group under the Finnish Safety Investigation Authority was commissioned by the Finnish government to investigate the breach. The investigation was deemed necessary as the breach was an exceptional event that threatened or seriously damaged the basic functions of society.

However, the Data Protection Ombudsman's investigation into this data breach is ongoing, so it is unclear whether the City of Helsinki will be issued with administrative fines.

South Africa

In July 2023, the Information Regulator imposed a ZAR 5M administrative fine on the Department of Justice and Constitutional Development (DoJ) following a major cyberattack in September 2021, which led to the encryption of internal documents, loss of over 1,200 files, and compromise of personal information.

The Information Regulator's investigation revealed that the DoJ had failed to maintain adequate cybersecurity measures, including allowing key antivirus and monitoring licences to expire. An enforcement notice was issued, requiring the DoJ to take remedial action within a specified timeframe. The DoJ failed to comply with the enforcement notice, whereafter the fine was imposed.

To the best of our knowledge, the only other fine the Information Regulator has sought to impose to date was in respect of the Department of Basic Education (DBE) in December 2024, also in an amount of ZAR 5M, and also following the DBE's failure to comply with an enforcement notice. The enforcement notice in question prohibited the DBE from publishing the results of the 2024 school matriculants in the national newspapers.

Notwithstanding the approach taken by the Information Regulator to date, we expect to see an increase in administrative fines if other remedial measures prove to be ineffective in practice.

Aside from cyber related fines, the Bellville Specialised Commercial Crimes Court recently sentenced Mr Lucky Majangandile Erasmus to eight years in prison, with three years suspended, following a cyberattack on Ecentric Payment Systems in December 2023. Erasmus, along with a co-accused, installed unauthorised remote access software on Ecentric's systems, enabling the theft of sensitive data, manipulation of access credentials, and attempts to extort the company through threats of public disclosure. The attack led to losses for four of Ecentric's retail clients. Whilst ransom demands were made, they were not paid. Erasmus entered into a plea agreement and was convicted on 17 charges, including data theft, attempted cyber extortion and cyber fraud.

Italy

Recent Fines Imposed by the Italian Data Protection Authority:

Autostrade Per L'italia S.p.a.

In July 2025, the Garante imposed fines of EUR420,000 on Autostrade per l'Italia S.p.A. for the unlawful use of an employee's personal data. The company used information from the employee's social media profiles and private chats to justify her dismissal, violating personal data privacy regulations. Specifically, the Authority found that Autostrade per l'Italia had illegally processed the employee's personal data, acquiring and using content from her Facebook profile and private chats on Messenger and WhatsApp to justify disciplinary proceedings against her and her subsequent dismissal.

INAIL (National Institute for Insurance Against Accidents at Work)

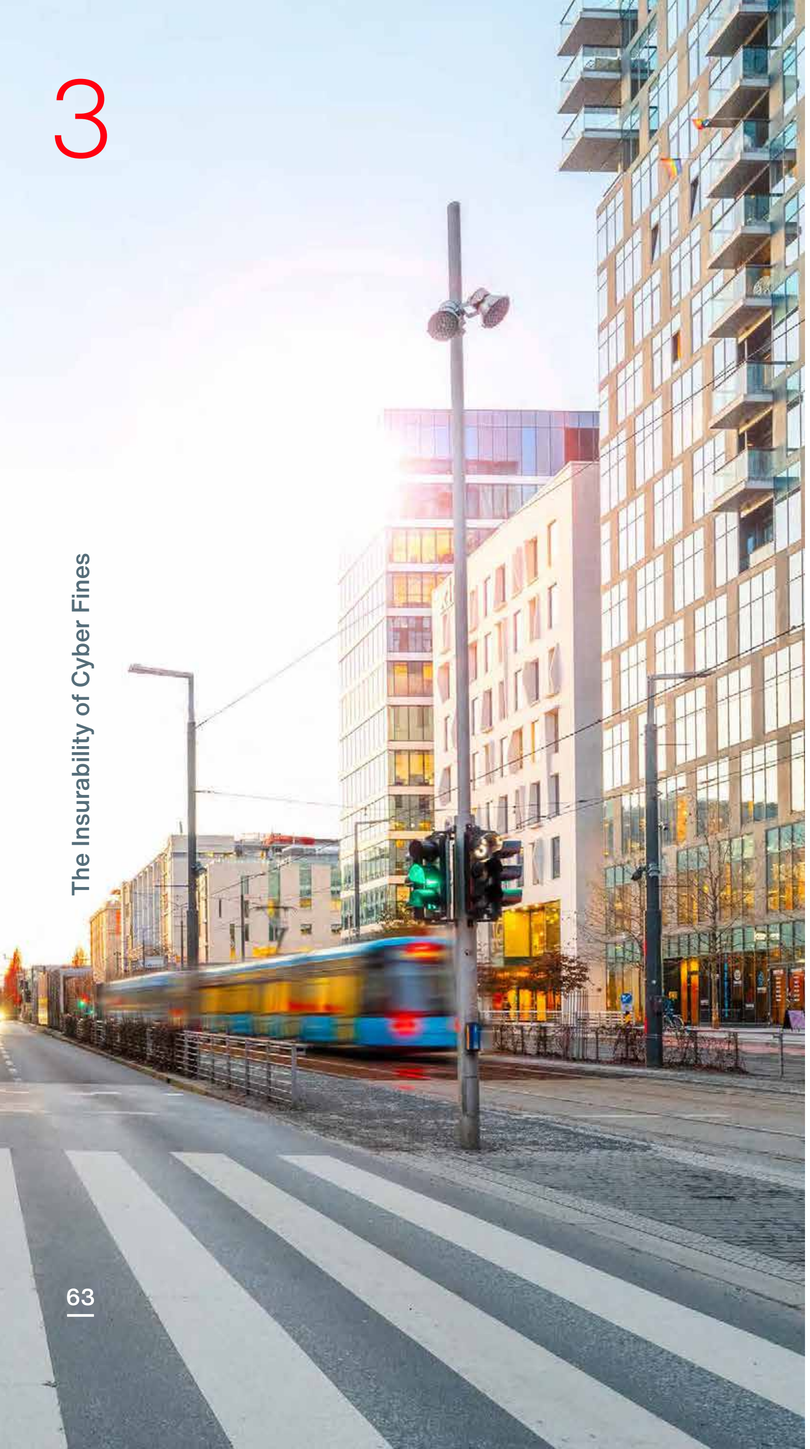
In 2025, INAIL was fined EUR50,000 following a data breach that resulted in unauthorised access to sensitive health and occupational accident data of employees for a malfunction in the IT system. The breach was attributed to inadequate technical and organisational measures, and the authority emphasised the need for public bodies processing sensitive data to maintain high standards of confidentiality and system integrity.

Enel Energia Spa

In February 2024, Enel Energia, a major electricity provider, received the highest fine ever issued in Italy, EUR79.1M, for violations of the GDPR. The penalty was imposed for failure to adopt adequate security measures to protect customers data, which led to the unlawful processing of such data for telemarketing purposes.

Unicredit

In March 2024, the Garante fined UniCredit EUR2.8M following a 2018 data breach that exposed the personal data (names, tax codes, internal bank IDs) of around 800,000 customers. The investigation found that UniCredit, as the data controller, failed to implement adequate technical and organisational measures to ensure data security, violating Article 32 of the GDPR.



Saudi Arabia

As stated above, one of the largest publicised “cyber” enforcement actions to date was in January 2021, whilst the CST announced fines totalling SAR 40m (roughly USD10.7m) against major telecom operators. The penalties targeted Saudi Telecom (STC), Mobily, Zain, and others. According to new reports, STC alone was fined SAR31m while Mobily, Zain, and Lebara Mobile were fined lesser amounts (around SAR 1 million each, and a few million combined for other violations). The fines were imposed for various violations of telecom regulations, some of which relate to cybersecurity or misuse of networks. The CST indicated the violations included: sending unsolicited spam messages, using frequencies without a licence, failure to comply with CITC directives on resolving user complaints, misuse of pre-registered SIM cards, providing SMS services without authorisation, and even an incident of damage to a network (cutting a communication cable).

Under the ECL, in 2022, the Ministry of Commerce announced it had penalise a number of e-stores for violations like failing to adhere to data security requirements, engaging in deceptive practices, etc. The fines in those cases were on the order of tens or hundreds of thousands of riyals (not millions) and some offending websites were blocked. Ministry of Commerce blocks seven e-stores for violating consumer rights and E-Commerce Law.

Unfortunately, as also said above, KSA is not a case-publication jurisdiction and does not operate a binding precedent system; accordingly, the above two incidents are primarily taken from prominent newsletters/official governmental announcements rather than reported case law.

Norway

Most recent Cyber Fines have been imposed by the Norwegian Data Protection Authority, for GDPR contraventions.

The largest fine imposed to date was NOK 65M (approx. EUR5.7M) directed at Grindr LLC for having disclosed personal data without legal grounds, violating Article 6(1) and 9(2) GDPR. The decision to impose the fine is currently being tried by the Court of Appeals.

Another prominent case concerns the DPA's fine of NOK 20M issued to the Norwegian Labour and Welfare Administration (NAV) for breaches of IT security and data protection regulations. The case attracted considerable media attention in Norway, and NAV appealed the DPA's decision to the Privacy Appeals Board, which overturned the DPA's decision.

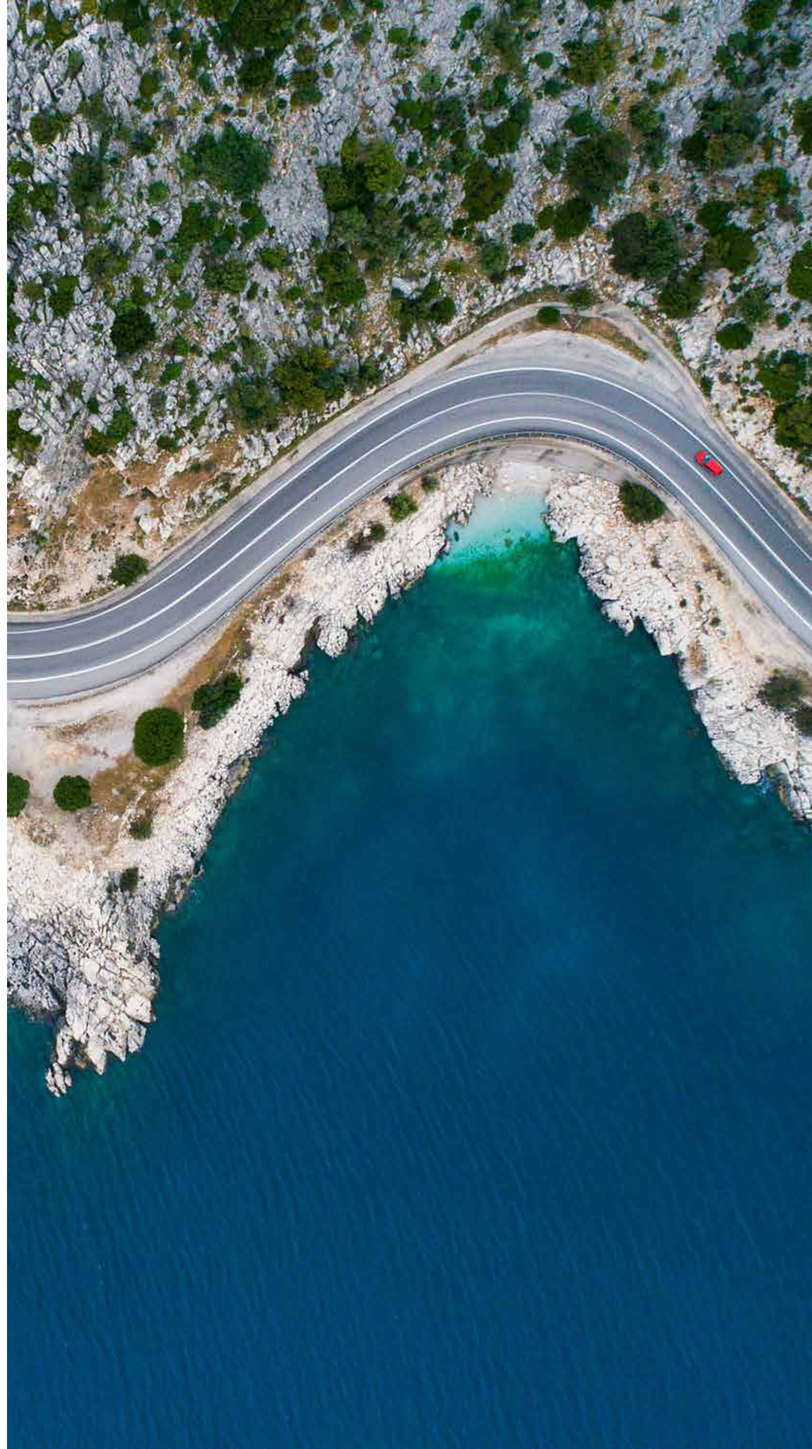
Turkey

Please find some recent noteworthy administrative fines issued by the Personal Data Protection Board below:

- The Personal Data Protection Board imposed an administrative fine of TRY2m (approx. USD48,970.40) on the social media platform Twitch due to a data breach. The investigation revealed that the data controller had failed to exercise due diligence in implementing configurations to address the problems in its system. It was also identified that the necessary security measures that should have been taken prior to the occurrence of the breach were implemented only after the incident (16 November 2024).
- The Personal Data Protection Board imposed an administrative fine of TRY1.45m (approx. USD35,503.54) on the social media platform X (formerly Twitter) for violating provisions related to data security. The Personal Data Protection Board determined that the processing of personal data obtained for the purpose of advertising activities was in breach of the principles of “lawfulness and fairness” and “being relevant, limited and proportionate to the purposed for which they are processed” (14 November 2024).
- The Personal Data Protection Board imposed an administrative fine of TRY1.1m (approx. USD26,933.72) on Marriott International Inc for failing to take the necessary technical and administrative measures to ensure data security, as required under the Data Protection Law (16 May 2019).

Sweden

The Swedish Authority for Privacy Protection (IMY) imposed significant administrative fines on Apoteket AB (SEK 37M) and Apohem AB (SEK 8M) following GDPR violations, specifically for processing personal data in breach of Article 32(1) of the GDPR. The companies used Meta’s analytics tool, Meta Pixel, on their websites, which resulted in the unauthorised transfer of sensitive personal data related to customers’ health-related purchases to Meta. IMY found that the companies had failed to implement appropriate technical and organisational measures to safeguard the data, causing the improper data transfers to continue for an extended period. The incidents were reported to IMY in 2022, and the companies have since improved their internal data protection procedures.



Poland

Morele.net Sp. Z o.o. — Originally Fined in 2019 and Subsequently Issued with a Replacement Fine of PLN 3.8M (Approx EUR883,720) in February 2024

Morele.net Sp. z o.o. (**Morele**) is one of the companies operating on the Polish e-commerce market. In Q4 2018, the company was a victim to two hacker attacks which resulted in compromising database and personal data of approximately 2,200,000 customers. UODO decided that the security measures implemented by the company were insufficient which resulted in an unauthorised access to the database. While calculating the fine, UODO primarily considered the number of affected individuals and the fact that although the company declared ongoing monitoring of its systems, it did not take any countermeasures to prevent the breach.[88] Morele appealed the decision. The Supreme Administrative Court overturned the UODO's decision in 2023 as it questioned the UODO's competence to assess the technical and organisational measures used by Morele to secure personal data. According to the court, the UODO must prove that it has the requisite knowledge to conduct such security analysis and, as a minimum, create an internal document setting out its conclusions. As a result, the UODO re-examined the case and created such a document of its findings which included the company not encrypting some data, not having two-factor authentication, not carrying out a risk analysis and not having technical and administrative solutions to monitor network traffic (which resulted in the company not being sure whether data had been stolen). The UODO's view was that if it had put in place the right solutions then it would have been able to detect unauthorised access attempts and taken actions to prevent the data theft. The company admitted its failings in this regard. As a result the UODO issued a fine of more than PLN 3.8M (approx EUR 883,720). This is the first time that the EDPB guidelines were used to determine the amount of the fine.[89] On 16 September 2024, the Provincial Administrative Court dismissed Morele.net's complaint against this decision of the UODO.[90]

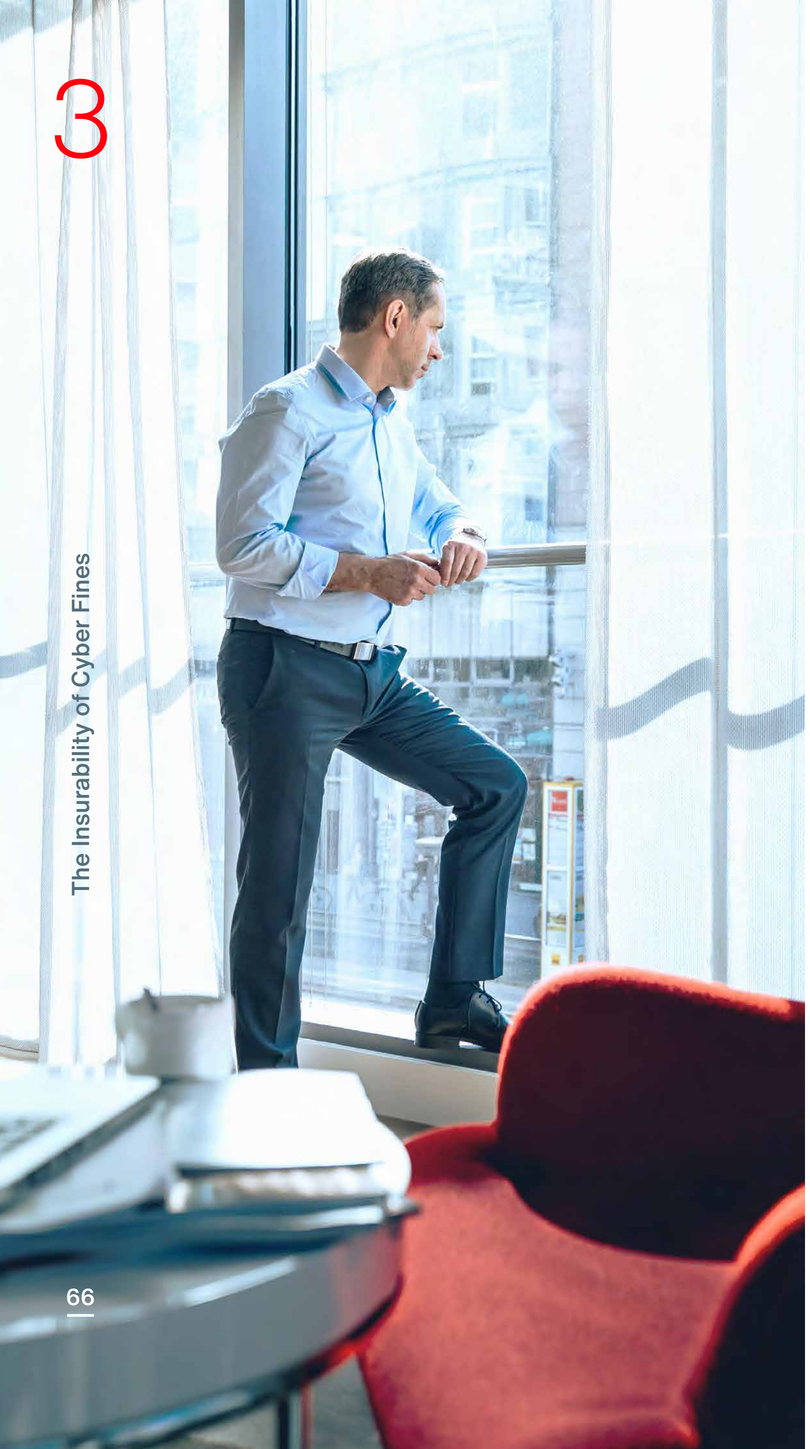
Fortum Marketing and Sales Polska S.A. — 19 January 2022, a Fine of PLN 4.9M (EUR 1M)

Fortum Marketing and Sales Polska S.A. (Fortum) deals with the supply of heat and electricity. GDPR infringement proceedings were initiated after a personal data breach was reported. According to the UODO, a data protection breach consisted in copying the data of the administrator's clients by unauthorised persons. This happened when a change was introduced in the ICT environment. In the contract concluded with the third party service provider, the company specified the personal data security requirements that should be applied by the data processor, e.g., pseudonymisationand encryption of personal data, however, the functioning of these safeguards has not been tested by the contractor before transferring IT system to the company. Such check was also not performed by the data controller. Fortum did not enforce the performance of the data processing agreement, did not comply with its own practice of implementing changes in the IT environment based on internal regulations and did not verify the processor's activities aimed at improving the functioning of the service. Thus, the company was punished with a fine of PLN 4.9M (EUR 1.5M) for the failure to implement appropriate technical and organisational measures to ensure the security of personal data and failure to verify the processing entity.[91] The decision is not final as it has been appealed to the Provincial Administrative Court.

Virgin Mobile Polska — 14 December 2019, a Fine of PLN 1.2M (EUR 457,797)

Virgin Mobile Polska Sp.z.o.o is a provider of mobile phone services. In December 2019, the company notified UODO that an unauthorised person had obtained access to personal data of over 114,000 customers, including name, PESEL identification number, series and number of ID card, tax identification number and telephone number. UODO decided that the company did not comply with the GDPR security

88. UODO's decision ZSPR.421.2.2019, available at uodo.gov.pl/decyzje/ZSPR.421.2.2019.
89. uodo.gov.pl/pl/138/2983.
90. uodo.gov.pl/pl/138/3362.
91. UODO's decision DKN.5130.2215.2020, available at uodo.gov.pl/decyzje/DKN.5130.2215.2020.



requirements because it did not carry out regular and comprehensive evaluation of the effectiveness of its security measures, but only responded to emerging suspicions of a vulnerability or in connection with organisational changes. Not tests were carried out to test the security of transfer of data between applications (i.e to test if a user verification step worked), and a vulnerability in this data exchange enabled an unauthorised person to obtain customer data.

When calculating the fine, UODO considered that the breach was serious as it posed a high risk for a large number of people (e.g., risk of identity theft), that the vulnerability had existed for a long time and the deterrent effect of a large fine. UODO also took account of the good co-operation by the company, quick remedy of the breach after its detection and implementation of additional measures to increase data security.[92] The decision is not final as it has been appealed to the Provincial Administrative Court.

Panek SA — December 2024, a Fine of PLN 15M (EUR 362,886)

Panek SA was fined for failing to put in place appropriate technical and organisational measures to secure the data it was processing. Whilst Panek's website was being reconstructed, Panek did not communicate properly with its processor which led to customer data being made available on its website. Approximately 21,453 people's data was affected by the breach. The IT centre that Panek used as its Processor was also fined PLN 20,037.[93] The decision is not final as it has been appealed to the Provincial Administrative Court.

