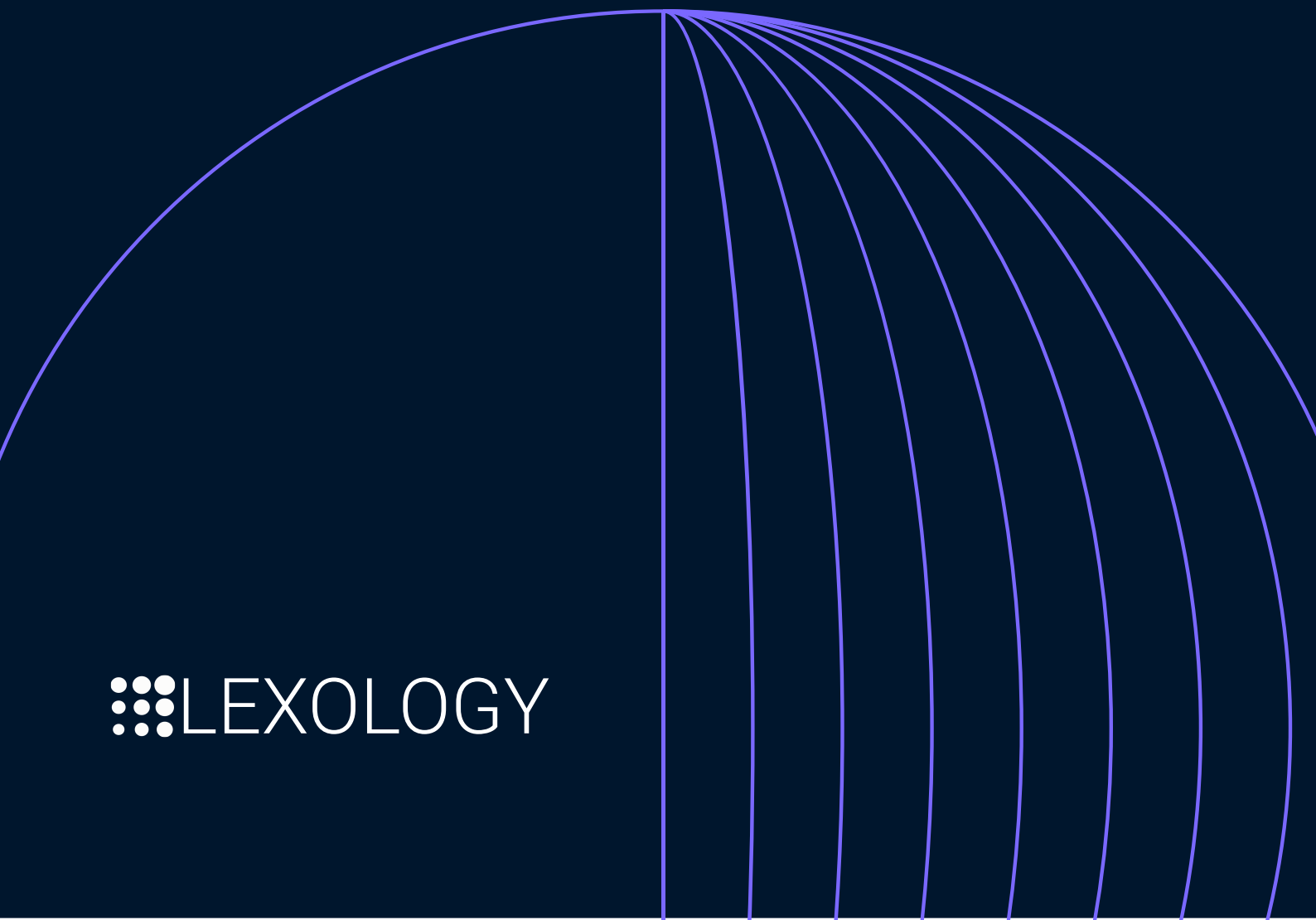
PANORAMIC

CYBERSECURITY 2025



LEXOLOGY

Cybersecurity 2025

Quick reference guide enabling side-by-side comparison of local insights, including into the applicable legal and regulatory framework; best practices, including information sharing and insurance; enforcement, including relevant regulatory authorities, notification obligations, penalties, and avenues of private redress; threat detection and reporting; and recent trends.