American Heart of Poland — 20 May 2024, a Fine of PLN 1.4M (EUR 328,337)

American Heart of Poland was fined for a hacking incident and a resulting data breach which affected 21,000 patients and employees. The incident covered a wide range of data, i.e.,: surname, first name, parents' names, mother's maiden name, date of birth, data on earnings or property, health data, bank account number, address of residence or stay, PESEL number, username or password, series and number of ID card, telephone number and e-mail address. The company learned of the data leak from hackers who demanded a ransom of USD3m for not disclosing the intercepted data. The company notified the UODO about the incident, and the people whose data had been leaked were informed of the threat associated with the incident. Following its investigation, the UODO criticisedthe company for security failures that led to the incident. The UODO also ordered the company to improve the way it processes data and set a deadline of 30 days for it to conduct a proper risk analysis for the processes of data processing by it and to implement on this basis appropriate technical and organisational measures to ensure data security. Going forward, the company must also implement the

92. UODO's decision DKN.5112.1.2020, available at uodo.gov.pl/decyzje/DKN.5112.1.2020.
93. UODO's decision DKN.5130.2415.2020, available at uodo.gov.pl/decyzje/DKN.5130.2415.2020.

principles of regular verification of the effectiveness of the adopted measures.[94] The decision is not final as it has been appealed to the Provincial Administrative Court.

ID Finance Poland — 17 December 2020, a fine of PLN 1M (EUR 248,802)

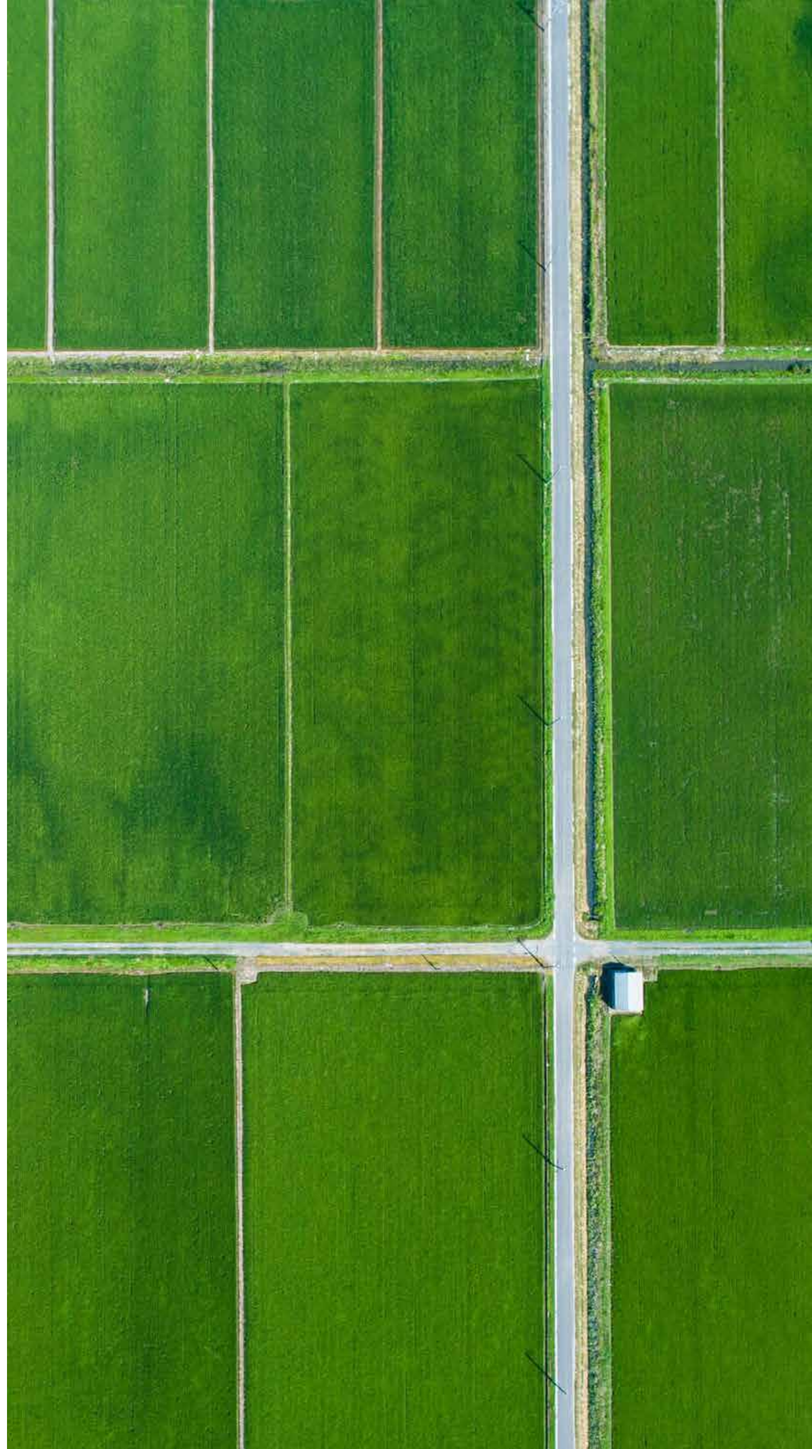
ID Finance Poland, owner of the MoneyMay.pl loan portal, was fined for lack of appropriate security measures. Security measures have not been restored after a processor's server was re-started; the controller did not respond to initial warnings of the vulnerability and an unauthorised person copied data and deleted it from the server, demanding a ransom for its return.[95] The UODO's decision has been repealed by the Provincial Administrative Court in Warsaw in 2022. The court decision has been appealed by the UODO to the Supreme Administrative Court, and the proceedings are ongoing.

England and Wales

There have been three particularly significant Cyber Fines in 2025, handed down by the ICO under the UK GDPR:

- Advanced Computer Software Limited — GBP 3.07M following a ransomware attack in August 2022 against Advanced's health and care subsidiary. Various failings were found, including absence of MFA on the account used to gain access, as well as weaknesses in access controls and Advanced's broader security posture. Notably, Advanced was acting as a processor in relation to the personal data, not as a controller. The fine was reduced from GBP 6.09M after Advanced made representations and agreed to a settlement.
- Capita (Capita plc and Capita Pension Solutions Ltd) — GBP 14M following a ransomware attack in March 2023 which led to the personal data of around 6.6 million people being compromised. Key security failings included delayed containment, inadequate privilege management and insufficient penetration testing. The fine was reduced from GBP 45M after Capita made representations and agreed to a settlement.
- LastPass UK - GBP 1.2M following a 2022 data breach that compromised the personal data of up to 1.6m of its UK users. Failures including the ability to access corporate accounts from personal devices, and a policy which permitted employees to link their personal and business accounts with a single master password, were found to have enabled a hacker to access a backup database.

94. UODO's decision DKN.5112.35.2021, available at uodo.gov.pl/decyzje/DKN.5112.35.2021.
95. UODO's decision DKN.5130.1354.2020, available at uodo.gov.pl/decyzje/DKN.5130.1354.2020.



Ireland

On 17 December 2024, the DPC fined Meta Platforms Ireland Limited (**MPIL**) EUR251M regarding a data breach which occurred as a result of unauthorised third parties exploiting user tokens on Facebook. The breach impacted approximately 29 million Facebook accounts globally, about 3 million of which were based in the EU/EEA. There were various categories of personal data affected, including the users' name, email address, phone number, place of work, gender and date of birth. MPIL reported the personal data breach in September 2018. The decisions to impose the administrative fines came following two inquiries by the DPC.

When commenting on the decisions and the fine, DPC Deputy Commissioner Mr Graham Doyle noted that there were failures by MPIL to build in data protection requirements throughout the design and development cycle, which exposed individuals to risks to their fundamental rights and freedoms.

The total fine of EUR251M is broken down as follows:

- Article 33(3) of the GDPR was breached as MPIL did not include sufficient information in its breach notification. MPIL was reprimanded and fined EUR8M;
- Article 33(5) of the GDPR was breached as MPIL failed to create a documentary record of the facts relating to each breach. MPIL was reprimanded and fined EUR3M;
- Article 25(1) of the GDPR was breached as MPIL did not ensure data protection standards were met in the design of processing systems. MPIL was reprimanded and fined EUR130M; and
- Article 25(2) of the GDPR was breached as the tokens deployed by MPIL gave unnecessarily broad access to the personal data of Facebook users. MPIL therefore failed to ensure that only personal data that was necessary for specific purposes was processed. MPIL was reprimanded and fined EUR110M.

Other fines which are notable for their size and the fact that they were imposed on technology companies, but which do not relate directly to third party cyber breaches include the following:

- On 2 May 2025, the DPC fined TikTok EUR530M following an inquiry into transfers of user data to China. The decision also included an order requiring TikTok to bring its processing into compliance with the GDPR within six months.
- On 24 October 2024, the DPC fined LinkedIn EUR310M for insufficient legal basis for data processing. The decision also included an order requiring LinkedIn to bring its processing into compliance with the GDPR within six months.
- On 27 September 2024, the DPC fined MPIL EUR91M for insufficient technical and organisational measures to ensure information security. MPIL had been storing the passwords of users as plaintext.
- On 1 September 2023, the DPC fined TikTok EUR 345M for not properly considering the privacy of under-13s on the platform. The decision also included an order requiring TikTok to bring its processing into compliance by taking the action specified within a period of three months.
- On 12 May 2023, the DPC fined MPIL EUR1.2B for insufficient legal basis for data processing. The transfers of personal data to the U.S. were considered to be systemic, repetitive and continuous. This is the largest fine ever imposed under the GDPR. The decision also included an order requiring MPIL to suspend future transfers of personal data to the U.S. within five months.

UAE

The DIFC Commissioner publishes decisions of the administrative fines issued each year. The Office of Data Protection also maintains a database of regulatory actions under the DPRs. We are however not aware of any noteworthy Cyber Fines to date. This may change once the PDPL becomes fully enforceable, however.

Germany

In June 2025, the Federal Data Protection Authority imposed a total fine of EUR45M on Vodafone. Of this amount, EUR15M were issued for violations related to processor management, and EUR30M for insufficient security measures that had enabled unauthorised access to eSIM profiles (Article 32 GDPR).[96]

In December 2024, the DPA of Hesse imposed a fine of EUR496,000 to a financial company for delayed information of data subjects on a cyber incident (Article 34 GDPR) — the public information indicates the fine was also imposed for unsolicited marketing, while the split is unclear.[97] Please note that a simultaneously discovered use of data without legal basis is included in this fine.

In August 2023, the DPA of Saarland imposed a EUR200,000 fine to an insurance company after a security gap caused a leak of sensitive information in August 2023.

Spain

Enforcement in Spain (particularly based on sanctions imposed by the AEPD) draws a clear pattern of high-impact GDPR sanctions for security-of-processing, confidentiality and privacy/security-by-design failures.

In December 2023, the AEPD imposed a total of EUR6.1M in fines on an energy company. The decision sanctioned security-of-processing and confidentiality breaches and notification failures following exposure of credentials and large volumes of customer data, coupled with deficiencies such as the absence of multifactor authentication (MFA), insufficient session controls, and delayed deactivation of compromised accounts. The case underscores the AEPD's expectation that basic security hygiene and prompt containment are part of Article 32 compliance.

In February and April 2024, the AEPD published two decisions arising from a March 2022 cyberattack on a different energy company group's GEA portal and the group's shared database architecture. The AEPD sanctioned one of the group companies with EUR3M for breaches of Article 5(1)(f) and Article 32 GDPR tied to inadequate segregation of companies' data and insufficient preventive measures. In the companion case, the AEPD sanctioned the other group company with EUR3.5M due to confidentiality and security-of-processing breaches affecting approximately 1.35

96. Press release of DPA (German only): bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html?nn=251944
97. Activity report, p. 31: datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-05/53-tb-online.pdf (German only)

million clients. The two decisions together highlight the AEPD's willingness to articulate distinct responsibilities of a group parent acting as processor and a group company acting as controller, to reject arguments that quick post-incident response suffices for Article 32 compliance, and to treat logical separation and architecture risks as core design obligations.

In April 2024 the AEPD imposed an EUR5M sanction against financial entity for a security incident in which clients could see details of transfers made by other customers, finding violations of Article 5(1)(f), Article 25, and Article 32 GDPR. The resolution emphasised design shortcomings and reactive, rather than proactive, remediation. Separately, 2024 saw high-value sanctions across energy, financial, telecom and digital-service sectors, including multiple fines resulting in an aggregate of EUR5M for an energy company's violations of GDPR principles and accountability.

In December 2024, the AEPD imposed a fine of EUR6.5M on a telecommunications company for violating the principle of integrity and confidentiality and for failing to implement adequate security measures which led to the leak and hijacking of approximately 100 GB of personal data from up to three million customers, former customers, employees, and suppliers; which constituted a breach of Article 5(1)(f), and Article 32 GDPR.

In January 2025, the AEPD imposed a EUR4M (reduced from EUR5M) on an insurance company for violating the principle of integrity and confidentiality, failing to implement adequate security measures, not applying data protection measures by design and by default, and not carrying out a Data Protection Impact Assessment when it was required, which led to a data breach that occurred in October 2022, in which the confidential information of up to 1.6 million people, including both current and former customers of the company, was compromised. Taken together, these factors led to the determination that Articles 5(1)(f), 25, 32, and 35 of the GDPR had been infringed.

Also in January 2025, the AEPD imposed an EUR3.2M fine on a retail and supermarket company for failing to adequately protect customer data after "credential stuffing" attacks exposed sensitive information from its loyalty programme. The AEPD found that the company breached Article 5(1)(f), Article 32, and Article 34 of the GDPR by not implementing sufficient security measures and failing to properly notify affected individuals, resulting in the penalty and an order to inform impacted customers within a month.

The trend line is clear: the AEPD is actively using both principle-based and technical obligations to sanction security and design failures exposed by or associated with cyber incidents, and it is prepared to impose high-value sanctions and non-monetary corrective orders to the extent relevant/appropriate.

Netherlands

There have been some recent examples of Cyber Fines in the Netherlands.

Under the GDPR, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) (**Dutch DPA**) imposed:

- May 2021: EUR450,000 fine on the UWV (Employee Insurance Agency) for not securely sharing messages via a professional group chat.[98]
- November 2020: EUR440,000 fine on the OLVG-hospital (a hospital in Amsterdam) for not having in place appropriate access rights and controls.[99]
- July 2019: EUR460,000 fine on the Haga-hospital (a hospital in The Hague) for not having in place appropriate access rights and controls.[100]

98. See: Boete UWV beveiliging groepsberichten | Autoriteit Persoonsgegevens.
99. See: boetebesluit_olvg.pdf.
100. In court the fine was lowered to EUR 350,000. Court of Den Haag 31 March 2021, ECLI:NL:RBDHA:2021:3090.

France

The table below lists recent CNIL fines issued partly due to non-compliance with the security obligations set out by the GDPR under Article 32 and Article 33-34. However, it is not possible to attribute the amounts solely to cybersecurity or information security breaches. In most cases, the CNIL sanctions are based on several cumulative violations, and the authority does not provide a breakdown of the fine amount for each specific infringement.

Sanctions, where imposed are not published and the amounts of fines are generally not disclosed. Accordingly, to the best of our knowledge, there is no publicly available information regarding Cyber Fines issued under the Law No. 2018-133 of 26 February 2018 on various provisions adapting to European Union law in the field of security (i.e., France has so far prioritised support and compliance for essential service operators [ESOs] and digital service providers [DSPs] rather than public sanctions).

Switzerland

So far there were no noteworthy Cyber Fines imposed in Switzerland.

Date of Decision	Fine [EUR]	Controller/ Processor	Quoted Art.	Type
04/02/2025	40,000	Real Estate Company	Art. 5 (1) c) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, **Art. 32 GDPR**, Art. 35 GDPR	Non-compliance with general data processing principles
23/01/2024	32,000,000	Amazon France Logistique	Art. 5 (1) c) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, **Art. 32 GDPR**	Non-compliance with general data processing principles
12/10/2023	600,000	Groupe Canal +	Art. 7 (1) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 28 GDPR, **Art. 32 GDPR**, **Art. 33 GDPR**, Art. L. 34-5 CPCE	Insufficient fulfilment of data subjects rights
08/06/2023	150,000	KG COM	Art. 5 (1) c), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 28 GDPR, **Art. 32 GDPR**, Art. 33 GDPR, Art. 82 Loi informatique et libertés	Non-compliance with general data processing principles
08/12/2022	300,000	Free SAS	Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR, **Art. 32 GDPR**, **Art. 33 GDPR**	Insufficient fulfilment of data subjects rights
10/11/2022	800,000	Discord Inc.	Art. 5 (1) e) GDPR, Art. 13 GDPR, Art. 25 (2) GDPR, **Art. 32 GDPR**, Art. 35 GDPR	Non-compliance with general data processing principles
13/09/2022	250,000	GIE Infogreffe	Art. 5 (1) e) GDPR, **Art. 32 GDPR**	Insufficient technical and organisational measures to ensure information security
19/08/2022	600,000	Accor SA	Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 21 GDPR, **Art. 32 GDPR**, L. 34-5 CPCE	Insufficient fulfilment of data subjects rights
15/04/2022	1,500,000	Dedalus Biologie	Art. 28 GDPR, Art. 29 GDPR, **Art. 32 GDPR**	Insufficient technical and organisational measures to ensure information security
28/12/2021	300,000	Free Mobile	Art. 12 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. 25 GDPR, **Art. 32 GDPR**	Insufficient fulfilment of data subjects rights

4

What Other Regulatory Penalties Arise From Cyber Incidents, and are they Insurable?

Are there other regulatory penalties which organisations may face, arising from cyber incidents? Is it possible to insure against those penalties and their financial consequences?

Chapter Summary

Beyond monetary fines, organisations now face a range of additional regulatory penalties arising from cyber incidents. These include corrective orders, operational suspensions, management bans, mandatory audits and public warnings.

Regulators can deploy a wide toolbox of penalties beyond monetary sanctions. Beyond those mentioned above, they can also include binding instructions, orders to cease processing, publication of decisions, licence/authorisation suspensions or withdrawals and periodic penalty payments for non-compliance.

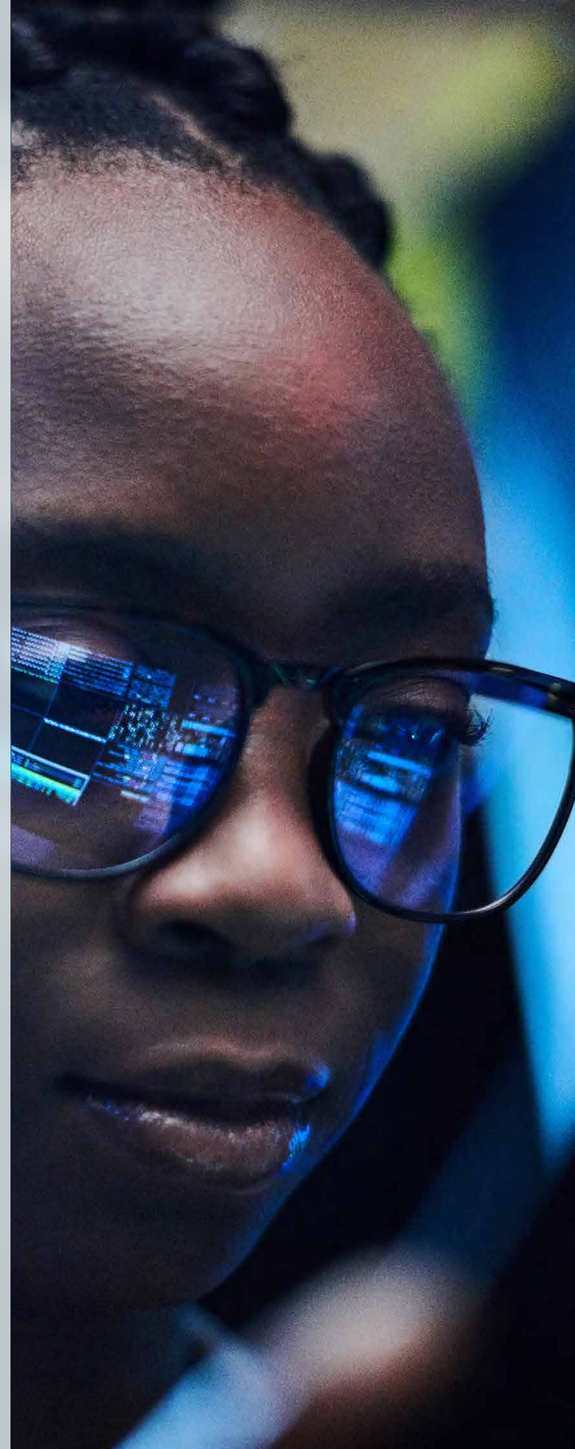
Such non-monetary sanctions can have significant operational and reputational consequences, disrupting business continuity and damaging stakeholder trust.

While direct indemnification for non-monetary sanctions like these is not possible, insurance may — in certain cases — cover the financial consequences, such as business interruption losses or the costs of implementing remedial measures.

Robust incident response planning, contractual clarity with service providers and proactive engagement with regulators are important factors in mitigating the impact of non-monetary penalties. Organisations need to understand the interplay between different regulatory regimes, as overlapping obligations under GDPR, NIS2, DORA and sectoral laws can lead to cumulative enforcement actions.

Practical Actions for Organisations to Consider Now

- Prepare for non-monetary sanctions: develop plans for business continuity, legal defence and reputation management in the event of regulators' penalties.
- Rehearse your responses to supervisory requests, such as document dumps, onsite inspections, or mandated audits — and ensure your playbook is ready to activate.
- Develop a regulatory engagement plan: prepare for audits, interviews and document requests.
- Include regulatory compliance in contracts: ensure your service providers and partners are contractually obliged to meet cybersecurity standards and participate in incident responses.



Belgium

Under the GDPR, the BDPA can impose a range of administrative and corrective measures (non-financial penalties), including:

- Warnings and reprimands for non-compliant behaviour.
- Orders to comply with data subject rights, to provide necessary information to data subjects, or to bring processing activities into compliance.
- Suspension, restriction, or prohibition, either temporary or permanent, of specific data processing activities, subject to further penalties if violated.
- Publication of enforcement decisions on the BDPA's website in non-anonymised form, thereby publicly identifying the responsible entity.[101]

Under the NIS2 Act, the CCB and the sectoral authorities upon the CCB's approval, can impose a range of non-financial penalties on essential and important entities, including:

- Orders to cease non-compliant conduct.
- Binding instructions to implement specific cybersecurity measures.
- Temporary or permanent suspension or withdrawal of authorisations or certifications to provide services in critical sectors.
- Temporary bans on individuals from holding management positions in essential entities in cases of repeated or serious violations.
- Mandatory implementation of audit recommendations.
- Publish decisions or sanctions, including the identification of the non-compliant entity and the nature of the breach.[102]

Under DORA, the NBB and FSMA can impose a range of non-financial penalties on financial entities, including:

- Issuing orders requiring natural or legal person to cease non-compliant conduct and refrain from repeating such behaviour.
- Mandating the temporary or permanent cessation of practices deemed contrary to the Regulation, with the aim of preventing recurrence.
- Adopting corrective measures, including those of a pecuniary nature, to ensure continued compliance by financial entities.
- Requesting, where permitted under national law, access to existing data traffic records held by telecommunications operators, provided there is a reasonable suspicion of a breach and the records are relevant to the investigation.
- Issuing public notices, including the identification of the non-compliant entity and the nature of the breach.[103]

In principle yes, as the non-insurability of criminal fines under Belgian law only extends to the fine itself, not to other penalties or financial consequences of any conviction. However, depending on the circumstances, such insurability may be challenged nonetheless.

Luxembourg

Under the GDPR, DORA and NIS2, sanctions extend beyond monetary fines:

Under the GDPR, the CNPD may issue orders to cease unlawful data processing, enforce compliance with specific obligations (Article 58[2][d], [f]), or suspend data flows to third countries (Article 58[2][j]). The CNPD frequently applies Article 58(2)(c) to compel controllers or processors to comply with data subject requests and on Article 58(2)(d) to require that processing operations be brought into compliance within a fixed deadline. Common corrective measures include updating the privacy policy to cover location data, improving the communication of policy changes, or adding a link to the policy at data collection points.

In certain cases, the Law of 2015, allows for criminal penalties including imprisonment of up to one year may apply. As a matter of example see Article 4(4) and Article 5(6). The CNPD may also impose periodic penalty payments (astreinte) of up to 5 percent of the average daily turnover for non-compliance with requests for

101. Article 58 GDPR; Article 221 Belgian Data Protection Act.
102. Article 58 and 60 NIS2 Act.
103. Article 50 (4) DORA.

information or failure to implement a corrective measure ordered by the CNPD pursuant to Article 58(2)(i) and 83 of the GDPR. This enforcement mechanism may be applied in addition to, or in place of, other administrative fines to ensure compliance.

With respect to DORA enforcement, under Article 27 of the Law of 2024, the CSSF or the CAA may, within the limits of their respective competences, issue a public statement specifying the identity of the responsible person and the nature of the violation against persons subject to their respective supervision. The Lead Supervisory Authority may also issue recommendations to critical ICT third-party service providers concerning the implementation of specific security measures, such as encryption, patch management and risk mitigation strategies, may require providers to submit reports detailing how they have addressed these recommendations (Article 35[1][c]),and may conduct investigations and inspections to verify compliance (Article 35[1][a]–[b]).

With respect to NIS2 enforcement, the Bill does not add any gold plating to the NIS2 Directive. Article 33(2) empowers the ILR to conduct on-site inspections (Article 33[2][a]), targeted security audits (Article 33[2][b]) and request access to cybersecurity documentation and evidence of implementation (Article 33[2][d]–[f]). Furthermore, Article 33(4) allows the ILR to issue warnings (Article 33[4][a]), adopt binding instructions to remedy deficiencies (Article 33[4][b]) and order entities to cease and desist from non-compliant conduct (Article 33[4][c]).

Under the Law of 30 May 2015, which implements the ePrivacy Directive 2006/24/EC and governs the confidentiality of electronic communications, unsolicited marketing and the security of public communications networks, Criminal Courts may impose fines of up to EUR 125,000.

Articles 509-1 to 509-7 of the Criminal Code Criminal Code addresses specific cyber offences, including fraudulent access to an information processing system.

As discussed under Question 2, Article 97 of the Law of 1997 contract prohibits coverage for criminal fines and penal transactions, unless they are borne by a civilly liable third party. Regulatory penalties must therefore be personally borne by the sanctioned entity or individual and are not insurable under Luxembourg law.

Finland

In addition to Cyber Fines, there are other regulatory penalties set out in the above-mentioned laws that may arise from cyber incidents. Although the regulatory penalties are mostly set out at the EU level in the NIS2 Directive, GDPR, DORA and CRA there are some national differences.

According to section 32 of the Cybersecurity Act, a competent authority may prohibit a person from acting in the essential entity’s management, for example as a member of the board of directors or the supervisory board, a managing director or in any other comparable position for a specified period of time. Such prohibition is possible if that person has repeatedly and seriously violated the governance obligations for the management of essential entities laid down in section 10 of the Cybersecurity Act. However, before making such decision, the competent authority must issue a warning to the entity, specifying the violation and allow the entity a reasonable period of time to remedy the violation.

It should be noted that the government proposal of the Cybersecurity Act states that liability for damages resulting from violating cybersecurity obligations can be imposed on the company's management. In a limited liability company, this liability is primarily determined in accordance with the duty of care provisions of the Limited Liability Companies Act (624/2006). Therefore, it is possible that management of an entity may be required to compensate the company for damage caused by negligence of cybersecurity obligations, such as the governance obligations.

In addition, section 34 of the Cybersecurity Act sets out other administrative penalties that can be imposed on entities, such as imposing periodic penalty payments. The competent authorities can also order an entity to comply with an obligation with a threat to perform the obligation at the entity's expense if it does not comply. Similarly, the authorities can order an entity to suspend an activity if an obligation is not complied with.

The FIN-FSA can also impose a penalty payment under section 40, subsection 2, subparagraph 13 of the Act on the Financial Supervisory Authority to anyone who

wilfully or negligently fails to comply with the obligations of DORA, such as ICT risk management and ICT related incident reporting and managing ICT third-party risks. The penalty payment can also be imposed on someone who is part of the entity's management, if that person has contributed in a significant way to the act or failure to comply with the obligations.

Similar to how insuring is not possible against Cyber Fines, it is not possible to insure against other regulatory penalties directly. Despite this, it could be possible to obtain an insurance policy against other financial consequences, such as the costs arising from the investigation of cyber incidents.

South Africa

In addition to potential imprisonment (as outlined above in section 1), individuals and entities may face non financial regulatory penalties under POPIA, where cybersecurity failures result in unlawful processing of personal information.

Formal Assessments

Under section 89 of POPIA, the Information Regulator may initiate a formal assessment, either on its own or at the request of any other party, to determine whether a responsible party's data processing practices comply with POPIA. This can potentially lead to further regulatory investigation, review and enforcement actions.

Suspension of Processing Activities

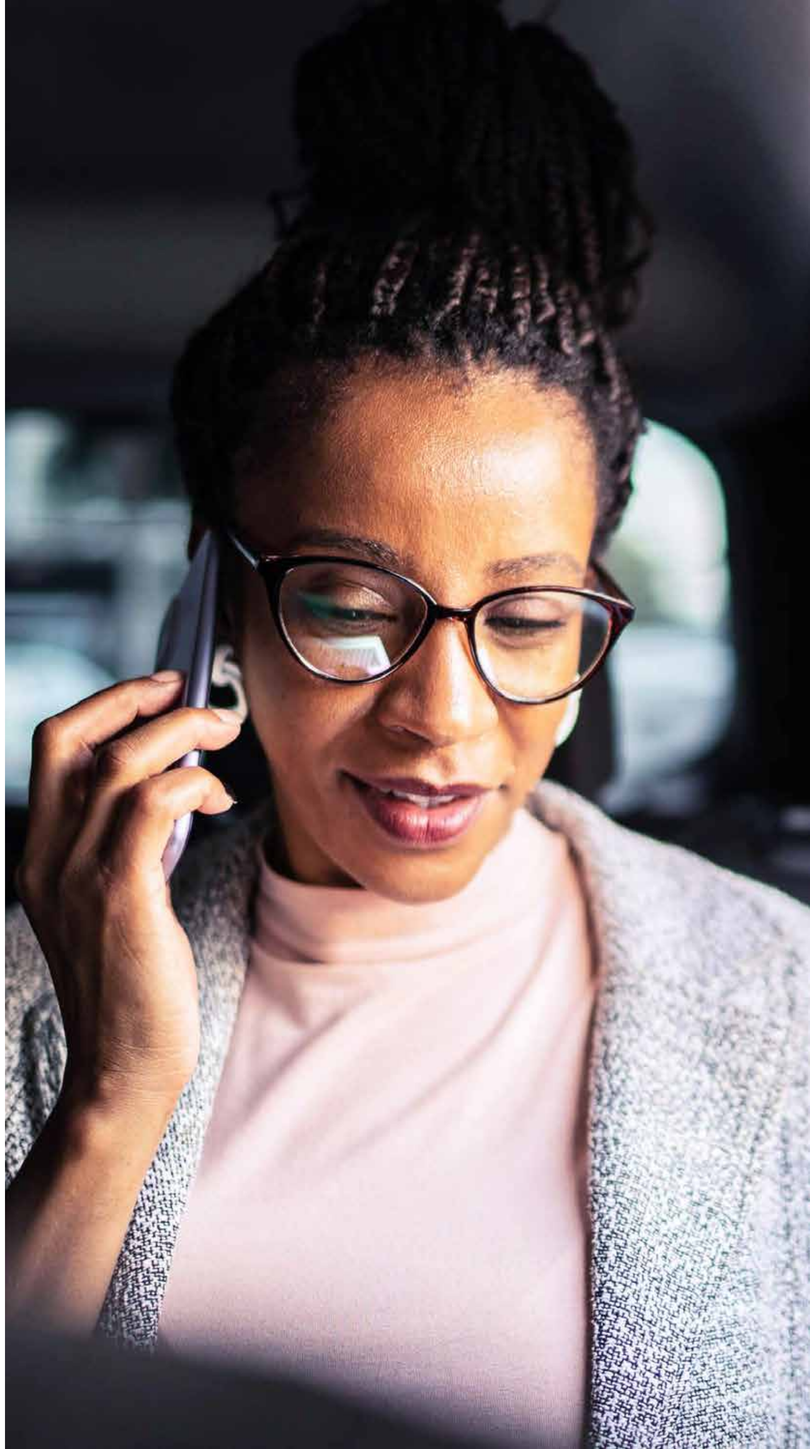
Under section 95(1) of POPIA, the Information Regulator may issue an enforcement notice requiring the responsible party to take or refrain from taking certain steps or stop processing personal information as specified in the notice, within a specific time-period. These notices are binding and non-compliance may escalate to administrative fines.

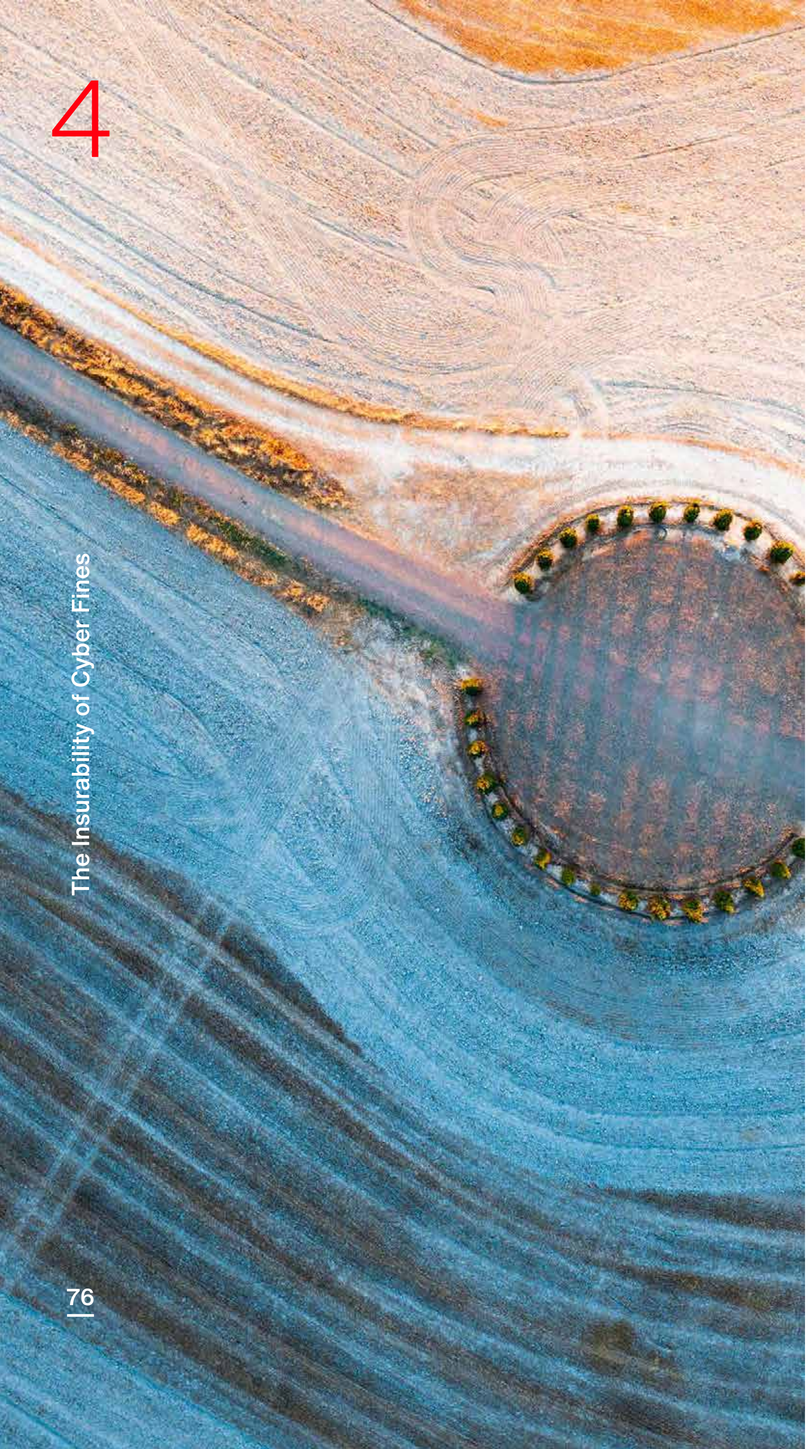
Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

While direct criminal fines and administrative penalties are often excluded from insurance coverage (as discussed above in section 2), South Africa's cyber insurance market does offer comprehensive support for associated costs arising from cyber incidents.

Insurers often provide modular cyber insurance policies that typically include:

1. Legal defence costs: Covering expenses related to regulatory investigations and litigation.
2. Audit and forensic services: Funding for post-incident assessments and compliance reviews.
3. Third-party liability cover: Protection against claims from affected individuals or entities.
4. Public relations and crisis management: Support for reputational recovery and stakeholder communication.





Business Interruption Coverage

Compensation for lost income due to system downtime or operational disruption.

These policies are designed to help organisations navigate the financial and operational fallout of cyber incidents, even if they may not be indemnified against certain fines imposed.

Italy

In addition to Cyber Fines, Italian organisations may face a variety of non financial regulatory sanctions following a cyber incident. For example:

- **Orders to cease non-compliant conduct:** regulatory authorities, such as the Garante and the ACN, may issue orders requiring organisations to cease processing activities that are in breach of data protection or cybersecurity laws.
- **Temporary or permanent bans on processing:** in the context of data protection, the Garante may impose temporary or definitive limitations, including bans on processing personal data.
- **Obligation to implement corrective measures:** the Garante and the ACN may require organisations to implement specific technical or organisational measures, including following audit recommendations, to remedy deficiencies in their cybersecurity posture.
- **Public warnings or reputational sanctions:** regulators may issue public statements or warnings about an organisation's non-compliance, which can have significant reputational consequences.
- NIS2 grants ACN with powers to impose non financial penalties for non-compliance, including:
  - issuing warnings, orders and instructions;
  - designate a monitoring officer responsible for overseeing compliance;
  - for essential entities, to suspend relevant certifications or authorisations concerning their specific service, should the deadline for taking preventative or remedial action not be met;
  - for essential entities, prohibiting senior management from exercising a managerial function until the threat or area of non-compliance in question is suitably resolved.

As regards the possibility to insure against the penalties and the financial consequences at hand, reference can be made to the principles set forth in the response to Question 2 above. The financial implications of a non financial fine do not appear insurable if these constitute the compensation of the fines themselves as providing for such insurance would deprive of sense the sanctions. Other financial implications of a non financial sanction such as legal costs for defending against its issuance might be deemed insurable.

Saudi Arabia

Other regulatory penalties that organisations may face arising from cyber incidents was addressed in Question 1 above.

Is it possible to insure against these penalties and their financial consequences was largely addressed this in Question 2 above. But to add, while companies may transfer certain financial risks (such as fines or breach-related costs) to insurance, non-monetary regulatory penalties are generally inherently uninsurable — measures like licence revocation/operational bans cannot normally be quantified in dollars by an insurer.

Norway

Coercive Fines

Under most of the legislation presented above, public authorities may impose daily coercive fines in cases of non-compliance with decisions and orders. Such coercive fines are likely not insurable, as they have a prominent penal purpose.

Damages

Some cyber security laws include provisions granting damages in accordance with GDPR. Norwegian law does not explicitly prohibit liability insurances covering damages claims.

Criminal Punishment (Fines or Imprisonment)

The following legislation relevant to cyber incidents entails potential for criminal punishment:

- Norwegian Security Act Section 11-4
- Norwegian Electronic Communication Act Section 15-14
- Norwegian Patient Records Act Sections 30 and 30 a
- Norwegian Health Register Act Sections 30 and 30 a
- Norwegian Health Research Act Section 54

Fines issued under these provisions are not insurable, as they are classified as criminal punishment under Norwegian law, cf. Norwegian Insurance Activities Act, Section 7-1, second paragraph.

Other Sanctions

The Norwegian Electronic Communications Act includes a number of regulatory sanctions apart from fines, cf. Sections 15-6 through 15-9. Whether these are insurable is not immediately clear and must be assessed individually pursuant to the assessment criteria outlined above, namely based on whether they first and foremost can be considered punitive or administrative.

Turkey

There are criminal sanctions, such as imprisonment and judicial fines, applicable to real persons. For organisations, in addition to the abovementioned administrative fines, suspension of activities or other sanctions may be possible in certain cases, as outlined below.

- According to Article 15 of the Data Protection Law, the Personal Data Protection Board may decide to extend its authority to suspend the processing of personal data or the transfer of personal data abroad, in cases where there is an explicit unlawfulness and where irreparable damages may arise.
- As noted above under Question 1, regulated companies are subject to sector-specific regulations under which the relevant regulators may impose sanctions due to non-compliance with cybersecurity requirements.

As explained above under Question 2, the insurability of Cyber Fines is not clear under Turkish legislation and there is a view stating that they are not insurable due to being against mandatory provisions of law. We believe that this argument would be even more applicable in the case of regulatory penalties which are not administrative fines (such as suspension). We have also not come across any insurance packages that cover such penalties in practice.

Sweden

Under the GDPR, a range of non financial penalties are possible such as warnings or reprimands, orders to bring processing operations into compliance with the GDPR, temporary or definitive limitation including bans on processing etc.

Under the Swedish NIS Act, non financial penalties consist of orders to cease non-compliant conduct or implement audit recommendations. Under the NIS2 Directive, a range of non financial penalties are possible such as suspension of authorisation to perform the service and orders to cease non-compliant conduct or implement audit recommendations.

Under the DORA Regulation, Member States are required to establish and enforce penalties for breaches, in Sweden this has been implemented through amendments to the relevant sector-specific legislation. In the insurance sector, for example, the Swedish Insurance Distribution Act (2018:1219) (Sw. Lag. [2018:1219] om försäkringsdistribution) provides that, in addition to imposing an administrative fine, the Financial Supervisory Authority may decide that a person serving on the board of an insurance intermediary, its CEO or equivalent senior manager, or their substitute, may not hold such a position with an insurance distributor for a period of not less than three and not more than ten years.

As noted under Question 2, the SFSA's Supervisory Statement concerns only fines, corporate penalties and administrative sanctions. Insuring these types of penalties is not considered consistent with good insurance standards. According to the SFSA, the reasoning is that insurance against fines and administrative sanctions would reduce the incentive to comply with laws and regulations, as it removes the legal consequences of violations. Such insurance therefore undermines the purpose of fines and sanctions. This assessment may also be regarded as applicable to other regulatory penalties that organisations could face as a result of cyber incidents, although the legal position in this respect remains uncertain.

Poland

Other Regulatory Penalties Which Organisations May Face Due to Cyber Incidents

Beyond monetary fines, Polish and EU legislation empowers authorities to impose severe non financial measures following cyber incidents, including but not limited to:

- Suspension of authorisation: under the NIS2 Directive (and its upcoming Polish implementation), authorities may suspend or revoke an entity's authorisation to provide essential or important services in the event of serious or repeated non-compliance.[104]
- The KNF may suspend a bank's authorisation to provide a given service under Article 138.3 Banking Law if recurrent ICT failures threaten stability or integrity of the financial system.
- Orders to cease non-compliant conduct: regulators may issue binding orders requiring organisations to remedy deficiencies, cease unlawful processing, or implement specific security measures.
- According to the proposed amendments to the NCSA aimed at implementing the NIS2 Directive, supervisory authorities will be authorised to order the implementation of specific incident response procedures, requiring the cessation of unlawful conduct, mandating the alignment of information security management systems with legal requirements and obliging entities to inform service recipients about significant cyber threats and recommended protective measures. The authority may also require the implementation of recommendations resulting from security audits, appoint a monitoring official to oversee compliance for a specified period.
- UODO frequently issues non-pecuniary orders under Art. 58.2 GDPR, such as temporary bans on processing and mandatory security audits.
- DORA introduces a broad toolbox for the KNF, including the power to require financial entities to terminate ICT-service contracts or prohibit the

104. Amendments proposed to Art. 53.9 of NCSA.

onboarding of new clients until deficiencies are corrected. Under DORA, KNF may also compel a financial entity to limit or cease provision of an ICT service until vulnerabilities are remediated.

- Public warnings and reputational sanctions: publication of the fact of non-compliance or breach, which can have significant reputational consequences.
- According to the proposed amendments to the NCSA aimed at implementing the NIS2 Directive, supervisory authorities will be authorised to order the public disclosure of information about breaches or serious incidents.

Insurability of Non Financial Penalties and Their Financial Consequences

At its core, insurance is a mechanism for transferring the risk of financial loss from the insured (policyholder) to the insurer. The insured pays a premium, and in return, the insurer agrees to indemnify the insured for certain defined losses or liabilities that are quantifiable in monetary terms. This principle is fundamental to all types of insurance, including cyber insurance.

The core function of insurance is to indemnify the insured for financial loss or liability, not to restore or guarantee a particular legal or regulatory status. Insurance is designed to compensate for quantifiable financial damages, not to prevent or undo non-monetary regulatory measures. By their nature, non financial penalties (such as suspension of authorisation or orders to cease conduct) are not insurable, as insurance is designed to indemnify against financial loss, not to prevent or reverse regulatory action. Polish law, in line with general European regulatory principles, does not permit insurance to neutralise or circumvent the effect of regulatory sanctions that are intended to enforce compliance or discipline market participants.

While the direct penalty (e.g., suspension of business) is not insurable, the financial losses resulting from such regulatory action (e.g., loss of income due to business interruption) may be covered under certain insurance policies, provided the loss is not excluded and is not a direct result of intentional or grossly negligent conduct. The precise scope of coverage will depend on the policy wording.

The direct cost of implementing remedial measures (for example, penetration testing, system hardening, forensics, mandatory audits or customer notification campaigns) is generally insurable and commonly sits in the “incident-response” or “first-party loss” sections of Polish cyber-policies. Where the regulatory order leads to revenue loss (e.g., downtime caused by suspension of an online service), indemnification is less certain and depends on whether the policy includes “business interruption” coverage triggered by non-physical damage. The ban on insuring intentional wrongdoing likewise applies. Although indemnification for managerial bans or revocation of licences is obviously impossible, defence-cost coverage for contesting such measures is standard. These costs are widely regarded as ‘remediation expenses’, not punitive in character.