Generated on: May 14, 2025

Contents

China
Kate Yin, Jeffrey Ding, Patrick Guo, Gil Zhang
Fangda Partners

European Union
Kristina Schreiber, Dennis Pethke
Loschelder Rechtsanwälte

France
Claire Bernier
ADSTO

Germany
Kristina Schreiber, Dennis Pethke
Loschelder Rechtsanwälte

Greece
Dimitra Karampela
Karatzas & Partners Law Firm

India
Sumit Ghoshal, Aprajita Rana, Shagun Badhwar, Suyash Tiwari
AZB & Partners

Italy
Paolo Balboni, Luca Bolognini, Francesco Capparelli, Giulia Finocchiaro
ICT Legal Consulting

Japan
Yasushi Kudo, Tsubasa Watanabe, Hayato Maruta
Nagashima Ohno & Tsunematsu

Netherlands
Robbert Santifort, Ilham Ezzamouri
Eversheds Sutherland

Singapore

Lim Chong Kin, **Anastasia Su-Anne Chen**

Drew & Napier LLC

Switzerland

Markus Naef, **Oliver Scharp**, **Carol Tissot**, **Nadine Zollinger**

Eversheds Sutherland

United Kingdom

Lawrence Brown, **Robert Allen**

Simmons & Simmons

China

Kate Yin, **Jeffrey Ding**, **Patrick Guo**, **Gil Zhang**
Fangda Partners

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The general cybersecurity and data protection regime in China includes the Cybersecurity Law (CSL) and its implementation regulations and measures. Various sectoral regulators have also issued sector-specific rules to regulate cybersecurity and data protection issues.

The Civil Code, which came into force on 1 January 2021 and supersedes the General Principles of the Civil Law, provides for the right to personal data protection. Any organisations and individuals that collect and process personal data must ensure the security of the personal data. Unlawful collection, use, processing or transfer of personal data is prohibited.

Article 253 of the Criminal Law and the Interpretation of the Supreme People's Court and the Supreme People's Procu
ratorate on Several Issues regarding Legal Application in Criminal Cases In
fringing upon the Personal Data of Citizens specify certain activities that may constitute the crime of infringing the right to personal data protection. There are also other provisions in the Criminal Law that criminalise the intrusion of information systems and other cybercrimes.

The Decision on Strengthening the Protection of Online Information (Decision) was adopted by the Standing Committee of the National People's Congress of China (NPC) in 2012 and provides certain general principles on the protection of citizens' online information. Any network service providers and other entities that collect and process citizens' online information must comply with the rules provided in the Decision.

The Provisions on the Protection of Personal Data of Telecommunication and Inte
rnet Users, published in 2013, provide relevant rules on the protection of users' personal data. These measures apply to telecommunications service operators and internet information service providers in terms of their collection and processing of users' personal data.

The Administrative Measures for the Multi-level Protection of Information Security (MLPS Measures), published in 2007, provide relevant rules for the Multi-level Protection Scheme (MLPS). These measures are generally referred to as MLPS 1.0. On 27 June 2018, the Ministry of Public Security released for public consultation the new Draft Regulations on Multi-level Protection System for Cybersecurity, which aimed to repeal and replace the existing MLPS Measures. MLPS 2.0 (which comprises various national standards that have been revamped) was released in June 2019.

The Data Security Law (DSL), which was promulgated by the NPC on 10 June 2021 and came into force on 1 September 2021, provides that any individuals or organisations that engage in data activities in China may be subject to the DSL. Data activities include data collection, retention, processing, use, provision, trade, public disclosure, etc, regardless of whether they are conducted through a network or not.

The Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation) (Data Security Measures), which took effect on 1 January 2023, classify data into 'core', 'important' and 'ordinary' categories and require companies to take different degrees of protection measures when collecting, processing, transferring and disposing of data. The Data Security Measures apply to all kinds of enterprises in the industrial, telecoms and radio communications fields, especially software and information technology (IT) service providers and telecoms business licence holders, and set out detailed requirements regarding data lifecycle protection.

The Personal Information Protection Law (PIPL), which was passed by the NPC on 20 August 2021 and came into force on 1 November 2021, covers various areas of personal data protection. For example, the PIPL specifically provides various data protection principles, including transparency, fairness, purpose limitation, data minimisation, limited retention, data accuracy and accountability. Many provisions of the PIPL seem to be inspired by the EU General Data Protection Regulation (GDPR). These include hefty fines of up to 5 per cent of the revenue of the preceding year of a company or individual that processes personal data for a serious breach of the PIPL. There are, however, key differences, notably that the PIPL has a strong focus on consent by individuals on how their personal data is processed. The concept of 'legitimate interest' for processing personal data, which is widely used in the European Union, is not recognised in the PIPL.