England and Wales

The ICO has powers to impose corrective measures alongside administrative fines. These include warnings for intended processing likely to breach the law, public reprimands with formal findings and required remedial steps and enforcement notices mandating specific actions. Competent authorities under the NIS Regulations can also issue enforcement notices requiring organisations to act or cease certain activities. Unlike regimes such as NIS2 or DORA, there is currently no ability to fine individual management teams or restrict their activities. Nevertheless, the UK government and the NCSC have stressed the importance of Boards taking ownership of cyber risk and have published a non-binding Cyber Governance Code of Practice to support resilience.

Because these measures do not carry obvious financial consequences, the issue of insurability does not arise.

Ireland

In addition to administrative fines, many of the regulations and acts discussed include other remedial measures which may be imposed separate to any fines. Some examples of these remedial measures include:

DPA 2018

Under Section 127 of the DPA 2018, the DPC has various corrective powers such as the power to issue warnings, issue reprimands, order compliance with a data subject's request, order that a breach be communicated to data subjects, impose limitations (including banning processing), imposing restrictions and ordering suspension of data transfers to recipients in third countries.

NIS2

Similarly to the regime for administrative fines, the other remedial measures permitted will depend on whether the entity they are being imposed on is either an essential or an important entity. However, generally, the competent authority in Ireland may order entities to cease any conduct that infringes on the directive and desist from any repetition, order entities to implement any recommendations provided to it from a security audit and designate an office to monitor compliance within the entity for a defined period of time.

DORA

Article 50 of DORA permits Member States to confer power to a competent national authority to apply remedial measures. The Central Bank Act 1942 has been amended to allow the CBI to impose sanctions such as issuing an order to cease conduct which breaches DORA and desist from any repetition of such conduct, or ordering a temporary or permanent stop to any conduct which is considered contrary to DORA's provisions. The CBI may also publish public statements which indicate the financial institution or person(s) who have breached and the nature of the DORA breach.

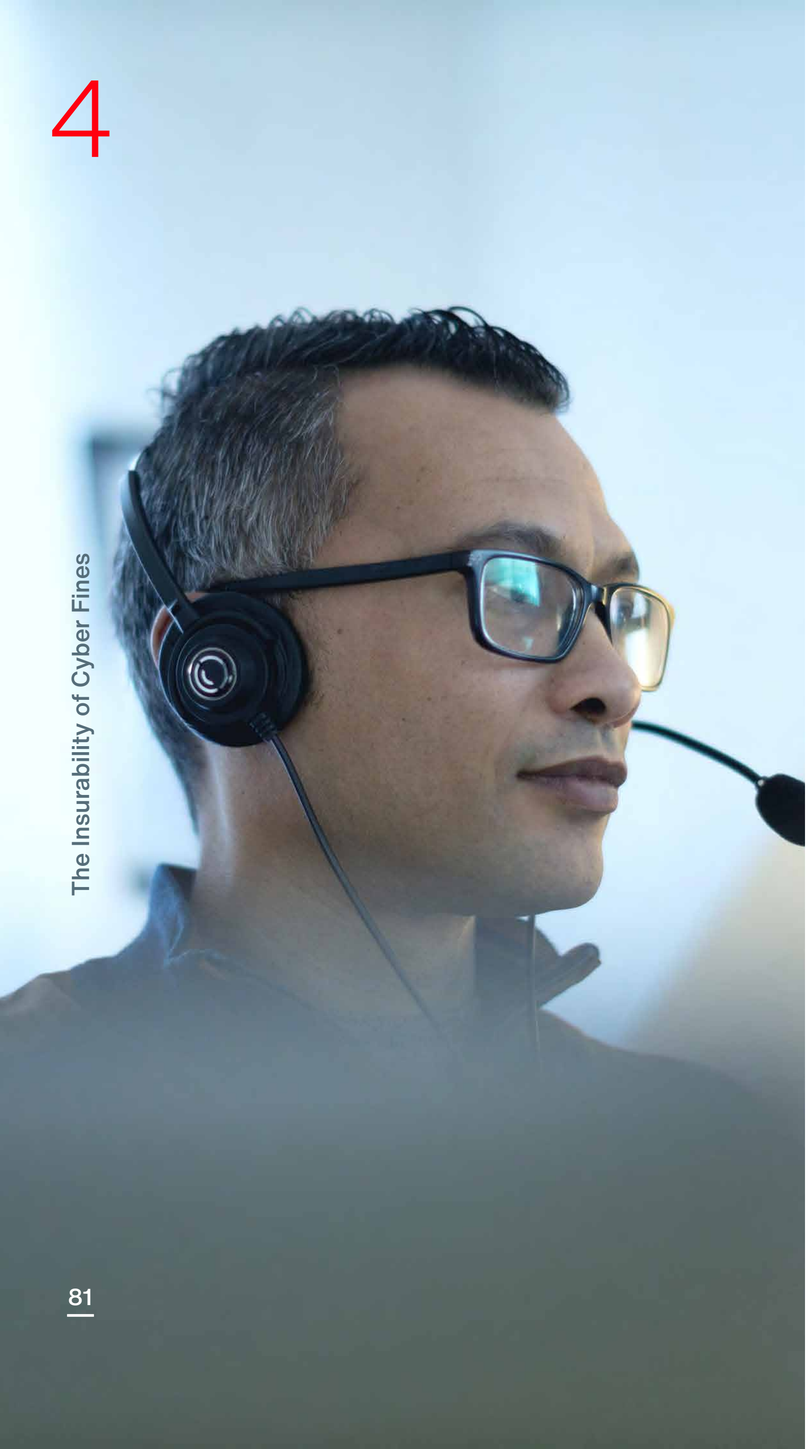
Similar to the insurability of Cyber Fines, there is no legislation or Irish court decision that would indicate whether it is possible to insure against any other potential regulatory penalties that may be imposed due to a cyber breach. As with the Cyber Fines, there are most likely public policy reasons affecting the likelihood of obtaining insurance in respect of or related to remedial penalties.

UAE

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

Yes, there are other regulatory penalties which organisations may face beyond the fines outlined in Question 1 above. These are broadly similar across the onshore and offshore regimes and include measures such as requiring the violating entity to take necessary actions and measures deemed appropriate by the relevant regulator to rectify their actions, suspending the entity from conducting certain activities, or withdrawing the entity's licence or ability to conduct certain activities altogether. The precise penalties will depend on the regulator and the severity of the incident.

Under the ICT Healthcare Law, health facilities may also lose their access to the central healthcare information system, which is a severe sanction making it virtually impossible to operate their business lawfully.



Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

As noted above, there is no legal restriction within the laws noted in Question 1 above on insuring against penalties and financial consequences arising from cyber incidents (e.g., business interruption losses due to suspension of activities). However, coverage will depend on the terms of the insurance policy and the willingness of insurers to underwrite such risks.

Germany

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

- Under the GDPR, Data Protection Authorities may take all necessary corrective measures to ensure GDPR compliance (Art. 58[2] GDPR). This includes orders to cease data processing (Art. 58[2][f] GDPR). For data-heavy businesses, this can amount to a full ban on operations.
- Financial institutions risk limitation of their licence for certain transactions (Sec. 45b[1], 25a KWG). In some circumstances, the BaFin may give direct instructions to managers, close the institution to clients and prohibit the reception of payments (Sec. 46 KWG).
- Telecommunications operators risk their licence if they disobey their special obligations repeatedly and severely (Sec. 202[3] TKG).
- German DPAs can notify the Business Supervisory Authorities (*Gewerbeaufsichtsbehörden*) of GDPR infringements (Sec. 40[3] BDSG, *Bundesdatenschutzgesetz*, Federal Data Protection Act). Continued and severe infringements may lead to rescindment or refusal of a business licence (Sec. 35 *Gewerbeordnung*, German Trade Regulations). We could not identify cases where authorities made use of this competence.
- Authorities may prohibit the operation of critical infrastructure (Sec. 9b[4] BSIG) if they pose a danger to the public order and safety.
- The renewed BSIG will equip the BSI with further competencies to publish information on pending cyber risks, to inform affected persons about recommended defence measures (Sec. 61[8] BSIG-new) and, as a last resort, to suspend licences and prohibit operations (Sec. 61[9] BSIG-new).

Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

As set out under Question 2, there are no explicit limits on insurability but insurance contracts may be legally void if they offend common decency (Sec. 138[1] BGB).

Whereas insurance of regulatory fines offends common decency by circumventing the punitive effect of fines, the same does not necessarily apply to other penalties. Most additional measures envisage public safety and protection of fundamental rights and do not serve

a punitive goal. Consequently, recovery from an insurer does not impede their effect and insurability could be affirmed. Please note that we could not identify case law that confirms this train of thought.

Spain

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

Across GDPR/LOPDGDD, LSSI, NIS, the forthcoming NIS2 framework and DORA in the financial sector, authorities deploy a wide array of non-monetary tools that can follow a cyber incident. These include warnings and reprimands; binding instructions; orders to bring processing or systems into compliance within fixed timelines; mandatory audits and independent reviews; temporary or definitive suspensions of processing or authorisations; orders to notify authorities and affected individuals; publication of decisions; and, under NIS2 in serious cases, temporary management bans for directors of essential entities.

Coercive daily penalty payments to compel compliance are also contemplated in certain situations. These non financial penalties are designed to ensure compliance and remediate risks, and they can have significant operational and reputational consequences for affected organisations. For instance, a suspension of an authorisation to perform services, orders to cease non-compliant conducts, or the public dis closure of incidents can disrupt business operations and damage an organisation’s reputation before customers and partners.

Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

Non financial penalties arising from cyber incidents such as orders to cease processing, management bans, or suspensions cannot be “insured against” in the sense of transferring the obligation to perform or avoid them (See Question 2 above). Insurance cannot prevent a regulator from issuing such orders or neutralise their effect. However, the economic consequences associated with responding to regulatory proceedings may be insured, particularly those involving activity suspension or disqualification from professional activities to the extent these may qualify as "other pecuniary losses" as outlined in insurance regulations and backed by Spanish case law. In practice, cyber insurance policies in Spain could usually cover the costs of investigating an incident; costs for legal defence; claims by third parties (customers/ suppliers/data subjects) triggered as a consequence of a breach; and breach mitigation costs such as, for example, public relations / communication expenses.

Netherlands

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

Under the GDPR and the Dutch Administrative Law, the Dutch DPA can impose several other regulatory penalties, namely: a) a periodic penalty payment which in an incremental payment due daily up to a certain maximum (*last onder dwangsom*); b) a processing ban; c) a reprimand and; d) a warning.[105]

Under the Wbni the supervising authority[106] can impose the following regulatory penalties: a) an order to have a security audit conducted by an independent expert; b) a binding instruction; c) period penalty payment.[107] Under the Cybersecurity Act, the supervisory authority[108] can impose: a) a security scan; b) an audit; c) the order to disclose the violation; d) an instruction to perform certain actions within a specific period; e) periodic penalty payment; f) a request for suspension of certificate or permit; g) a request for suspension of the management.[109]

Under the Dutch Telecommunications Act the supervising minister and ACM (*Autoriteit Consument & Markt*) can impose a ban on the provision of electronic communications networks or services.[110] Under administrative law, the ACM can impose a periodic penalty payment.

Under DORA the authority can: a) issue an order to cease conduct that is in breach with the regulation and to refrain from repetition of that conduct; b) require the temporary or permanent cessation of any practice that violates with the regulation; c) require data traffic records held by a telecommunications operator; d) issue public notices.[111] Under Dutch administrative law, the financial regulators (DNB and AFM) are also allowed to impose a period penalty payment.

There is debate whether this is a regulatory penalty, but in principle all regulators in the Netherlands have the right to publish the administrative decision, for example, by means of which an administrative fine is imposed. Due to the reputational risk, this publication can have substantial (financial) consequences.

Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

Most of penalties mentioned above are not monetary penalties, which in our view makes it difficult to insure against them specifically. It may, however, be possible to insure against the adverse financial consequences they cause. As we understand, cyber insurance policies in the Netherlands contain generally a clause that states that administrative penalties and their associated costs are covered.[112] Since there is no case law on this point, we cannot assess whether such clauses would ultimately hold up in court.

Periodic penalty payments are monetary penalties and qualify as administrative penalties. They are usually not covered by cyber insurance, since they typically not imposed for a one-time cyber incident, but rather for a continuous violation of the GDPR.[113] We expect that, because these payments are intended to end unlawful conduct under the GDPR, allowing an insured to pass these costs to an insurer would be contrary to the public policy. Again, in the absence of case law, we cannot say with certainty whether period penalty payments are insurable.

105. According to the website of the Dutch Data Protection Authority: Fines and other sanctions from the AP | Autoriteit Persoonsgegevens.
106. For the sectors Energy and Digital Infrastructure this is the Minister of Economic Affairs and Climate. For the sectors Banking and Financial Market Infrastructure this is De Nederlandse Bank (DNB). For the sectors Mobility and Supply and distribution of drinking water, this is the Minister of Infrastructure and Water Management. For the sector Healthcare, this is the Minister of Medical Care and Sport.
107. Artt. 26 & 27 Wbni.
108. In Art. 15 Draft Cybersecurity Act the different supervisory authorities are appointed. These are all different ministers.
109. Artt. 71-75, 77, 78, 82-86, 89, 90, 92 Draft Cybersecurity Act.
110. Art. 15.2a Dutch Telecommunications Act.
111. Art. 50 (4) DORA.
112. N.M. Brouwer, *De Cyberverzekering vanuit civielrechtelijk perspectief*, p. 102.
113. N.M. Brouwer, *De Cyberverzekering vanuit civielrechtelijk perspectief*, p. 85, footnote 34.

France

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

Under NIS2 and French transposition, competent authorities (e.g., ANSSI/sectoral regulators) can order audits, issue binding instructions, require specific security measures and — in serious cases — restrict or suspend activities/authorisations. These non-financial measures are central to post-incident enforcement.

In the financial sector, ACPR/AMF have a broad supervisory toolkit aligned with DORA (reporting, testing, third party risk), including public communications and corrective orders.

CNIL may also enforce corrective measures.

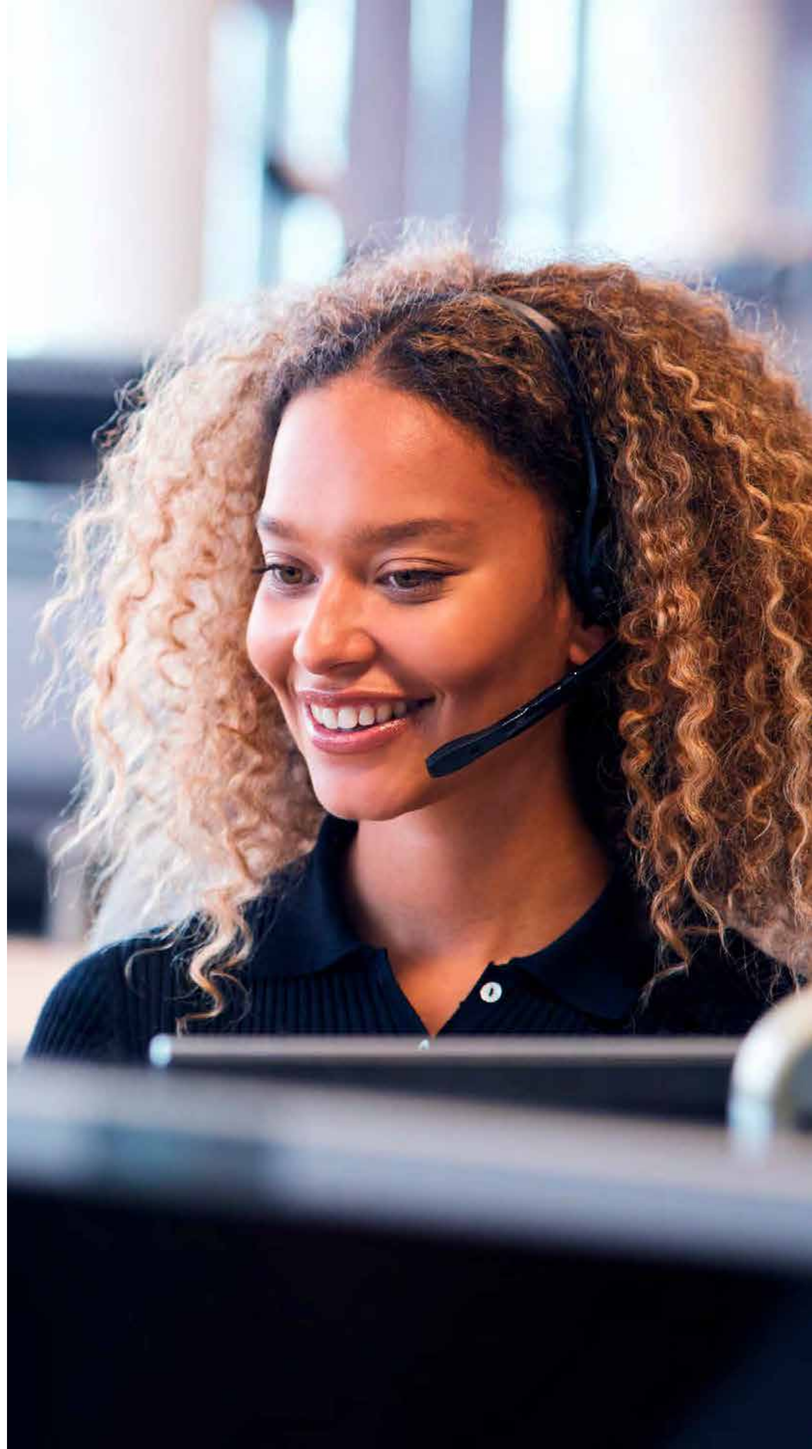
Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

Non-punitive, compensatory or purely corrective measures remain potentially insurable if there is no intentional misconduct. Indeed, the insurance contract is characterised by three essential elements: a risk, a premium and the coverage of this risk in the event of a loss. The risk must be uncertain and not result from the intentional or fraudulent act of the insured (French Insurance Code, art. L. 113-1, al. 2). Insurance is thus designed to cover financial consequences that are both fortuitous and lawful.

In this regard, corrective measures (e.g., audits/remediation) following an accidental cyber event may be insurable, subject to policy terms and insurance law requirements. In this regard, the HCJP report on insurability of cyber fines especially states that the financial consequences of corrective measures ordered by the CNIL may be insurable, such as those resulting from:

- Formal notices to inform data subjects of a breach; or
- Formal notices to bring processing operations into compliance with applicable provisions, where such compliance is no longer ensured because of the attack suffered.

In reality, where those administrative measures are unrelated to any notion of sanction but are intended solely for preventive, protective or corrective purposes, the financial loss to which their implementation would expose the insured should constitute an insurable risk.



Switzerland

Are There Other Regulatory Penalties Which Organisations May Face, Arising from Cyber Incidents?

For example, under NIS2 in the EU, a range of non financial penalties are possible such as suspension of authorisation to perform the service and orders to cease non-compliant conduct or implement audit recommendations.

Data Protection

The FDPIC is authorised to take a variety of administrative measures if there are suspicions that data protection regulations have been violated (including if the requirements regarding data security under the FADP have not been adhered to).

It may open an investigation ex officio or in response to a report if there are sufficient indications that a data processing activity could violate data protection regulation. The federal body or private person (i.e., the affected controller or processor) must, in this case, provide the FDPIC with all the information and documents that are needed for the investigation.[114] Otherwise the FDPIC may order such cooperation as well as access premises and installations, question witnesses and request appraisals by experts (even potentially with the support of federal authorities and cantonal or communal police).[115]

If the FDPIC concludes that data protection regulations have actually been violated, it may i.a. order that the processing be modified, suspended or terminated, wholly or in part and the personal data deleted or destroyed, wholly or in part. In particular, it may order that the controller or processor take the measures in accordance with the requirements regarding data security or provide the FDPIC, or if applicable, the data subject with the necessary information under the data breach notification obligations.[116]

Critical Infrastructure

In case of a cyber incident, the NCSC may publish information on such incident if this serves to protect against cyber threats. This information may only reveal details about the natural or legal person concerned if they consent to this and if it relates to misused identification features and addressing elements.[117] The NCSC may also forward information from reports regarding cyber incidents to other authorities and organisations active in the field of cybersecurity as well as file a criminal complaint with law enforcement authorities.[118]

114. Article 49 FADP.
115. Article 50 FADP.
116. Article 51 para. 1 and 3 FADP.
117. Article 73c ISA.
118. Article 73d ISA.

Financial Sector

Where there are (indications of) violations of the provisions of the FINMASA, FINMA may within its supervisory function:

- Open proceedings;
- Ensure the restoration of compliance with the law;
- Require the supervised persons or entities to provide collateral;
- Issue a declaratory ruling;
- Set a deadline and perform the required act itself or have it performed at the expense of the defaulting party if the enforceable ruling is not observed within the deadline;
- Prohibit a person responsible from acting in a management capacity at any person or entity subject to FINMA's supervision for a period of up to 5 years;
- Publish a final ruling;
- Confiscate profit;
- Prohibit employees of a supervised entity responsible for trading in financial instruments or employees of a supervised entity acting as client advisers from trading in financial instruments or acting as a client adviser for a fixed period or permanently;
- Appoint an independent and suitably qualified person to investigate circumstances relevant for supervisory purposes at a supervised person or entity or to implement supervisory measures that it has ordered (an investigating agent);
- Revoke the licence of a supervised person or entity.[119]

Telecommunications Sector

Under the TCA, OFCOM may conduct surveillance and take legal remedies if it detects an infringement of the law. If a telecommunications licence has been granted by ComCom in the first place, ComCom takes the corresponding measures based on the proposal made by OFCOM to:[120]

- Call on the legal or natural person responsible for the infringement to remedy the infringement or take measures to prevent any repetition of it. The person responsible for the infringement must inform OFCOM of the measures it has taken;
- Require the legal or natural person responsible for the infringement to surrender to the Confederation any revenue generated during the infringement;
- Restrict, suspend, revoke or withdraw a telecommunications licence or restrict, suspend or totally forbid the activity of the legal or natural person responsible for the infringement;
- Make a telecommunications licence subject to conditions;
- Withdraw the proficiency certificate from the holder or make it subject to conditions.

Telecommunications providers are obliged to provide the competent authorities with the information required to implement such surveillance and legal remedies.[121]

Finally, if a telecommunications service provider infringes the applicable law, the licence or a decision having force of law, it may be required to pay an amount up to 10 percent of the amount of its average turnover in Switzerland in the last three financial years by way of an administrative fine. The fine is set taking into account gravity of the infringement and the enterprise's financial situation.[122]

Nuclear Energy Sector

The NEA empowers the supervisory authorities to examine submitted projects and ensure that licence holders and owners of nuclear goods meet their obligations in accordance with the provisions of the NEA. In particular, such supervisory authorities may:

- Order all necessary and reasonable measures aimed at preserving nuclear safety and security;
- In the event of an immediate threat, impose immediate measures that deviate from the issued licence or ruling;

119. Articles 29 et seqq. FINMASA.
120. Article 58 TCA.
121. Article 59 TCA.
122. Article 60 TCA.

- If necessary, seize nuclear goods or radioactive waste and eliminate sources of threat at the cost of the owner;
- Call on the intervention of cantonal and communal police forces, as well as the investigation bodies of the Federal Office for Customs and Border Security. If there is evidence that offences against the provisions of the NEA may have been committed, the supervisory authorities may call on the intervention of the relevant federal police authority. Border controls are the responsibility of the customs authorities;
- Keep detailed records of nuclear materials and radioactive waste in Swiss nuclear installations. These records shall also encompass nuclear materials and radioactive waste abroad, insofar as they are in the possession of Swiss licence holders. They shall provide information about their location, intended use, processing and storage;
- Insofar as is required for the enforcement of the NEA, its implementation provisions or rulings based thereon, be provided with all information and documentation they may need in order to make comprehensive assessments or carry out effective controls;
- Enter all plots of land, buildings and installations of persons obliged to provide information and any sites on which geological investigations are being carried out, without prior notification and may install monitoring devices and seals, collect material and soil samples and inspect all relevant documentation. They may confiscate any incriminating material.[123]

Is It Possible to Insure Against Those Penalties and Their Financial Consequences?