The Regulations on Network Data Security Management (Network Data Regulations), which was released on 30 September 2024 and came into force on 1 January 2025, set out specific protection requirements and obligations on network data handlers on the basis of the PIPL, CSL and DSL, and fine-tune mechanisms for the management of important data. In addition, the Network Data Regulations also stipulate the obligations for internet platform service providers, specifying data protection requirements for entities such as third-party service and product providers.

In addition to the above-mentioned laws and regulations, there are also various national standards on cybersecurity and data protection. For example, the Information Security Technology – Personal Data Security Specification (GB/T 35273-2020) provides various recommended rules on personal data protection, the Draft of Information Security Technology – Security Requirements for Processing of Important Data outline the various security requirements that information systems and platforms processing important data should comply with throughout the entire data processing lifecycle, the Information Security Technology – Implementation Guidelines for Notices and Consent in Personal Information Processing (GB/T 42574-2023) specify the methods and steps for notifying data subjects about personal information processing rules and obtaining their consent, and the Practice Guide for Cybersecurity Standards – Guidelines for Identifying Sensitive Personal Information further clarify the rules for identifying sensitive personal information, as well as its categories and examples, serving as a significant reference for enterprises.

Law stated - 14 March 2025

Most affected economic sectors

2

Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The CSL applies to the construction, operation, maintenance and use of networks in China. Any organisation or individual that uses a network will be a network operator regardless of the sector. More stringent requirements apply to critical information infrastructure (CII), in particular data localisation requirements. CII operators also fall within the scope of network operators.

Article 31 of the CSL defines 'CII' as information infrastructure in public communication and information services, energy, public transportation, water conservancy, the financial industry, public services, government information systems and other information infrastructure that may materially affect the national interest, public interest or society as a whole if it is compromised, damaged, disrupted or impacted upon by a data breach or otherwise. Though the CSL does not provide the specific scope of CII nor the approach to identify CII, network operators in these critical industries or sectors may be more likely to be designated as CII operators.

On 17 August 2021, the long-awaited Regulations on Critical Information Infrastructure Security Protection (CII Regulations) were released and took effect on 1 September 2021. The definition of 'CII' under the CII Regulations is essentially the same as that under the CSL. For important industries and sectors, the relevant regulators, termed 'Protection Departments', will be charged with the responsibilities of protecting CIIs in their relevant industries and sectors. Once a Protection Department has identified the CII, it must notify the operators and the Ministry of Public Security.

There are also various sectoral rules regarding cybersecurity and data protection that apply to network operators in certain industries, such as fintech, financial services, pharmaceutical and medical services, land surveying and autonomous driving.

Law stated - 14 March 2025

International standards

3 Has your jurisdiction adopted any international standards related to cybersecurity?

China actively participates in the making of international standards and will recognise certain international standards by transposing relevant rules into the national standards according to the Standardisation Law. Article 8 of the Standardisation Law provides that the Chinese government will actively facilitate the interoperability of international standards in China. The standards in China (including national, sectoral or provincial standards or standards applicable to certain associations) may adopt some of the terminology of the international standards to ensure correlation between them and China's national standards, and may also adopt the same rules in the international standard with or without modification when transposing them as national standards. For example, the Information Technology – Security Techniques – Information Security Management Systems – Requirements (GB/T 22080-2016) were made by the National Cybersecurity Standardisation Technical Committee (formerly named the National Information Security

Standardisation Technical Committee, also known as TC260) with reference to ISO 27001:2013, developed by the International Organization for Standardization.

Law stated - 14 March 2025

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The CSL requires network operators to designate a specific person to be responsible for its cybersecurity and data protection issues (the cybersecurity responsible person). Failure to do so would render the network operator subject to the administrative penalty imposed by the relevant supervisory authorities according to article 59 of the CSL, including a rectification order, warning or administrative fine in the case of a failure to rectify the non-compliance or in the case of a significant impact on cybersecurity as a result of the violation of the law. The cybersecurity responsible person is responsible for assisting the network operator in complying with the CSL and safeguarding data and cybersecurity.