Generally, yes. Various Swiss insurance companies offer both D&O — as well as cyber insurances which cover costs incurred in connection with criminal, supervisory, or administrative proceedings (such as lawyers' fees, investigation, court and expert witness costs) following a cyber incident. Some even cover fines as far as such fines are insurable under applicable laws. As mentioned above, this cannot encompass criminal fines. However, it may include administrative fines as it is not fully clear under Swiss law whether such administrative fines are insurable as they are generally not intended to directly affect the person concerned in the same way as criminal fines are. Some or most insurance providers explicitly exclude coverage for intentional wrongdoing or gross negligence in connection with cyber incidents.

123. Articles 72 et seq. NEA.

5

Are Cyber Incidents Prompting Data Breach Class Actions?

Chapter Summary

Class actions and collective redress mechanisms for data breaches and cyber incidents are increasing. The implementation of the EU Representative Actions Directive is driving an increased interest in collective litigation, particularly in consumer-facing sectors.

Class actions can amplify the financial and reputational impact of cyber incidents, especially when combined with regulatory enforcement. It is important to have early notification, transparent communication and comprehensive legal and insurance strategies to manage the risks that class action claims present.

Jurisdictions such as Portugal, the Netherlands, France and Ireland have active or emerging class action regimes, with recent cases targeting technology companies, social media platforms and healthcare providers. In England and Wales, claims continue to be brought on an opt-in basis in the absence of an opt-out procedure.

The procedural mechanisms vary — opt-in versus opt-out and the requirements for qualified entities — but the trend is towards greater accessibility and coordination for affected individuals.

Outside the EU, and England and Wales, class actions are less common, with some countries lacking a formal mechanism for collective redress.

Typical claims focus on non-material damages for distress and privacy harms, with low-to-modest per-capita awards but high aggregate and defence costs, especially where consumer bodies orchestrate litigation.

In terms of global exposure, U.S. class action litigation against European companies is increasing. In the most recent cases, insurers have provided cover, as there was no territorial or U.S. restriction in the policy wording.

Practical Actions for Organisations to Consider Now

- Monitor litigation trends: subscribe to legal alerts and track class action cases and developments in your sector.
- Assess your exposure to class action claims: evaluate data volumes, breach history and the extent of your consumer-facing operations.
- Strengthen your data protection and breach notification processes to minimise the potential for class action triggers.
- Include litigation risk in board reporting: ensure directors are aware of potential exposure and mitigation plans.
- Consider your U.S. exposure.

Belgium

The class actions regime under Belgian Law allows groups of consumers and Small and Medium sized Enterprises (**SMEs**) to collectively seek redress for harm caused by the same event or practice, including violations of data protection rules (such as GDPR violations).[124]

A class action is admissible, provided that the following three requirements are met:

- The alleged cause concerns a breach by the defendant of one of its contractual obligations, of one of the European regulations or the laws referred to in Article XVII.37 Code of Economic Law.
- It is brought by a qualified representative that meets the criteria set out in Article XVII.39 Code of Economic Law (such as recognised consumer organisations — with NOYB or None of Your Business, European Centre for Digital Rights founded by Max Schrems as a notable representative[125]) on behalf of a group of consumers or SMEs.
- The use of a class action is more efficient than pursuing an individual lawsuit.

The Brussels Enterprise Court (*Ondernemingsrechtbank/ Tribunal de l'entreprise*) has exclusive jurisdiction over class actions. In October 2024, a Dutch NGO (SOMI: Stichting Onderzoek Marktinformatie) has started a class action in Belgium against TikTok for (among others) GDPR and data breaches.[126] Consumers can still join the claim. The main issue put forward by SOMI is the lack of protection of minors on the app. We are not aware of any progress in the procedure.

Luxembourg

Although no high-profile cyber related litigation has yet arisen in Luxembourg, the risk environment is changing rapidly. DORA obliges financial entities to comply with their obligations and notably renegotiate critical ICT outsourcing agreements by January 2025. The CSSF and CAA have indicated informally that enforcement will begin in 2026.

Portugal

For potentially affected companies, class actions represent an increasing risk due to certain characteristics of the Portuguese legal system that tend to favor plaintiffs, particularly the "opt-out" regime and the low court fees.

Under Law No. 83/95 of 31 August, a representative plaintiff may, by operation of law, act on behalf of the entire class without an express mandate or authorisation from each individual member. The resulting judicial decision is binding on all class members, except those who exercise their right to opt-out.

The opt-out mechanism is triggered when the initial pleading is filed. At that point, the court sets a deadline for affected individuals to declare their exclusion from the collective proceedings or, alternatively, to participate individually alongside the representative plaintiff. Where notification is required, it may be carried out via social media or public notice.

In recent years, several high-profile class actions have emerged in the technology and social media sectors in Portugal. For example, the consumer association DECO brought an action against Meta (formerly Facebook) involving an estimated 60,000 Portuguese users allegedly affected by a data breach. The proceedings were discontinued in 2021 following an agreement between Meta and DECO to cooperate on a three-year initiative aimed at enhancing the digital experience of Portuguese users. In another case, the non-profit association Omnibus has initiated proceedings against TikTok, alleging the improper handling of Portuguese users' personal data and seeking EUR1.12b in damages.

Finland

Cyber incidents have not prompted data breach class actions in Finland so far. According to the Finnish Act on Class Actions (444/2007), the procedural mechanism for initiating class actions is only available for the Finnish Consumer Ombudsman in civil cases involving

124. Article XVII.35-XVII.70 Code of Economic Law.
125. Ministerial Decree of 30 September 2020 recognising an association for the purpose of initiating a collective redress action.
126. Nederlandse stichting start gezamenlijke rechtszaak tegen TikTok in ons land: "Minderjarigen worden onvoldoende beschermd"| VRT NWS: nieuws ; Privacy en Online Veiligheid | SOM.

a group of consumers and a trader concerning consumer protection matters. Such matters can include disputes concerning the marketing of products and services, defective goods and unfair contractual terms. Despite the procedural mechanism having been available since 2007, no class actions have yet been brought in Finland.

However, following the implementation of the EU's Representative Actions Directive (EU) 2020/1828 into the Finnish Act on Class Actions in 2023, the class action mechanism was expanded to be applied also to representative actions as set out in the directive. The directive enables member states to designate consumer organisations and public bodies as qualified entities that can act as claimants in the interest and behalf of consumers. The Data Protection Ombudsman has been designated as one of the qualified entities by the Finnish Ministry of Justice. This enables the Data Protection Ombudsman to also bring representative actions in matters concerning consumer data protection. The Data Protection Ombudsman could utilise the class action mechanism if a cyber incident were to cause a data breach involving consumer personal data.

It is also possible that a consumer organisation could apply to the Ministry of Justice for designation as a qualified entity for the purpose of bringing a representative action relating to a cyber incident. However, such a consumer organisation must fulfil certain criteria set out in the Act on the designation of organisations promoting the collective interests of consumers as qualified entities (1102/2022) (**Qualified Entities Act**). According to section 3 of the Qualified Entities Act, the organisation must, among other things, be a non-profit registered association as defined in the Associations Act (503/1989) and have engaged in public activities for the protection of consumer interests for at least 12 months prior to submitting the application for designation.

Additionally, the organisation's statutory purpose must demonstrate its legitimate interest in safeguarding consumer rights, as outlined in the provisions of EU law referenced in Annex I of the Representative Actions Directive, including the GDPR. In Finland, there are currently no consumer organisations that protect consumer interests in data protection or cyber matters. The organisation must also be independent and not influenced by individuals or entities with an economic interest in the bringing of a representative action. Therefore, such an organisation could not be formed solely for the purpose of bringing a representative action.

According to section 2 of the Class Actions Act, a case may be heard as a class action (and therefore, as a representative action) in Finland if:

- Several persons have claims against the same defendant, based on the same or similar circumstances;
- The hearing of the case as a class action is expedient in view of the size of the class, the subject matter of the claims presented and the evidence presented;
- The class has been defined with adequate precision.

Finland has implemented an opt-in mechanism that allows consumers to express their wish to benefit from the representative action and therefore become members of the action. If a qualified entity, such as the Data Protection Ombudsman, plans to initiate a representative action, it is required to publish information about these plans, as well as the status of ongoing representative actions and the outcomes of potential hearings, on its website. Primarily, the qualified entity is liable for all legal costs incurred from the case and the court's decision bind all members who have opted in to the case.

So far, the Data Protection Ombudsman has not initiated any representative actions. For instance, legal proceedings relating to the aforementioned Vastaamo case began before the Representative Actions Directive was applicable in Finland. At the time, the case prompted discussion and debate about expanding the class action mechanism in Finland, given that it involved more than 30,000 potential plaintiffs against a single hacker. The Consumer Ombudsman also considered bringing a class action in relation to the Vastaamo case but ultimately concluded that the case involved violations of data protection and privacy and that a class action was not an appropriate way to address the matter5. Although the representative action mechanism has addressed data breaches and class actions to some extent, its scope is still limited to consumer matters.

The role of the Consumer Ombudsman in cybersecurity-related class actions may increase in the future. The CRA establishes specific cybersecurity conformity requirements for products intended for consumer use. If products are found to violate these requirements after being sold to consumers, or if their cybersecurity features do not align with the marketing of the products, they could be considered defective under the Finnish Consumer Protection Act (38/1978). This could enable the Consumer Ombudsman to initiate class actions relating to the nonconformity of cybersecurity requirements of products.

In addition, civil actions brought by several different plaintiffs against one respondent at the same time could be handled in the same proceedings, if the claims are based on essentially the same grounds. However, this would not constitute a class action suit per se, and each claim would result in a separate judgement, with each plaintiff carrying an individual risk in relation to the case.

South Africa

While there is currently no observable trend of class actions arising from cyber incidents in South Africa, there is a risk of class actions in the future.

With regard to the legal basis for such claims, under section 99 of POPIA, a data subject, or the Information Regulator on request from the data subject, may institute a civil action for damages against a responsible party for breach of any provision of POPIA. An award of damages must be just and equitable but may include damages for patrimonial and non-patrimonial loss, aggravated damages in a sum determined in the discretion of the court, interest and costs of suit.

The procedural mechanism for instituting class actions has been developed through the common law and is informed by the Constitution of South Africa, 1996.

Section 38(c) of the Constitution provides that "anyone acting as a member of, or in the interests of, a group or class of persons' has the right to approach a competent court to allege that a right in the Bill of Rights has been infringed or threatened".

In 2012, the Supreme Court of Appeal in Children's Resource Centre Trust and Others v Pioneer Foods (Pty) Ltd and Others[127] extended class action litigation to include civil damages claims which fall outside the scope of the Bill of Rights and established the criteria for certification of a class action in South Africa.

Before a class action may be instituted, certification of the class is required. The potential plaintiffs must obtain permission, from a court, for certification of the class. In Mukaddam v Pioneer Foods (Pty) Ltd and Others[128] the Constitutional Court held that the power of a court to certify a class is discretionary and that in exercising its discretion a court must be guided by the requirements and principles identified in the Children's Resource Centre case, including that:

- The class is identifiable by objective criteria;
- The cause of action raises a triable issue;
- Sufficient issues of fact or law are common to all members of the class;
- The relief sought or damages claimed flow from the cause of action;
- Class action should be the most appropriate means of allocating damages to members of the class;
- The proposed representatives of the proposed class must be suitable to conduct the action and represent the class; and
- A class action should be the most appropriate means of determining the claims of the members of the class given the composition of the class and the nature of the proposed action.

Once a class has been certified, the matter will proceed by way of trial action.

Although we have not yet seen any major data breach class action in South Africa, high-profile incidents such as the breach affecting TransUnion in March 2022, have significantly heightened public and regulatory scrutiny.

In 2022, TransUnion experienced a data breach where a criminal third-party gained access to an isolated

127. Children's Resource Centre Trust and Others v Pioneer Foods (Pty) Ltd and Others 2013 (2) SA 213 (SCA).
128. Mukaddam v Pioneer Foods (Pty) Ltd and Others 2013 (5) SA 89 (CC).

TransUnion server. The breach was reported as “one of the biggest breaches” dealt with by the Information Regulator, and impacted the personal information of millions of consumers and business information of thousands of organisations.

The scale and sensitivity of the exposed data prompted enforcement action by the Information Regulator and sparked public concern over data protection practices. Incidents of this magnitude can serve as a catalyst for collective litigation, especially as awareness of data rights under POPIA continues to grow and the procedural framework for class actions becomes more established.

Italy

Article 840bis of the Italian Civil Procedure Code Entered Into Force on 19 May 2021

Requirements and Characteristics

A class action can be issued only for homogeneous (thus, not mandatorily identical) rights of the persons belonging to the class. This means that all rights arising from the same unlawful act (whether contractual or non-contractual) can be protected through a class action, regardless of the differences in the damage caused to individuals (provided, however, that such damage can be determined according to uniform criteria). Homogeneity of rights occurs when the rights are based on the same cause of action.

The admissible relief is monetary in the sense that it is admitted for seeking compensation for damages or return of undue amounts. Class action is also admitted for obtaining the inhibition of unclear whether the class action is also admitted for seeking solely the declaration of nullity, the annulment, the termination of contracts (as well as other relief aimed at impacting on validity and effectiveness of contracts) without seeking monetary relief.

The persons who have standing to bring the class action are the persons belonging to the class (in consideration of their rights) as well as associations and organisations while the persons who can be addressed with a class action are enterprises and entities responsible for issuing public services or services of public utility that are the authors of harmful conducts.

Proceedings (First Instance Degree)

The proceedings are initiated by filing a petition before the Court of the place of residence of the defendant. The competent division of the Court is the Division specialised in Business and Corporate Law. As soon as the petition is filed, the judge shall issue the decree scheduling the first hearing of appearance of the parties and setting-forth the time limit for the appearance in court of the defendant which shall be non-higher than 10 days before the first hearing of appearance.

The petition and the decree shall be published by the court clerk in the public area of the website of the Italian Ministry of Justice within 10 days as of the filing of the decree.

The petition and the decree shall be served by the plaintiffs to the defendant. Among the service and the first hearing of appearance at least 40 days (if the defendant is in Italy) or 60 days (if the defendant is abroad) shall elapse.

The defendant shall appear in the proceedings filing its statement of defence in which it shall file all its objections, defences and shall seek the joinder of third parties, raise counterclaims and shall also file documents and seek the admission of means of evidence.

The judge shall decide the admissibility of the class action within 30 days as of the first hearing of appearance by issuing a judicial order. The action is inadmissible when (i) it is manifestly ungrounded, (ii) when it does not regard homogeneous rights; (iii) when the plaintiff is in conflict of interest with the defendant and (iv) when the petitioner does not appear able to handle the homogeneous individual rights of the persons belonging to the class.

The judicial order ruling the admissibility of the class action is published in the court telematics system portal by the court clerk within 15 days as of the issuance of the judicial order.

By the judicial order declaring the admissibility of the class action, the judge grants a time limit for the adhesion to the class action by other persons with the same homogeneous rights. The time limit at hand is set-forth upon penalty of forfeiture and shall be non-lower than 60 days and non-higher than 150 days as of the publication of the judicial order on the admissibility of the class action in the court telematics system portal.

The taking of evidence stage is Deformalised and is conducted by the judge with autonomy. The judge assumes the means of evidence within the formalities deemed appropriate and in the adversarial proceedings among the parties.

The petitioner can seek that the judge orders to the defendant the filing of exhibits. The order of filing can be issued upon the condition that it is proportioned to the ruling to be issued, which is decided by the judge taking into account how important the facts under the order of filing are with a view to the ruling, the costs of the filing, whether the proofs requested to be ordered are confidential.

When the judge deems that the lawsuit is ready to be decided (ie, after the taking of evidence stage), the judge, having made the parties state their conclusions, schedules the hearing for the final discussion of the lawsuit and issues the judgment as a result of this hearing.

The judgment is a decision on the merits by which the judge decides if to uphold or to deny the class action and is published in the court telematics system portal by 15 days as of the issuance.

Article 140bis of the Consumers' Code (Legislative Decree No. 206 of 2005 as Amended by Legislative Decree No. 28 of 2023) and Following

This is a specific class action which can be brought only by consumer associations that meet certain requirements and are included in a specific register maintained by the Ministry of Enterprises and Made in Italy, as well as by independent public bodies (e.g., Bank of Italy, Consob, IVASS, AGCM, Data Protection Authority). It can concern violations of "collective interests of consumers" exclusively in the areas listed by the legislator in a specific annex to Legislative Decree 28 of 2023 (which, among other things, includes legal provisions regarding unfair terms, unfair commercial practices and misleading advertising) and allows for the request of compensatory measures (and therefore also for damages and restitution), or injunctive relief.

Class Actions Issued in Italy

Italian class actions are published in the telematics system portal of the Ministry of Justice. Hereafter the link to the comprehnsive list of pending and concluded class actions: servizipst.giustizia.it/PST/it/pst_2_16.wp?actionPath=/ExtStr2/do/classaction/ricercaClassAction&currentFrame=8.

A class action with regard to the protection of personal data was issued in 2022 against **Nexi** (which is an Italian leading company operating in the digital payment sector) before the Court of Milan. The case regarded the claim for compensation for damages against Nexi for "phishing" frauds suffered by clients in connection with online payments. It results extinguished.

Netflix is also currently party to a class action proceeding pending before the Court of Rome issued by an association of consumers regarding the allegation of illegitimacy of contractual terms for being in breach of the Consumers' Code for being disproportionate in favour of the enterprise in detriment of the consumers.

In consideration of the recent reform of class action and precisely in consideration of the provision of a general class action regime (falling out of the scope of the Consumers' Code), it is reasonable to expect an increase in the issuance of class actions in case of data breach incidents.

Saudi Arabia

KSA civil procedure does not provide a general class action avenue of remedy; outside capital-markets disputes, plaintiffs ordinarily must sue individually (multi-plaintiff joinder/consolidation is discretionary and governed by ordinary civil-procedure rules). By contrast, the only formal class-action framework today is in the securities arena under the Resolution of Securities Disputes Proceedings Regulations (**RSDPR**) administered by the CRSD/ACRSD. Please see the following for more info: RSDPR_en.pdf. There are no key class actions that exist to date in the cybersecurity sphere.

Norway

As far as we know, there have not been any class actions in Norway related to data breaches. More generally, class actions are a somewhat rare occurrence in Norway.

Turkey

Turkish law does not recognise class actions. There is a limited group action mechanism regulated under the Turkish Civil Procedure Code No. 6100 which allows certain associations and other legal entities to initiate proceedings to protect the rights of their members or a specific group, but only in cases explicitly permitted by law and without possibility of claiming individual compensation on behalf of those represented.

Therefore, such actions generally aim to establish or prevent a legal situation or to obtain a declaratory judgement. Apart from this mechanism, Turkish law provides no other procedural framework equivalent to class actions, and collective redress is typically pursued through joinder of parties or consolidation of similar claims within standard litigation procedures.

In the event of a breach of data protection obligations, the claimant may file a complaint before the Personal Data Protection Board to seek an administrative investigation and potential sanctions, in addition to initiating a civil action for compensation before the competent courts and where the breach also constitutes a criminal offence, filing a criminal complaint.

Sweden

It is possible to bring class actions in Sweden for failures to comply with the security requirements under the GDPR (Art 80 GDPR). In Sweden, there is an opt-in system for class actions i.e., individuals concerned must actively opt-in to participate in the class action.

We are not aware of any key class actions regarding data breaches in Sweden.

Poland

Collective redress is governed by the Act of 17 December 2009 on pursuing claims in group proceedings (consolidated text: Journal of Laws 2024, item 1485), allowing groups of at least ten claimants to sue for homogeneous claims based on the same factual grounds.

The Act applies to cases concerning claims arising from liability for damage caused by a dangerous product, from torts, from liability for non-performance or improper performance of a contractual obligation, or from unjust enrichment and, with respect to consumer protection, also in other matters, including cases for the determination of the use of practices infringing the collective interests of consumers or claims related to their use.

In group proceedings, the pursuit of claims for the protection of personal rights is excluded, except for claims arising from bodily injury or health disorder, including claims available to the closest family members of a person who has died as a result of bodily injury or health disorder.

While most personal data breaches are treated as infringements of personal rights — which generally cannot be pursued in group proceedings — there could be exceptions where a data breach may constitute a different form of tort. In such cases, class actions could be possible, offering both compensation and injunctive relief. However, group proceedings remain rare in Poland due to procedural complexity and challenges in quantifying damages for each claimant.

According to publicaly avaialble records, to date, no class actions related to data protection breaches have been brought in Poland.

Outside the class mechanism, individual claims for moral damages resulting from unlawful disclosure of personal data have proliferated, often citing CJEU judgment C-300/21 — UI v. Österreichische Post AG. The amount of compensation awarded by the court in such cases is not high, however, and aligns with the general European trend. Polish courts have awarded so far between PLN 1,000 and PLN 20,000 as a compensation to claimants.

England and Wales

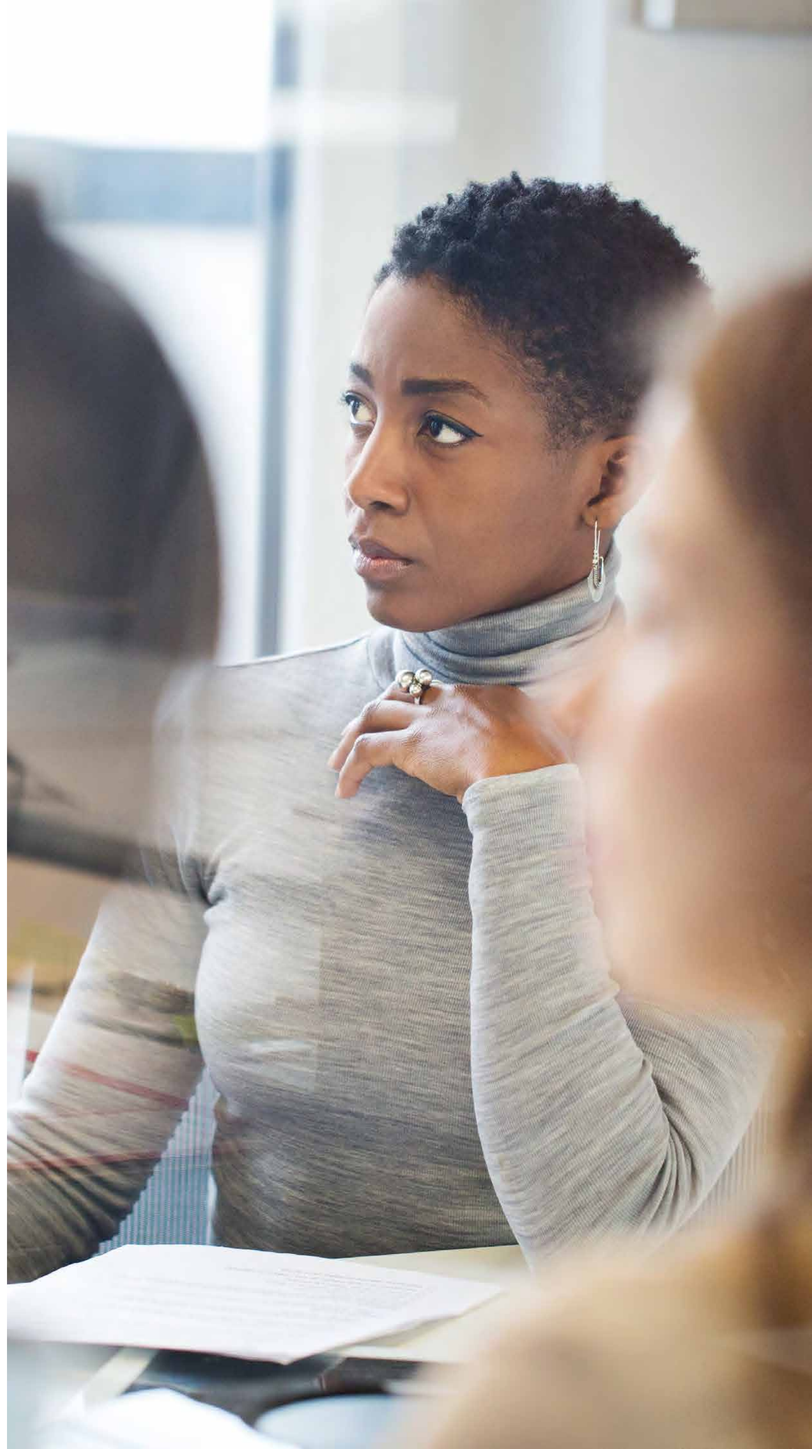
Following the Supreme Court's ruling in Lloyd v Google in 2021, there is no opt-out class action mechanism for bringing mass data breach claims because claimants cannot satisfy the requirement of an identical interest across the group. Although the Court suggested that "bifurcated proceedings" might allow representative actions on common issues, followed by individual assessments of loss, this procedural model has not been attempted. At the time of writing, the approach preferred by claimants and the lawyers who represent them is an "omnibus claim" adopting a "lead claimant model", where multiple individual claims are brought together and common issues are addressed by evaluating a representative sample. It appears that Courts and parties currently view this as a more efficient solution than a Group Litigation Order.

A notable mass data breach claim is presently being brought against Capita, following a cyber incident in March 2023 when the data of 6.6 million individuals was stolen. After the claim had been commenced, in October 2025 the UK ICO fined the relevant Capita entities GBP 14M for failing to implement technical and organisational measures in connection with the incident. Key failures included the inability to prevent privilege escalation and lateral movement, a failure to fix known vulnerabilities, inadequate incident response (taking 58 hours to quarantine a device against a one-hour target) and a lack of routine penetration testing and risk assessment for critical systems.

Ireland

Before 2024, it was not possible for groups to take class action lawsuits in Ireland. That position was changed with the introduction of the Representative Actions for the Protection of the Collective Interests of Consumers Act 2023, which was commenced on 30 April 2024.

This act introduces class actions for the protection of collective interests of consumers. Irish consumers can now take collective actions before the High Court through a body known as a qualified entity (QE), which is a legal person or public body representing consumer interests which has been designated by the Minister for Enterprise, Trade and Employment. The QE operates as the plaintiff in representative actions. The types of claims that a QE can take are somewhat limited.



In May 2025, the High Court granted the Irish Council for Civil Liberties (ICCL) permission to take Ireland's first ever class action. This action targets Microsoft's online advertising business. The ICCL alleges that Microsoft's real-time bidding advertising system collects users' sensitive personal data and then allows this data to be shared with third parties. It alleges that this system raises concerns under GPDR regarding user consent, data security and data processing.

It remains to be seen what the outcome of this class action will be. Finally, it is worth noting that in Ireland there are very tight restrictions on third party litigation funding (essentially prohibiting it).

Germany

European and German law does not provide for class actions in the actual sense, meaning an individual suing on behalf of a group.

In practice, there are five equivalents and mechanisms for collective actions (we assume you are dealing with GDPR already):

- Remedial action (Abhilfeklage);
- Model declaratory action (Musterfeststellungsklage);
- Representative action for unfair competition practices;
- Representative action for infringement on consumer protection laws; and
- Group action for collection.

Remedial Action (Abhilfeklage)

Directive (EU) 2020/1828 obliges Member States to allow representative actions for the protection of the collective consumer interests.

Consumer interests are affected by violations of the provisions of Union law referred to in Annex I of the Directive (EU) 2020/1828 (see Art. 2[1]). This includes violations of the GDPR (Annex I Nr. 56).

The threshold, at which consumer interests become "common", is not specified in the Directive. The German legislator requires the infringement to possibly affect at least 50 consumers. This low quantity and standard of proof is usually met in cyber incidents.

Claims must be "essentially comparable" (Sec. 15 VDuG, *Gesetz zur gebündelten Durchsetzung von Verbraucherrechten*, Act on the Bundled Enforcement of Consumer Rights). They can aim at any specific performance, including damages or cease-and-desist.

Only qualified entities may bring an *Abhilfeklage*:

They must be independent non-profits constituted in compliance with the national law of the Member State (Art. 4(3) Directive (EU) 2020/1828).

Furthermore, they must be recognised in the relevant Member State. In Germany, this requires registration pursuant to Sec. 4a UKlaG (*Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen*, Law on injunctions for consumer rights and other violations), which is granted when the entity has a membership of least 75 natural persons or 3 associations and has been registered in the associations registry and enacted its purpose for at least one year prior.

In most cases, the *Abhilfeklage* will proceed as follows:

- A qualified entity brings an *Abhilfeklage* before the Higher Regional Court.
- The court will publish the *Abhilfeklage* in the register for representative actions, allowing consumers to register as participants.
- If the suit has merits, the court will issue a basic judgment, which contains the conditions under which consumers are entitled to the specific performance sought in the *Abhilfeklage* (Sec. 16(2)(1) VDuG).
- Generally, the court will encourage the parties to a settlement (Sec. 17[1] VDuG).
- If the case is not settled and the basic judgment becomes legally binding, the court will issue a final remedial judgment (*Abhilfeeendurteil*, Sec. 18 VDuG). If the claimants sought damages or other monetary compensation, the court will determine a collective sum to be paid to a trustee (Sec. 19 VDuG).
- Consumers that fulfil the requirements set out in the basic judgment will receive their share from the trustee.

Model Declaratory Action (Musterfeststellungsklage)

The *Musterfeststellungsklage* (Sec. 1-13 VDuG) allows qualified entities (see above) to sue for ascertainment of a claim (e.g., damages, cease and desist or specific performance). The claim must possibly involve at least 50 (registered) consumers and a commercial entity.

After a declaratory judgment, consumers must still pursue individual actions. In these separate lawsuits, courts is bound by the ascertained facts of the *Musterfeststellungsklage*, e.g., whether a violation of duties occurred or if the defendant acted with fault. However, the court will still assess the damages on an individual basis.

Musterfeststellungsklagen are commonly introduced by consumer protection associations against large online enterprises, such as a Musterfeststellungsklage against Meta Platforms Ltd., seeking damages for data leaks.

Representative Action for Unfair Competition Practices

If Controllers disregard their duties, competitors or qualified entities can sue for cease and desist and elimination pursuant to Sec. 8(3), 3a UWG (*Gesetz gegen unlautere Geschäftspraktiken*, Law against unfair competition practices). Courts have confirmed the possibility of such actions for Art. 5(1)(c), 9, 13 et. seqq. and 25(2) GDPR and may extend this to Art. 32 GDPR if a cyber incident was caused by insufficient TOMs.

Representative Action for Infringement on Consumer Protection Laws

Qualified entities may sue for cease and desist and elimination (in their own name) if a company infringes on consumer protection laws, including the GDPR (Sec. 2(2)(13) UKlaG).

Group Action for Collection

An increasingly popular option is a group action for collection, where the claimants will buy and get transferred a large quantity of individual, low-value claims and asserts them as their own. Consumers consider this option advantageous as they receive immediate compensation without any involvement in lawsuits. Current examples include the abovementioned Meta leak.[129]

129. Sammelklage gegen Facebook wegen Datenleck | Verbraucherzentrale.de.

Spain

Article 80 of the GDPR allows Member States to empower consumer associations to take action against violations of the rights established therein and does not require that such associations be constituted specifically for the purpose of acting in the field of data protection. In Spain, the LOPDGDD does not provide for any provision in this regard.

Nonetheless, Spain recognises a mechanism for collective redress anchored in Article 11 of the Civil Procedure Act, which enables consumer associations to bring actions and seek protection for collective interests, including providing public notice to allow affected individuals to join. The currently prevailing model is considered an opt-in, and Spain has historically experienced fewer large-scale data breach collective damages actions compared to other EU countries.

While there have been individual and group claims, and consumer associations have been active in the data-protection arena, the absence of an opt-out mechanism has moderated the scale of cybersecurity-related mass damages litigation to date.

That landscape is now shifting, however, as a result of the transposition of the EU Representative Actions Directive. In February 2025, the Council of Ministers approved a draft bill to introduce a dedicated collective actions procedure into the Civil Procedure Act. The draft provides for an opt-out mechanism for redress actions below certain per-beneficiary thresholds, for public notice via an electronic platform, for qualified entities and the Public Prosecutor to bring actions and for the appointment of a liquidator to distribute lump-sum redress.

Once enacted, the new regime is expected to materially increase litigation risk for large-scale data breaches, especially in sectors such as telecommunications and financial services, where group claims are already more frequent.

Netherlands

Cyber incidents and data breaches are prompting class actions in the Netherlands. The applicable mechanism is the Act on Redress of Mass Damages in a Collective Action (hereafter: WAMCA). This relatively new act allows for collective actions, also in the case of personal data breaches.

Under WAMCA, a foundation or organisation may bring a class action on behalf of affected individuals provided it meets certain requirements — for example being sufficiently representative.[130] It may not operate for profit.

Since WAMCA came into effect on 1 January 2020, data breach class actions have been filed. For example:

- A data breach at Oracle, concerning personal data of internet users.[131]
- A data breach of corona test and vaccination data at the Municipal Health Service (GGD).[132]

A class action is also expected in connection with a recent breach of Clinical Diagnostics, a laboratory by Stichting Bevolkingsonderzoek Nederland.[133] In early July 2025, the hacker group Nova compromised the company, stealing and publishing on the dark web personal data of women who participated in a cervical cancer screening, including personal identification numbers and medical information. Instead of promptly reporting the incident, Clinical Diagnostics first negotiated directly with the attackers and paid money to keep the breach quiet. Affected individuals can now register for the class action. Next steps remain unclear.

130. Art. 3:305a DCC.
131. Court of Amsterdam 29 December 2021, ECLI:NL:RBAMS:2021:7647; Court of Appeal of Amsterdam 18 June 2024, ECLI:NL:GHAMS:2024:1651. It is however important to note that in the appeal, the claim foundation no longer based its case on a data breach, but on the violation of internet users' privacy rights.
132. Court of Amsterdam 17 July 2024, ECLI:NL:RBAMS:2024:4264.
133. More information about this data breach can be found at: Datalek bevolkingsonderzoek blijkt nog groter: zeker 700.000 vrouwen getroffen. Information about the class action: datalekbevolkingsonderzoek.nl.

France

Procedural Mechanism for Bringing Class Actions in France

Class actions were introduced in France in 2014 (French law n° 2014-344 of 17 March 2014), initially limited to consumer claims and anti-competitive practices. In 2016 (French law n° 2016-1547 of 18 November 2016), a class action regime was introduced for disputes over the processing of personal data.

The French law n° 2025391 of 30 April 2025 transposed the EU Representative Actions Directive (2020/1828) and unified France's class action regime for class actions initiated on or after 3 May 2025. The class action related to protection of personal data is therefore now subject to the common rules governing class action proceedings.

As a result of this new regime, where several natural and/or legal persons in a similar situation suffer damage caused by a common breach of the provisions of the GDPR or the French Data Protection Law by a personal data controller or processor, a class action may be brought before the competent court. The action may be brought either to put an end to the breach (injunction class actions) and/or to hold liable the person who caused the damage in order to obtain compensation for the material and moral damage suffered (compensation class actions). Eight specialised courts (Bordeaux, Lille, Lyon, Marseille, Nancy, Paris, Rennes, Fort-de-France) have exclusive jurisdiction to hear class actions.

Under the new regime, class actions remain the prerogative of approved associations, which must demonstrate conditions of independence and transparency to apply for approval to bring class actions. Class actions are also available, under more restrictive conditions to: (i) non-profit associations which can bring injunction class actions only if they have been duly registered but not approved, can demonstrate twenty-four months of effective and public activity and their statutory purpose includes the defence of interests that have been infringed, (ii) representative unions, which can bring class actions related to discrimination and protection of personal data and (iii) the public prosecutor who may also bring, as principal party, injunction class action or intervene in an on-going injunction or compensation class action.

The reform further allows the pre-trial judge to order interim measures to halt any breach that would result in a clearly unlawful disturbance, or to prevent imminent harm.

Key Class Actions

In practice, filings and awards remain limited in France to date, though the reform is expected to spur more cases. Collective actions following major incidents (e.g., in health and telecoms, action by the Association for Assistance to Parents of Children Suffering from Anticonvulsant Syndrome [APESAC] or Class action lawsuit against Free Mobile) have occurred but are not yet widespread.

Switzerland

Current Swiss law does not know a procedural mechanism for bringing class action suits. Accordingly, cyber incidents have not been prompting data breach class actions in Switzerland.

The Swiss Civil Procedure Code (CPC) only provides for the option of a so-called voluntary joinder according to which two or more persons may jointly appear as plaintiffs provided rights and duties resulting from similar circumstances or legal grounds are to be assessed, the individual cases are not subject to different types of procedure and the same court has material jurisdiction.[134] In such a case, each party must present their full case before the court, alleging the necessary facts and submitting the necessary evidence. Accordingly, each of the joint parties may also proceed independently from the others.[135]

134. Article 71 para. 1 CPC.
135. Article 71 para. 2 CPC.

6

What Other Post-Incident Disputes are you Seeing?

Chapter Summary

Cyber incidents can trigger a wide range of legal disputes, requiring organisations to adopt a holistic approach to risk management, contractual governance and stakeholder engagement.

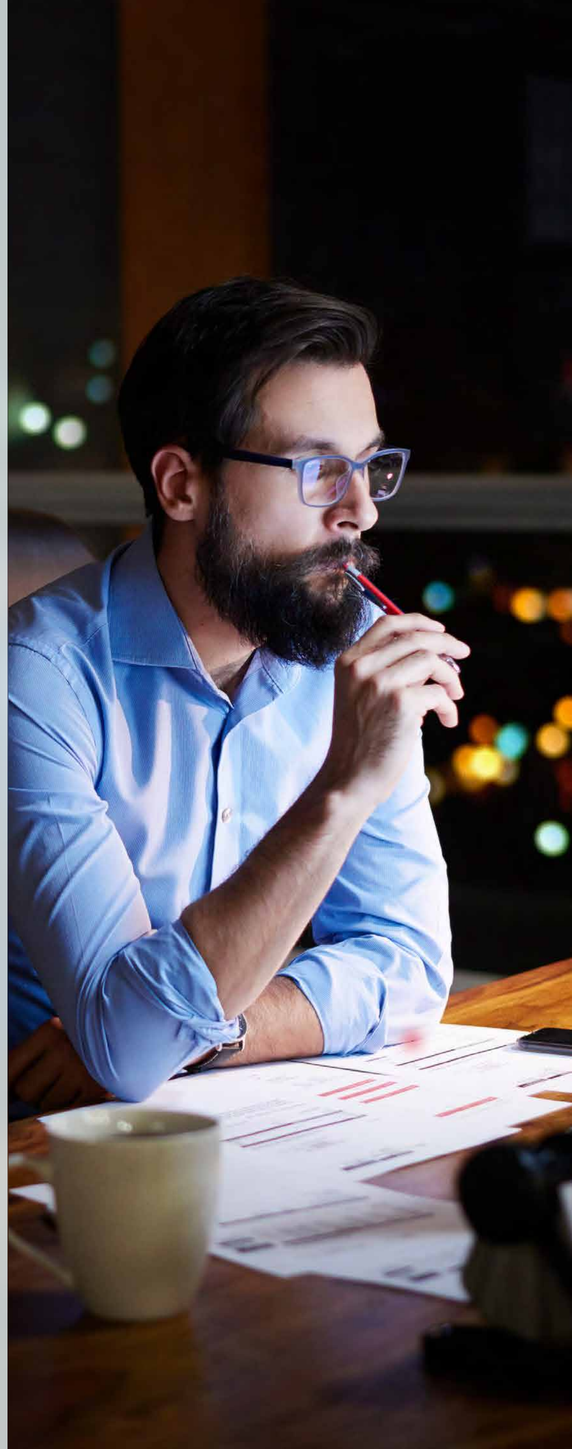
There is an increasing use of arbitration and alternative dispute resolution to post incident disputes, as well as a growing importance of the inclusion of clear contractual terms in contracts and robust due diligence in managing third-party risk.

Examples of this kind of litigation includes contractual disputes between organisations and their service providers, particularly regarding the adequacy of cybersecurity measures, incident response and indemnification obligations. There is potential for litigation over regulatory investigations, the proportionality of sanctions and the adequacy of technical and organisational measures.

Disputes can also arise over the classification of entities under regulatory frameworks, the allocation of liability in supply chains and the application of contractual provisions such as force majeure clauses.

Practical Actions for Organisations to Consider Now

- Review contracts and SLAs for clauses relating to the clear allocation of cyber risk and incident response obligations. Ensure force majeure and indemnity provisions address cyber incidents.
- Negotiate clear service levels and remedies: specify the obligations and liabilities that suppliers and partners need to uphold, as well as minimum security standards and insurance.
- Conduct regular supply chain risk assessments: evaluate vendor resilience and incident response capabilities.



Belgium

We increasingly see post-incident litigation, both against the entities that have been the victim of a cyber incident and their managers resp. directors, for having taken inadequate steps to protect against and mitigate the effect of cyber incidents. Such claims are being brought in contract and in tort.

Luxembourg

Although no high-profile cyber related litigation has yet arisen in Luxembourg, the risk environment is changing rapidly. DORA obliges financial entities to comply with their obligations and notably renegotiate critical ICT outsourcing agreements by January 2025. The CSSF and CAA have indicated informally that enforcement will begin in 2026.

Portugal

Despite the absence of significant cases in the Portuguese context, we have chosen to set out two topics (non-data related) which we consider will be particularly relevant and likely to be the subject of disputes once the European legislative package has been fully implemented in Portugal.

Firstly, we must consider business interruption. In fact, disputes over who is liable when a supplier's system failure (like a ransomware-induced shutdown or software bug) interrupts a client's business are expected to arise, even if no personal data is exposed. These disputes can become particularly complex when they involve suppliers and third-party service providers. Regarding the breach of service levels agreements (SLAs), these may result in both contractual and extra-contractual liability.

Secondly, disputes concerning the classification of entities as 'essential' or 'important' under the NIS2 Directive and its national implementation are also anticipated. Undeniably, the designation as 'essential' entails more stringent regulatory requirements, ex-ante supervisory measures and higher fines and penalties. Therefore, it is foreseeable that a significant number of disputes will emerge regarding the procedural mechanisms and legal expedients employed to challenge or avoid such classifications by the National Cybersecurity Centre (**CNCS**), the administrative authority responsible for ensuring compliance with NIS2 and, in the future, with the proposed implementing law (as set out in the Article 8 of the Draft Law No. 7/XVII).

Finland

Disputes following cyber incidents are common in Finland, particularly when they occur through a third-party service provider. In such cases, the agreements between those involved are reviewed to establish the service provider's liability and any potential remedies.

As these disputes do not enter any court proceedings, they are usually not public. Instead, settlements are usually negotiated between the parties involved, or through alternative dispute resolution methods such as arbitration.

South Africa

Contractual disputes between responsible parties and their operators are increasingly common, however, we are not aware of any reported judgments in this regard. Anecdotally, such disputes typically arise under service-level or operate agreements and tend to concern failures to implement or maintain appropriate security safeguards, or to meet restoration and uptime commitments.

Furthermore, commercial contracting parties are advised to proactively address cyber incidents in their agreements, for example through force majeure clauses.

Force majeure clauses are contractual in nature and cover events beyond a party's control, such as natural disasters, war, terrorism or pandemics, that prevent contractual performance. However, given the frequency and impact of cyberattacks, parties may now consider expressly including cyber incidents (e.g., ransomware, system compromise, or denial-of-service attacks) within the scope of agreed force majeure events. Local courts tend to construe force majeure clauses restrictively, therefore cyber incidents must be expressly listed or may not be treated as qualifying events.

The inclusion of cyber events in force majeure clauses can serve two purposes:

- firstly, to relieve a party from performance obligations where a cyberattack disrupts operations; and
- secondly, to limit or exclude liability where one party suffers loss and the other seeks to avoid responsibility.

However, such clauses must be carefully drafted and would only regulate obligations and liabilities as between the contracting parties, and would not override or displace the statutory duties imposed on the responsible party under POPIA.

Italy

Other post-incident disputes may include inter alia:

- Contractual disputes among clients and suppliers of for the realisation of digital services.
- Disputes among data centre owners and/or managers and contractors which built the data centre for inadequacy of the archives and storages (ie, for contractual defaults under the data centre construction contract).
- Disputes among business for reputational damage suffered by commercial partners in connection with the data breach incident (although the commercial partner did not directly suffer it).
- Disputes for supply chain interruption.
- Disputes for contractual defaults towards third parties caused by the business damage/interruption caused by the data breach incident.
- Cyber insurance disputes.
- Disputes for environmental damage (e.g., in case of attack to industrial systems which causes the incident).

Saudi Arabia

Aramco had about 1 TB of data leaked not through a direct hack of Aramco, but via a third-party contractor's security lapse. The contractor (unidentified publicly) had Aramco data which got exposed. In such a case, Aramco could have a strong claim against that contractor for a breach. While details of any legal action are not public (Aramco likely handled it privately), this incident underscores the risk in which big companies will hold their smaller vendors accountable if the latter's weaknesses cause a loss.

In KSA, many contracts include arbitration clauses (often through local arbitration centre/ad hoc). So, some cyber related vendor disputes might be resolved in arbitration, which is private. But in our view, as dependence on third-party cloud and IT providers grows (which is a major trend under Vision 2030's digital transformation), we expect more such disputes to be public. Internationally, this has been seen and KSA companies are becoming similarly assertive.