The CSL imposes liability on the 'directly responsible person' or the 'other responsible person' of the network operator for its violation of the CSL in certain circumstances. For example, article 64 of the CSL provides that the directly responsible person or the other responsible person of the network operator may be subject to a fine ranging from 10,000 yuan (approximately US$1,400) to 100,000 yuan (approximately US$14,000) for the network operator's infringement of an individual's right to personal data protection. However, the CSL is silent on what constitutes the 'directly responsible person' or the 'other responsible person', which may be determined by prosecutors and courts on a case-by-case basis.

On 14 September 2022, the Cyberspace Administration of China issued the Draft Decision on Amending the CSL (Draft Revised CSL) for soliciting public comments, which proposes a maximum fine of 1 million yuan (approximately US$140,000) for violations of the law by the 'directly responsible person' or the 'other responsible person'. So far, the Draft Revised CSL has not been adopted by the NPC Standing Committee, and hence is not in force for now.

The 'directly responsible person' or the 'other responsible person' may also be penalised under the DSL, which provides that if an organisation carrying out data processing activities fails to perform the data security protection obligations stipulated in the DSL, it may be fined up to 200,000 yuan (approximately US$28,000).

The CSL and DSL are both silent on the obligations of directors to remain informed about the adequacy of the company's protection of networks and data. However, according to the Company Law, directors have fiduciary duties towards the company, and it is not yet clear whether a company's violation of the CSL will be interpreted as a director's breach of fiduciary duties to direct the company to comply with laws and regulations.

Law stated - 14 March 2025

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Cybersecurity

The CSL defines 'cybersecurity' as meaning 'to maintain the stable and reliable operation of network and to safeguard the integrity, confidentiality and usability of network data, by taking necessary measures to prevent the network from attack, intrusion, interference, damage, unauthorised use and accidents'. Although the CSL does not define data privacy, the relevant articles of the CSL provide that data privacy refers to the protection of the confidentiality, integrity and availability of personal data.

Given that cybersecurity and data privacy intertwine as data is stored on an information system that relies on IT infrastructure and requires protection, the rules on cybersecurity would also apply in the context of data protection. A cybersecurity incident may not always lead to a data breach, such as in the event of a cybersecurity incident that gives rise to the outage of the network or information system, but the data is encrypted to prevent a data breach.

Cybercrime

The Criminal Law criminalises certain offences related to computers and computer networks that are commonly regarded as cybercrimes. Criminal activities include but are not limited to:

- illegally intruding into a computer system;
- illegally accessing or controlling data stored on a computer system;
- providing computer programs or tools to intrude into or illegally control a computer system;
- damaging a computer system;
- failing to fulfil the security management obligations for an information network; and
- illegally using an information network.

The Opinions on Several Issues Concerning the Application of Criminal Procedure in Information Cybercrime Cases issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on 30 August 2022 clarified the scope of cybercrimes as:

- activities that endanger the security of computer information systems;
- the refusal to fulfil the obligations of managing the security of information networks, illegal use of information networks and assistance in criminal activities involving information networks; and
- other criminal cases involving fraud, gambling and infringement of personal information of citizens etc, in which the main activities are conducted through an information network.

Law stated - 14 March 2025

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The CSL requires network operators to adopt security measures (ie, technical and organisational measures) for cybersecurity and data protection, such as:

- formulating internal security management systems and operation instructions concerning cybersecurity and data protection, and specifying the responsibilities of each relevant department;
- designating a cybersecurity responsible person;
- adopting technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitoring and recording network operation and cybersecurity events and maintaining the cyber-related logs for no less than six months;
- adopting the rules of data classification and taking appropriate measures according to the data categories; and
- backing up and encrypting important data.

In the event that there is dissemination of prohibited content online, a massive data breach, loss of evidence for criminal investigation or other serious consequences as a result of a network operator's refusal to take appropriate technical and other necessary measures to protect information security as required by laws and regulations, and to rectify the situation as required by the relevant regulators, the failure may constitute the crime of 'refusal to perform security management obligations for the information network' under article 286 of the Criminal Law.