There is also a statute in KSA called the Regulation for Protection of Confidential Commercial Information. It is, in essence, a law that protects trade secrets and provides a harmed party with a private cause of action against a violator who misappropriated the harmed party's trade secrets. One could imagine scenarios where cyber incidents may fall under the purview of this regulation to the extent that trade secrets get exposed.

Norway

As previously stated, the fine imposed on Grindr LLC by the DPA is currently being challenged in the Court of Appeals, which in August 2025 is set to decide whether the fine is valid or not.

Turkey

We are not aware of any post-incident disputes to highlight in particular. Companies may seek recourse based on the existing contractual relationships.

Sweden

Cybersecurity incidents may result in claims for compensation for material or non-material damage by affected individuals under the GDPR (Art 82 GDPR). Further, cybersecurity incidents may result in contractual claims in business-to-business relations against service providers that have not implemented sufficient security measures as stipulated in the contract.

Poland

Claims against Managed Security Services Providers and business-to-business claims are fully permissible under Polish law in connection with improper performance or non-performance of a contract concluded between the provider and the recipient of such services. Nevertheless, there is no information in publicly available sources about any ongoing proceedings of this type that have arisen from a cyber incident.

England & Wales

While there have been relatively few reported court judgments in England and Wales, the disruption caused by cyber security incidents provide fertile ground for disputes.

In addition to data protection claims discussed elsewhere in this survey, notable categories of litigation include:

- Contractual disputes: where a victim organisation is unable to meet its contractual obligations to customers or suppliers, claims for compensation may follow. Although the nature of these claims varies between contracts, they commonly turn on whether the victim complied with contractual IT security requirements, breached service level agreements, the effect of any exclusion or limitation of liability clauses and the extent to which the claimant can establish its loss.
- Wider commercial disputes: while contractual disputes for disruption related losses may be the most common other forms of commercial dispute also arise. Recent examples include Lonestar Communications v Kaye & Ors, in which the claimant successfully recovered losses arising from a campaign of multi-vectored Distributed Denial of Service Attacks carried out by the defendants and CMOC Sales & Marketing Ltd v Persons Unknown & Ors, where the claimant was able to recover stolen funds of approximately USD 1.5M following a business email compromise, via a series of worldwide freezing orders and proprietary injunctions. Cyber insurance coverage disputes are also possible although, as yet, there have not been any reported judgments in this jurisdiction.
- Claims against Managed Security Service Providers (MSSPs): claims against MSSP and other IT security advisers, are regularly contemplated following an incident. Their viability generally depends on whether the adviser breached its duties in a causally relevant way and on the scope of any contractual liability caps or exclusion clauses.
- Injunctions: victims of cyber-attacks involving data theft may occasionally seek an interim or final injunction preventing the attacker from using or disclosing the stolen data. When such injunctions are obtained, they are made against ‘persons unknown’ (XXX v Persons Unknown being one such example where the claimant also obtained an anonymity order, as indicated by the case name).
- ICO appeals: section 162 of the DPA 2018 entitles any person who receives an information, assessment, enforcement or penalty notice to appeal to the First-Tier Tribunal for its variation or cancellation. As well as a number of fines by the ICO having been reduced following dialogue with the affected data controllers, there have been a number of appeals under this section (most notably in the cyber incident context, DSG Retail Limited v Information Commissioner).

These categories are not exhaustive. They illustrate the wide-ranging contentious potential of cyber incidents — on par with other disruptive events that can expose weaknesses in contractual, operational and governance arrangements.

Ireland

Disputes Between Data Subject and Data Controller or Processor

Article 82 of the GDPR grants the right of compensation to data subjects whose rights under the GDPR have been infringed. Such compensation may be sought against any controller involved in the infringing processing or against any processor who did not comply with their obligations under the GDPR regarding their processing or who acted outside the scope of their instructions from the controller. Under the right to compensation, the data subject may seek material and/or non-material damages. Non-material damages

are generally described as damages which do not include any financial loss and instead concern claims of pain and suffering, emotional distress, anxiety and inconvenience.

Under Section 117 of the DPA 2018, a data subject whose data was involved in a data breach may bring a 'data protection action' against the controller or processor who was involved in the breach. This action and the possible judicial remedies are separate from any complaint to or action by the DPC.

In a data protection action, a data subject may be entitled to remedies including injunctive relief and material or non-material monetary damages. The recent Irish case of Dillion v Irish Life [2025] IESC 37 concerned a claim for non-material damages, specifically for distress, upset, anxiety, inconvenience and loss, under section 117 of the DPA 2018 in relation to a breach of the plaintiff's personal data held by the defendant. The Supreme Court held that actions for anxiety or distress by data subjects under the DPA 2018 are not personal injuries actions and therefore do not need to follow the prescribed legislative process for taking personal injury action in Irish courts. However, the Court made clear that any potential award that is solely for metal distress would be "very modest". By distinguishing this type of data breach claim from personal injuries actions, there are now fewer procedural hurdles to clear for data subjects who wish to bring an action for distress and anxiety under section 117 of the DPA 2018.

Disputes Between the Data Controller and Data Processor/ Service Provider and Customer

In the event of a data breach, actions between data controllers and data processors may occur in order to determine which party is primarily responsible for the breach and if they need to indemnify the other party against any further actions by impacted data subjects or regulators.

There may also be actions for breach of contract between a service provider and their customer. Many of the law and regulation mentioned above, such as DORA and NIS2, require parties to include in their contracts certain requirements and obligations around their cybersecurity and ICT services. If a service provider is found to have had a data breach, this may be evidence that their systems are not secure, and they may be in breach of some of their contractual provisions with their customers. Customers may then be able to sue for damages arising out of any costs of replacing the service provider or for disruption to their business.

UAE

Class actions are not available in the onshore UAE.

For the DIFC and ADGM, while their respective courts do not have any laws or procedures for class action proceedings, the courts are empowered to make a group litigation order to manage claims which give rise to common or related issues of fact or law. Such an order can also be sought by application.

Germany

We see a trend to sue contractual partners for damages, e.g., service providers that caused the breach, including based on “full GDPR compliance” clauses in contracts.

There is also a trend in Germany of consumer law firms to sue individually (i.e., no class action) for damages under Ar. 82 GDPR. Many consumers in Germany have legal insurance that covers court and legal fees, so it’s easy to go to court in Germany.

Furthermore, some claim collection agencies are heavily advertising to the German market for GDPR damages claims, e.g., Privacy Reclaim against Google for alleged GDPR non-compliance of Android.[136]

Spain

Cyber incidents in Spain can generate business-to-business disputes beyond regulatory enforcement and consumer claims. Controllers may pursue claims against processors and other vendors under GDPR allocation and under contractual indemnities for failures to meet contractual service levels or industry standards. Processors and ICT vendors may face negligence and professional-liability claims tied to incident causation and response gaps. Additionally, payment-related incidents may trigger disputes over Payment Card Industry Data Security Standard non-compliance assessments.

Netherlands

There are three cases we would like to highlight:

A Judgment Dated 6 April 2023 of the Court of Rotterdam[137]

In April 2023, the Rotterdam District Court ruled in a summary proceeding between Blauw Research B.V. (Blauw), a market research company and Nebu B.V.(Nebu), its IT service provider, following a significant cyberattack on Nebu’s systems. The attack resulted in the theft of data, potentially affecting many of Blauw’s clients. Blauw demanded detailed information about the incident, the measures taken by Nebu, and an independent forensic investigation, citing their data processing agreement. The court found that Nebu was obliged to fully cooperate and provide extensive information to Blauw, including details about the attack, the recovery process and any data exfiltration. The court also ordered Nebu to commission an independent forensic investigation and to keep relevant data available for further analysis. Deadlines and financial penalties were set for non-compliance, emphasising the importance of transparency and cooperation in handling data breaches under contractual and data protection obligations.

A Recent Judgment Dated 29 January 2025 of the Court of Rotterdam[138]

This is a follow-up case of the previous. In this court case, Blauw alleged that Nebu failed to implement adequate security measures and breached its contractual obligations, and it is seeking damages. The court has not yet issued a ruling on the merits as an expert was assigned to assess security measures in place at Nebu.

136. privacyreclaim.com.
137. Court of Rotterdam 6 April 2023, ECLI:NL:RBROT:2023:2931.
138. Court of Rotterdam 29 January 2025, ECLI:NL:RBROT:2025:1497.

A Recent Case Dated 26 March 2024 of the Court of Midden-Nederland[139]

In this case, the Dutch DPA sought information from a hosting provider following a data breach, but when the provider only partially complied, the AP demanded the investigation report directly from Northwave Nederland B.V., a third party not under its direct supervision, and imposed a penalty for non-compliance. The court found that the AP should first exhaust its supervisory powers over the hosting provider — the main subject of the investigation — before turning to third parties like Northwave. Since the AP had not shown that the hosting provider would refuse to comply if a penalty was imposed, the court ruled that demanding information from Northwave was disproportionate and unnecessary at this stage. As a result, the court temporarily suspended the enforcement of the AP's penalty decision against Northwave until two weeks after the objection procedure is completed and ordered the AP to pay Northwave's legal costs, emphasising the need for proportionality and subsidiarity in regulatory enforcement actions.

France

Beyond data breaches, cyber incidents in France can trigger a range of post-incident disputes grounded in various legal sources.

- Regulatory investigations, such as those conducted by the CNIL or sectoral authorities like the ACPR or ANSSI, may give rise to disputes over the interpretation of compliance obligations set out in sector-specific regulations (e.g., the French Data Protection Act, the NIS Directive as transposed by Loi n° 2018-133, or the Monetary and Financial Code). Disagreements may concern the proportionality of remedial measures or the technical standards required, as referenced in Article 32 of the GDPR or relevant ANSSI guidelines.
- Contractual disputes between service providers and clients often arise over the adequacy of cybersecurity measures, with parties invoking contractual liability under Articles 1103 and 1231-1 of the French Civil Code, which require parties to perform contracts in good faith and provide for damages in case of non-performance.
- In supply chain contexts, organisations may seek recourse against third-party vendors under Article 1240 of the Civil Code (general tort liability) if a vendor's security failure causes harm (i.e even in the absence of a personal data breach, affected individuals or business partners may bring civil claims for damages under Article 1240 of the Civil Code, seeking compensation for service outages, loss of business opportunities, or reputational harm, provided they can establish fault, damage and causation)

Switzerland

Cyber incidents may carry with them various post-incident disputes under Swiss law based on contract and/or tort. Firstly, data subjects may claim damages or satisfaction for a violation of their personality rights in connection with a cyber incident. Additionally, companies that were the target of a malicious cyber incident may claim damages from IT / IT security service providers for failing to sufficiently secure the IT systems of the company. Governing bodies may also be held accountable for failure to implement necessary security measures in civil court by their companies.

139. Court of Midden-Nederland 26 March 2024, ECLI:NL:RBMNE:2024:1804.

7

Under the EU AI Act

What are the applicable cybersecurity duties? What are the potential consequences (i.e., fines and penalties) arising from a security breach impacting a high-risk AI system, including where the security breach involves the loss of personal data?

Chapter Summary

The EU AI Act imposes strict cybersecurity requirements for providers and deployers of high-risk AI systems. The Act mandates robust, lifecycle-wide cyber measures, including risk management, technical resilience, incident detection and reporting and human oversight.

Providers must conduct cybersecurity risk assessments, maintain detailed technical documentation and ensure systems are resilient against attacks such as data poisoning and model evasion. Non-compliance can result in substantial administrative fines — up to EUR 35M or 7 percent of global turnover for prohibited practices, and up to EUR 15M or 3 percent for failures in high-risk system requirements.

Where a security breach involves personal data, parallel enforcement under the GDPR may lead to cumulative penalties.

Organisations need to integrate cybersecurity into AI system design and operation, maintain ongoing monitoring and compliance and prepare for multi-regime enforcement. They also need to be mindful of reputational and operational risks associated with AI-related cyber incidents and the importance of proactive governance and cross-functional collaboration.

Practical Actions for Organisations to Consider Now

- Conduct AI risk assessments: document your cybersecurity measures and mitigation strategies and update them regularly.
- Implement security by design and by default: ensure all AI systems are resilient to attacks and data breaches, and staff are trained on AI-specific cybersecurity risks and compliance requirements.
- Maintain comprehensive technical documentation and event logs: facilitate regulatory review and incident investigation and ensure prompt reporting of serious incidents to authorities.
- Be prepared for multi-regime compliance: your AI systems may be subject to overlapping requirements under the EU AI Act, GDPR, NIS2 and sectoral laws.

Belgium

The EU AI Act[140] imposes specific cybersecurity obligations, especially for providers and deployers of high-risk AI systems. These duties are designed to ensure that AI systems are robust, secure and resilient against cyber threats throughout their lifecycle. As an EU regulation, the EU AI Act is directly applicable in all Member States, including Belgium. Belgium is in the process of implementing the necessary national measures to enforce the EU AI Act, but as of August 2025, full implementation (including the designation of the competent authorities, establish enforcement mechanisms and define penalties) is not yet complete. The EU AI Act itself, however, is already in force and directly applicable in Belgium. The EU AI Act's cybersecurity requirements are complemented by other EU laws and regulations, such as the NIS2 Act, Cybersecurity Act and Cyber Resilience Act.

The key cybersecurity requirements for high-risk AI systems include:

- Operation of a risk management system that is iterative and covers the entire lifecycle of the AI system, including ongoing assessment and mitigation of cybersecurity risks.
- Implementation of robust security measures (accuracy, robustness and cybersecurity).
- Ensuring quality, integrity and confidentiality of data used by the AI system, including measures to prevent unauthorised access.
- Ensuring logging capabilities to record relevant events, which is essential for detecting, analysing and responding to cybersecurity incidents.
- Establishing procedures for monitoring, reporting and addressing vulnerabilities, including timely deployment of security patches and updates.
- Prompt reporting of serious incidents or malfunctions, including those resulting from security breaches.
- Assess and manage cybersecurity risks arising from third-party components, software, or data integrated into the AI system.
- Establishment of a post-market monitoring system to detect and address new risks, including cybersecurity threats, as they arise during the system's operation.
- Maintenance of up-to-date technical documentation detailing the security measures implemented, including risk assessments, mitigation strategies and incident response plans.
- Provide clear instructions to users (deployers) regarding the secure operation, maintenance and monitoring of the AI system, including guidance on cybersecurity best practices.

The EU AI Act establishes a tiered penalty regime for non-compliance, including breaches of cybersecurity obligations. The severity of the fine depends on the nature of the infringement:[141]

- Non-compliance with prohibited AI practices (e.g., manipulative or deceptive AI, biometric categorisation): administrative fines of up to EUR35M or, if the offender is an undertaking, up to 7 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher.[142]
- Non-compliance with high-risk AI system requirements: administrative fines of up to EUR15M or, if the offender is an undertaking, up to 3 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher.[143]
- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request: administrative fines of up to EUR7.5M or, if the offender is an undertaking, up to 1 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher.[144]

140. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act).
141. For SMEs and startups, the lower of the fixed amount or the percentage applies.
142. Article 99 (3) AI Act.
143. Article 99 (4) AI Act.
144. Article 99 (5) AI Act.

If a security breach results in the loss of personal data, the incident may also trigger obligations and penalties under the GDPR, where the BDPA can impose fines of up to EUR20M or 4 percent of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher. Hence, undertakings may face parallel investigations and sanctions from both EU AI Act and GDPR.

Luxembourg

The EU Artificial Intelligence Act (**AI Act**) places a duty to integrate cybersecurity by design on providers and deployers. Article 15 AI Act requires high-risk AI systems to be designed, developed and tested with state-of-the-art technical and organisational measures preventing unauthorised access, manipulation and adversarial attacks (data poisoning, model evasion, etc.) across the entire lifecycle, including post-deployment learning phases. Article 17 AI Act embeds those measures in a documented risk-management system that must be continuously updated. Article 26(5) AI Act also requires deployers to immediately inform the provider and the relevant market surveillance authorities when a serious incident is identified. The EU AI Office has emphasised that the AI Act marks a paradigm shift: cybersecurity must be treated as an integral feature of AI system development, not as a separate domain.

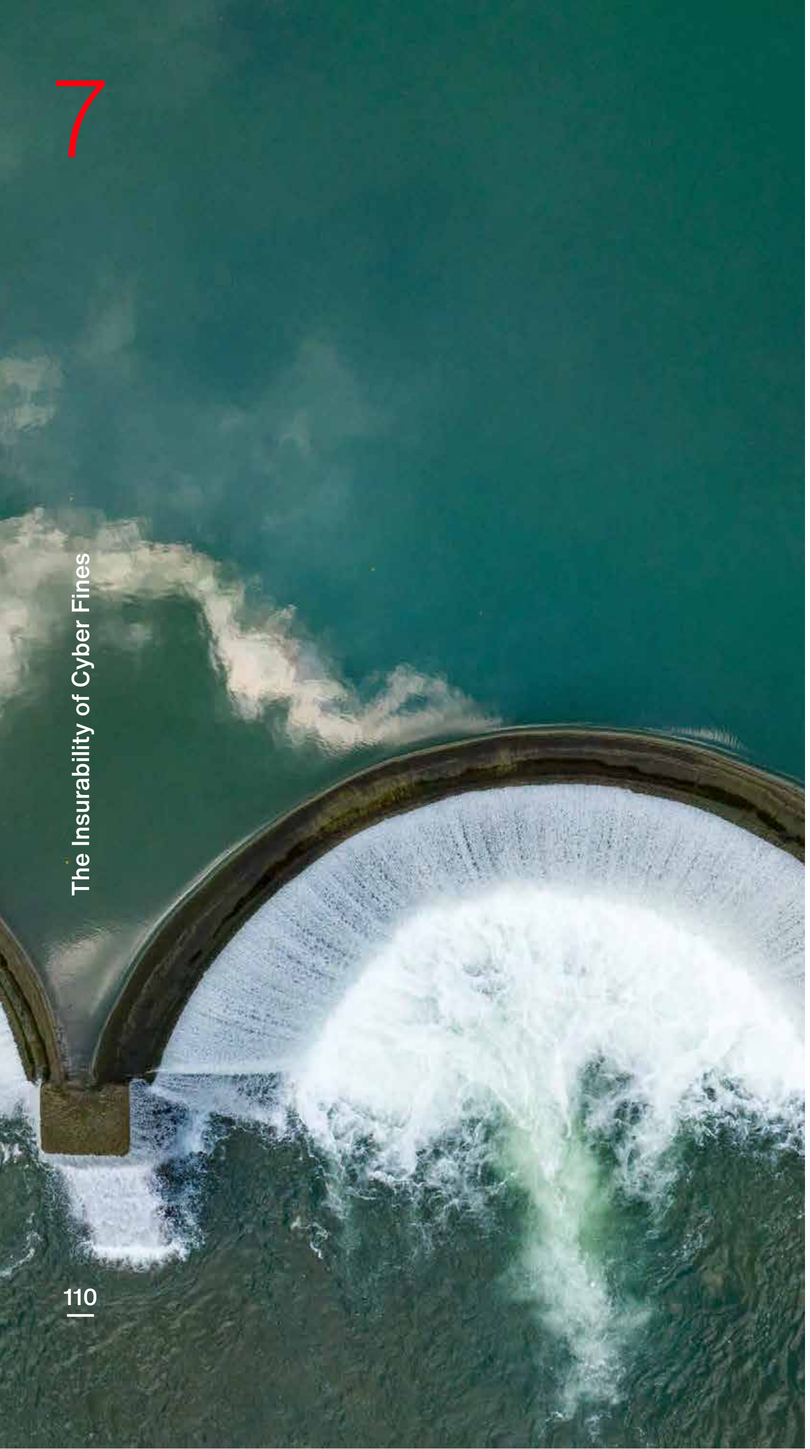
A security breach that reveals shortcomings in a provider's or deployers cybersecurity controls constitutes non-compliance with Articles 15 and 17 AI Act and may trigger the penalties set out in Article 99 AI Act (as a breach of Article 16[a] AI Act): up to EUR15M or 3 percent of total worldwide annual turnover (whichever is higher) for substantive infringements and up to EUR7.5M or 1 percent of worldwide turnover for supplying incorrect, incomplete or misleading information to authorities. Recital 10 clarifies that the AI Act is without prejudice to the GDPR; consequently, where the breach also entails a personal-data compromise, parallel enforcement by the CNPD under Articles 83(4)–(6) GDPR may lead to cumulative fines, subject to the principle of proportionality.

Portugal

The obligations are broad in scope and apply across the entire lifecycle of the system. They begin at the conceptual and design stages, covering the secure development of the system; continue through the ongoing monitoring and assessment of risks; and encompass mechanisms for timely incident reporting and effective response. Adequate human oversight is also required, as well as the maintenance of a robust quality management framework and strong governance over data, ensuring its confidentiality, integrity and availability at every stage of the system's operation.

Breaches involving high-risk AI systems that result from non-compliance with the obligations set out in the AI Act must be framed within the sanctioning regime set out in Article 99 of that Act, which can add up to fines up to EUR15M or 3 percent of the organisation's total worldwide annual turnover, whichever is higher. Nevertheless, it should be noted that the Portuguese legislator has not yet established the applicable sanctions, therefore, at present, the aforementioned sanctioning framework is not in force.

Additionally, if the security breach also involves the loss of personal data, the General Data Protection Regulation (GDPR) will apply, potentially imposing fines of up to EUR20M or 4 percent of the organisation's total worldwide annual turnover, whichever is higher.
In addition, such incidents may give rise to civil liability and litigation, enabling affected individuals to claim compensation for both pecuniary and non-pecuniary damages. Beyond the legal and financial repercussions, organisations should also account for the significant reputational harm that often follows high-profile security breaches.



Finland

The government proposal for national legislation to implement the EU AI Act is still being considered by the Finnish Parliament. The legislative process is expected to be completed in autumn 2025[6]. Consequently, the national provisions concerning cybersecurity duties or sanctions for breaching the duties have not yet been implemented. However, the proposed legislative model sets out applicable cybersecurity duties in accordance with the EU AI Act.

For example, administrative fines can be imposed on violations of cybersecurity duties as set out in Article 15 of the EU AI Act. Article 15 obligates, among other things, that high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness and cybersecurity and that they perform consistently in those respects throughout their lifecycle.

Such obligation, along with the various other conformity, quality and risk management system as well as documentation requirements that could affect the cybersecurity of high-risk AI systems is proposed to be set to the providers, importers, distributors, authorised representatives and deployers in accordance with the EU AI Act.

Therefore, the applicable cybersecurity duties under proposed national implementing legislation are distributed to the various parties involved in the value chain of different types of AI systems, as set out in the EU AI Act.

A security breach impacting a high-risk AI system could result in administrative fines for violating the aforementioned cybersecurity duties. The proposed national implementing legislation will set out the amount of the administrative fine imposed for breaching these obligations in accordance with the EU AI Act.

As the EU AI Act does not affect the application of existing EU data protection laws, a security breach involving a high-risk AI system could result in an administrative fine being imposed by the Office of the Data Protection Ombudsman in accordance with section 24 of the Data Protection Act.

Italy

Implementation of robust security measures: providers and users of high-risk AI systems must implement appropriate technical and organisational measures to manage risks related to the security of the system. This includes protection against unauthorised access, data breaches and manipulation of the system or its data.

Security by design and by default: high-risk AI systems must adhere to the principle of security by design and by default, ensuring that security is embedded from the earliest stages of development and maintained throughout deployment and operation.

Data governance: providers must ensure the integrity and confidentiality of data used in training, validation and testing and implement data governance measures to prevent and mitigate biases and vulnerabilities.

Incident detection and reporting: providers and deployers are required to have mechanisms in place to detect, respond to and resolve security incidents affecting high-risk AI systems. There is a duty to report serious incidents or malfunctions — including those impacting health, safety, fundamental rights, or critical infrastructure — to the relevant market surveillance authorities without undue delay.

Technical documentation and record-keeping: providers must maintain detailed technical documentation and automatic logging of events to ensure traceability and facilitate post-market monitoring and incident investigation.

Human oversight: systems must be designed to allow for effective human oversight, including the ability to intervene or shut down the system in the event of a security incident.

For non-compliance with requirements relating to high-risk AI systems (including cybersecurity duties): up to EUR15M or 3 percent of the total worldwide annual turnover (whichever is higher) for the preceding financial year.

For providing incorrect, incomplete, or misleading information to authorities: up to EUR7.5M or 1 percent of worldwide annual turnover (whichever is higher).

For non-compliance with prohibitions (e.g., use of banned AI practices): up to EUR35M or 7 percent of worldwide annual turnover (whichever is higher).

If a security breach of a high-risk AI system results in the loss of personal data, there may be overlapping obligations and penalties under the GDPR. The GDPR provides for fines of up to EUR20M or 4 percent of worldwide annual turnover (whichever is higher) for serious infringements, such as failure to implement appropriate technical and organisational measures to ensure data security.

Reputational Damage: Public reporting obligations and the right of individuals to lodge complaints may result in reputational harm.

Reporting and Cooperation: providers and deployers must cooperate with authorities during investigations and provide access to technical documentation and logs. Failure to report incidents or cooperate can itself be a ground for additional penalties.

Sweden

High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.

A security breach involving the loss of personal data may be subject to fines under the GDPR (see 1 above).

Poland

The EU Artificial Intelligence Act (hereinafter "**EU AI Act**") exemplifies a highly advanced risk-based approach to European regulation. One of its distinguishing features is the detailed classification of various risk levels associated with AI technology: (1) prohibited AI practices, (2) high risk, (3) limited risk and (4) minimal risk AI systems. Each level comes with its own set of requirements.

Cybersecurity Duties Applicable to the High-Risk AI Systems

The EU AI Act imposes explicit and stringent cybersecurity obligations on providers of high-risk AI systems — these are AI systems that present significant risks to health, safety, or fundamental rights in certain sectors or use cases (e.g., biometrics, critical infrastructure, education, employment, law enforcement and more). These obligations are designed to ensure that such systems are trustworthy, robust and resilient against both accidental failures and malicious attacks.

Key cybersecurity duties for high-risk AI systems include:

Security-by-Design and by Default

High-risk AI systems must be designed and developed to ensure a high level of cybersecurity, accuracy and robustness. This means the system must be resilient to errors, faults and inconsistencies, whether these arise internally or from the external environment.[145]

Protection Against AI-Specific Attacks

Systems must be safeguarded against exploitation by unauthorised third parties. The EU AI Act specifically highlights protection against:

- Data poisoning: manipulation of training data to corrupt the system's learning process.
- Model poisoning: tampering with pre-trained components used during training.
- Model evasion: altering input data to deceive the AI system into producing unintended outcomes.
- Other attacks: such as adversarial examples, confidentiality attacks and attempts to manipulate outputs or performance.[146]

145. Article 15(1) of the EU AI Act.
146. Art. 15(5); Recitals (76) — (77) of the EU AI Act.

Technical Resilience

Providers must implement proportionate technical and organisational measures, such as:

- technical redundancy (e.g., backup systems, fail-safe mechanisms).
- preventive and responsive measures to detect, respond to and control cyberattacks.[147]

Lifecycle Consistency

Cybersecurity must be maintained throughout the entire lifecycle of the AI system, not just at launch. Providers must maintain a *post-market monitoring plan* and *immediately* report "serious incidents" (e.g., security breaches causing serious damage to health, safety, fundamental rights or property) to market-surveillance authorities within 15 days.[148]

Cybersecurity Risk Assessment

Before placing a high-risk AI system on the market or putting it into service, providers must conduct a cybersecurity risk assessment. This assessment must:

- identify and evaluate cybersecurity threats;
- document measures taken to ensure resilience;
- be updated regularly to reflect evolving threats and system changes.[149]

Documentation and Record-Keeping

All cybersecurity measures, risk assessments and quality assurance processes must be documented and made available to competent authorities upon request. Technical files must describe cybersecurity architecture and controls; systems must enable automatic logging of events to facilitate incident investigation.[150]

Cybersecurity Duties Applicable to Other AI Systems

The EU AI Act does not impose explicit cybersecurity obligations on non-high-risk AI systems. However, providers of all AI systems are expected to consider cybersecurity as a best practice, especially if the system processes personal data, interacts with users, or influences physical/virtual environments. Providers should adopt a risk-based, security-by-design and security-by-default approach — integrating cybersecurity from the earliest design stages and ensuring default settings offer the highest level of protection. Compliance with other applicable legislation (e.g., GDPR, CRA, NIS2 Directive) remains essential for all AI systems.

147. Art. 15(4) of the EU AI Act.
148. Art. 73 of the EU AI Act.
149. Art. 43(1) — (4) of the EU AI Act.
150. Art. 18 of the EU AI Act.

What Regulatory Penalties Could Arise From a High-Risk System Breach?

Financial Penalties

Failure to meet the EU AI Act's cybersecurity obligations for high-risk systems can result in administrative fines of up to EUR15M or 3 percent of the total worldwide annual turnover (whichever is higher). If the breach involves practices explicitly prohibited by the EU AI Act (e.g., certain manipulative or discriminatory uses), fines can reach up to EUR35M or 7 percent of global turnover. Providing false or incomplete information to authorities can result in fines of up to EUR7.5M or 1 percent of global turnover. For small and medium-sized enterprises, the lower of the percentage or the fixed amount applies.[151]

The EU AI Act requires that high-risk AI systems processing personal data must comply with GDPR and other data protection laws. A breach may therefore trigger investigations and penalties under both regimes. Where the breach also entails loss of personal data, cumulative enforcement by the UODO under GDPR remains possible; Recital 12 EU AI Act clarifies that the Act is "without prejudice to Union data-protection law".

Thus, a single cyber-incident impacting a high-risk AI system could expose an entity to parallel fines: up to 3 percent for EU AI Act violations and up to 4 percent for GDPR violations, in addition to remedial orders such as withdrawal from the market or mandatory source-code audits.

Entities already subject to NIS2 or DORA must also consider the EU AI Act as an additional, not alternative, layer: an incident may therefore engage three concurrent reporting chains (CSIRT-KSC, KNF-DORA and AI Act) and expose the organisation to compound monetary and operational sanctions.

Other Consequences

Providers must immediately take corrective actions to bring the system into compliance, withdraw, disable, or recall the system if it is found non-compliant or presents a risk.

Serious incidents (including those resulting in death, serious damage to health, or serious breaches of fundamental rights) must be reported to market surveillance authorities.

Beyond regulatory fines, a security breach can erode trust, damage reputation and result in loss of business or market position.

151. Article 99 of the EU AI Act.

Ireland

The European Union's Artificial Intelligence Act (**AI Act**) entered into force on 1 August 2024, with phased legal applicability of its provisions thereafter. It aims to ensure that the development and deployment of AI in the EU is done responsibly. It introduces a uniform framework across all EU countries, using a risk-based approach to AI.

In terms of the applicable cybersecurity duties, the AI Act separates AI operators into several different categories, each with specific duties. The categories included are: 7.2.1 **Providers**: any person that develops an AI system, or general-purpose AI model with a view to placing it on the market in the EU or putting it into service within the EU under its own name or trademark, whether for payment or for free.

- **Deployers:** any person using an AI system under its authority except in the course of personal, non-professional activity.
- **Importers:** any person in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the EU.
- **Distributors:** any person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.

The Act establishes certain duties and obligations on each operator type, with the most onerous duties being imposed on providers. These provider obligations include obligations to establish a risk management system in respect of their AI system, to ensure their systems allow for automatic event logging and to ensure that high-risk AI systems have the appropriate level of accuracy, robustness and cybersecurity. If a cyber incident or breach of any AI system does occur, this may indicate that an AI system provider is not sufficiently fulfilling these obligations and may be at risk of penalties for such violations.

In contrast, a deployer has fewer obligations than a provider. A deployers main obligation is to take appropriate measures in using an AI system and to do so in conformity with the instructions provided on how to use the system. Additionally, deployers are obligated to use the instructions as part of their data protection impact assessment, which is a GDPR requirement for controllers to carry out an assessment of any impact the processing operations may have on their protection of personal data. Regarding any possible cyber breach or incident in an AI system, a deployer may be at lower risk of penalties for a breach if they are using the system appropriately and as instructed by the provider of the AI systems.

Both distributors and importers have more limited obligations under the AI Act. Their main obligations concern their risk assessments at both a pre-market and post-market stage and ensuring that if there are any sufficient reasons to believe that the AI system is not in conformity with the requirements of the Act, that they do not place it on the market, or if already on the market, that they remove it therefrom. If there is a cyber breach of the AI system, the importer or distributor may also be at lower risk any penalties under the AI Act unless they have reason to know of the breach and they then fail to take corrective action either by placing it on the market or by refusing to recall it therefrom.

For General-Purpose AI Models (**GPAI Models**), there are distinct obligations on providers which are separate to the obligations that apply to them for any AI systems they develop. Some of these obligations include a requirement to document technical information about their models and have a publicly available summary about the content used to train the model. For GPAI Models with systemic risk, which are models that have risks of potential large-scale harm, there are additional obligations on providers. These additional obligations include that providers must document and report any serious incidents, as well as ensure that the model has adequate cybersecurity protection. Any breach of a GPAI Model, particularly a GPAI Model with systemic risk, may be considered to be a violation of the obligations that are imposed on providers and the EU Commission may seek to impose fines or take other regulatory action against them.

Penalties

Under Article 99 of the AI Act, Member States are required to lay down the rules on penalties and other applicable enforcement measures. Article 99 sets out various administrative fines that can be applied to breaches of certain sections of the AI Act. While the maximum fine of EUR35M or 7 percent of total worldwide annual turnover may be imposed for prohibited AI practices, such as AI systems that use social scoring techniques, for breaches of the obligations imposed on the various categories of operators, Member States may impose lesser fines of up to EUR15M or 3 percent of worldwide annual turnover for the preceding financial year, whichever is higher.

Article 99 penalties only apply to infringements of operators' obligations in relation to AI systems and these penalties shall be administered by the Member States. For GPAI Models, it is the European Commission who may impose administrative fines on providers who they find either intentionally or negligently infringed on any relevant provisions of the Act, failed to comply with any measures requested under the Act, failed to comply with a request for a document or information, or failed to make available to the European Commission access to the GPAI Model. If found to have breached one of these conditions, the European Commission may impose a fine of up to EUR15M or a fine not exceeding 3 percent of their total worldwide annual turnover in the preceding financial year, whichever is higher.

Germany

What Cybersecurity Duties are There?

The AI Act (Regulation [EU] 2021/206) expressly addresses cybersecurity in Art. 15(1), (4) AI Act. Operators of high-risk AI systems shall design and provide technical solutions for cybersecurity.

The EU names five cybersecurity vulnerabilities specific to AI, which operators shall take into account:

- Attacks trying to manipulate the training data set (data poisoning).
- Attacks trying to manipulate pre-trained components used in training (model poisoning).
- Inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion).
- Confidentiality attacks.
- Model flaws.
- Operators must conduct their Conformity Assessment (Art. 43 AI Act, Recital 78) with regards to cybersecurity and include a detailed description of relevant measures in their technical documentation (Art. 11 AI Act) and include relevant information in their transparency instructions (Art. 13(3)(b)(ii) AI Act).
- The same obligations apply to GPAI operators (Art. 78 AI Act).

What Regulatory Penalties Could Arise From a High-Risk System Breach?

Non-compliance with the AI Act is subject to regulatory fines of up to EUR35M or up to 3 percent of global annual turnover, whichever is higher (Art. 99[4] AI Act).

If the security breach lead to the loss of personal data, the GDPR fines set out under Question 2 apply.

Spain

What Cybersecurity Duties are There?

The Regulation (EU) 2024/1689 (**EU AI Act**) entered into force on August 1, 2024, with staged application. Most obligations for high-risk AI systems phase in by August 2, 2026, or August 2, 2027, depending on whether the system is incorporated into regulated products. According to Article 15 of the EU AI Act, high-risk AI systems must be designed and developed to achieve an appropriate level of robustness, accuracy and cybersecurity for their intended purpose and to be resilient against attempts to manipulate the system or its data. Providers must conduct a risk assessment before placing the system on the market or putting it into service and document the results of such risk assessment, which shall include an identification of the potential risks posed by the AI system and the measures taken to prevent or mitigate those risks.

Additionally, providers shall implement risk management and data governance across the lifecycle, maintain up-to-date technical documentation and logs to demonstrate compliance and enable post-market monitoring, ensure transparency for deployers and effective human oversight and monitor performance after deployment with prompt reporting of serious incidents or malfunctions to market surveillance authorities. Deployers must oversee operation, ensure the suitability of input data, provide human oversight, inform affected workers and users and cooperate with regulators.

What Regulatory Penalties Could Arise From a High-Risk System Breach?

A security breach compromising the robustness or cybersecurity of a high-risk AI system can trigger enforcement under the AI Act, in parallel with GDPR and sectoral regimes. The AI Act sets significant fine tiers. Non-compliance with prohibitions is punishable by up to the higher of EUR35M or 7 percent of worldwide annual turnover. Non-compliance with provider, deployer, importer, distributor and notified body obligations, including robustness/cybersecurity, logging, oversight and incident reporting, is punishable by up to the higher of EUR15M or 3 percent. Providing incorrect, incomplete, or misleading information to authorities is punishable by up to the higher of EUR7.5M or 1 percent.

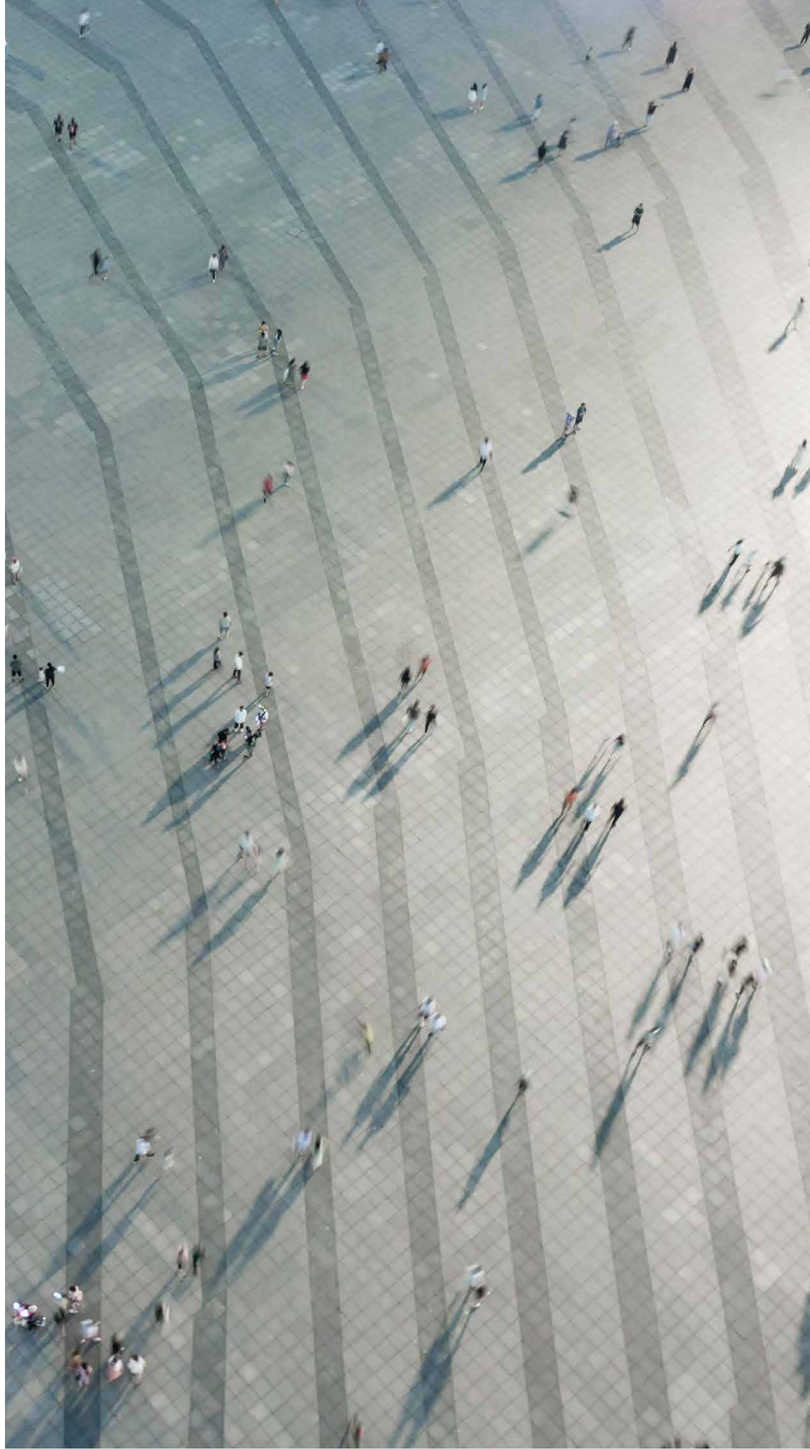
Small and medium-sized enterprises benefit from proportionate adjustments. National market-surveillance authorities enforce against operators; the EU AI Office oversees general-purpose model obligations. Where an AI-related security breach involves personal data, GDPR notification to the AEPD and, if required, data subjects applies in parallel, and a single incident can attract cumulative corrective orders and separate administrative fine frameworks under both instruments. Entities within scope of NIS2 face risk-management and incident-reporting duties and sanctions; financial entities face DORA oversight. The aggregate exposure becomes multi-regime and incident-response planning should anticipate cross-regulatory timelines and content requirements.

Netherlands

What Cybersecurity Duties are There?

The applicable cybersecurity duties under the EU AI Act are the following:

- **Art. 15: Accuracy, robustness and cybersecurity:** High-risk AI systems must be designed in such a way that they achieve an appropriate level of (amongst other things) cybersecurity.
- **Art. 55: Obligations of providers of general-purpose AI models with systemic risk:** Providers of general-purpose AI models with systemic risk have to ensure an adequate level of cybersecurity protection.



What Regulatory Penalties Could Arise From a High-Risk System Breach?

If providers of high-risk AI systems fail to comply with Art. 16 of the EU AI Act (which refers to Art. 15 of the EU AI Act), they may face fines up to EUR15M, or 3 percent of the worldwide annual turnover form the preceding financial year. This sanction regime will only apply, once the providers must comply with Art. 15 of the EU AI Act.[152]

If the providers of general-purpose AI models fail to comply with Art. 55 EU AI Act, they may face fines up to 3 percent of their total worldwide turnover from the preceding financial year or EUR15M, whichever is higher, where the European Commission an intentional or negligent infringement of Art. 33 EU AI Act. Article 33 EU AI Act already applies.

The EU AI Act does not affect the obligations of providers to comply with the GDPR.[153] The EU AI Act and the GDPR exist in parallel. This means that if the security breach impacting a high-risk AI system also constitutes a personal data breach within the meaning of the GDPR, the Dutch DPA may also impose an administrative fine. In the Netherlands, the supervisory authority enforcing the GDPR in the Netherlands is de Dutch DPA. The competent authority enforcing the EU AI Act has not yet been designated.

Finally, when deciding whether to impose an administrative fine and in what amount, authorities should take into account any administrative fines already imposed by other market competent authorities.[154]

France

What Cybersecurity Duties are There?

Article 15 requires high-risk AI to achieve appropriate accuracy, robustness and cybersecurity, including resilience to adversarial attacks (e.g., data poisoning/ model manipulation) and lifecycle wide consistency; technical/organisational measures and redundancy/ failsafe may be necessary.

Post market monitoring & serious incident reporting obligations (notably under Arts. 72–73) complement cybersecurity by ensuring continuous compliance after deployment.

These obligations coexist with GDPR/NIS2 where personal data or covered entities are involved.

What Regulatory Penalties Could Arise From a High-Risk System Breach?

Up to EUR15M or 3 percent for breaches of high-risk AI obligations (e.g., cybersecurity, documentation, post market monitoring).

If a security breach also involves personal data loss, parallel GDPR enforcement (CNIL) and remedial orders may apply in addition to AI Act sanctions.

152. Art. 99 EU AI Act.
153. Par. 40 EU AI Act.
154. Art. 99(7)(b) EU AI Act.

8 General Recommendations

Governance

Establish clear accountability for cyber risk management at board and senior management levels.

Compliance

Stay current with evolving regulatory frameworks in all jurisdictions where you operate.

Incident Response

Develop and test incident response plans, including breach notification and regulatory engagement.

Training

Regularly train staff on cybersecurity, data protection and regulatory requirements.

Insurance

Work with brokers and legal counsel to optimise cyber insurance coverage, focusing on insurable costs.

Vendor Management

Assess and monitor third-party risk, ensuring contracts address cyber incident responsibilities.

Documentation

Keep detailed records of compliance activities, risk assessments and incident responses.

Authors

EMEA	Pablo Constenla
Belgium	Thomas Declerck Peter Van Dyck Felix Declerck Françoise Billen
England & Wales	Charlie Weston-Simons Steven Hadwin
Finland	Eija Warma-Letinen Bertram Lahdenper
France	Laurie-Anne Ancenys Dalila Korchane Hippolyte Marquetty
Germany	Catharina Glugla David Schmid
Ireland	Sheena Doggett David Widger Nicholas Cole Chris Bollard Mary Sheehan Shauna Scannell
Italy	Piermaurizio Tafuni Francesca Corbinelli
Luxembourg	Catherine Di Lorenzo Barbara Azoulay Clara Boxus
Netherlands	Nicole Wolters Ruckert Marleen Huisman
Norway	Georg Abusdal Engebretsen Mathias Bjerkoy
Poland	Justyna Ostrowska
Portugal	Filipe Lowndes Marques Margardia Torres Gama
Saudi Arabia	Chadi Hourani Saeed Khunaizi
South Africa	Gerhard Rudolph Nikita Shaw Nicole Gilfelleon
Spain	Laur Badin Andrea Lisnier Alba Diaz
Sweden	Viveka Classon Nicklas Thorgerzon Josef Jatta Kölin Louise Brorsson Salmon Mikael Stahl
Turkey	Umut Gurgey Berkan Tomay Irmak Su Aydinli
UAE	Tom Butcher Tala Taifour

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram.
Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

aon.com