The MLPS Measures require that the information system operator or user shall take certain prescriptive measures to ensure the security of the information system according to the grade of information system. The Information Security Technology – Baseline for Classified Protection of Cybersecurity was implemented on 1 December 2019 to provide further clarity in conjunction with implementing the new Draft MLPS 2.0 Regulations. It provides the following security measures:

- apply access control to the information systems;
- take measures to protect the physical safety of information systems, such as anti-theft, fireproof and anti-invasion measures;
- ensure the security of telecommunications;
- determine the safety parameters and take relevant protection measures accordingly;
- conduct identity authentication for the access of information systems;

- perform data backups;
- set up internal company policies on security management and determine the responsible person or department;
- provide training to employees on cybersecurity and data protection;
- grade the information systems and file the grade of the information system with the local police if graded as Level II or above;
- design a security plan for the information systems;
- ensure the security of the products and services purchased for the information systems; and
- prepare a security incident response plan and protocol.

Sectoral rules may provide more requirements on the protective measures for cybersecurity and data protection that apply to the network operators in certain sectors, such as banking and financial services.

Lastly, the Cyberspace Administration of China issued the Administrative Measures for Compliance Audits of Personal Information Protection (Compliance Audits Measures) on 12 February 2025, which will take effect on 1 May 2025. The Compliance Audits Measures were promulgated to echo the compliance audit requirements under articles 54 and 64 of the PIPL, and article 27 of the Network Data Regulations, including periodic audits initiated by data handlers themselves and dedicated audits launched by authorities if they find that there is a relatively high risk in personal data processing activities or that a personal data security incident has occurred. Although the Compliance Audits Measures mainly focus on the compliance requirements of processing and protecting personal data, they also provide some requirements on organisations' cybersecurity capacity and technical measures, such as:

- adopting specific management or security technology measures to categorise personal data;
- adopting security measures to guarantee the confidentiality, integrity and availability of personal data with reference to relevant national standards or technical requirements; and
- eliminating or reducing the identifiability of personal data, etc.

Law stated - 14 March 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The laws and regulations on the promotion of cybersecurity apply to the protection of networks, which applies to any theft of intellectual property if it is stored on an information system or a network, such as the crimes of illegally obtaining data from information systems

(article 285 of the Criminal Law) and damaging an information system (article 286 of the Criminal Law).

Law stated - 14 March 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The CSL provides stricter requirements for the protection of CII.

Article 31 of the CSL defines 'CII' as information infrastructure in public communication and information services, energy, public transportation, water conservancy, the financial industry, public services, government information systems and other information infrastructure that may materially affect the national interest, public interest or society as a whole if it is compromised, damaged, disrupted or impacted upon by a data breach or otherwise. However, the CSL does not provide the specific scope of CII nor the approach to identify CII.

The CII Regulations provide further rules in this regard. Under the CII Regulations, the relevant regulators (termed the 'Protection Departments') will be charged with the responsibilities of protecting CIIs in their relevant industries and sectors. In particular, Protection Departments have the power to make rules for identifying CII and to identify the CII according to such rules. In determining the rules, the Protection Departments will take the following factors, among others, into consideration:

- the importance of the network infrastructure and information systems to the key or core operation of the relevant industry or sector;
- the level of harm on the network infrastructure and information systems in the event of destruction, loss of function or data leakage; and
- any consequential impact on other industries or sectors.

Once the Protection Department identifies the CII, it must notify the operators and the Ministry of Public Security.

The Cyberspace Administration of China released the revised Measures on Cybersecurity Review to implement article 35 of the CSL, which require that any purchase of network products and services by the CII operators that affects or may affect state security is subject to relevant cybersecurity assessment.

The Cyberspace Administration released the Draft Measures for the Administration of Publishing Cyberthreat Information (Draft Measures) on 20 November 2019. These measures provide stricter requirements on the publication of the regional comprehensive analysis report on cybersecurity attacks, incidents, risks and vulnerabilities that relate to important sectors, such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defence, science and technology. In addition to the prior report to the Cyberspace

Administration, reporting to the relevant sectoral regulator would also be required if the Draft Measures are brought into force.

Law stated - 14 March 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

According to article 29 of the CSL, China supports cooperation between network operators in the collection, analysis and reporting of cybersecurity information and the emergency response for the purpose of improving network operators' capabilities for cybersecurity protection. However, as stipulated in article 26 of the CSL, carrying out activities such as cybersecurity certification, testing and risk assessment and releasing cybersecurity information, such as system bugs, computer viruses, network attacks and intrusions, are subject to relevant rules.

The Draft Measures for the Administration of Publishing Cyberthreat Information provide relevant rules, including:

- the published cyberthreat information must not contain seven types of content, including the source code and production methods of computer viruses, Trojan horses, ransomware and other malware;
- the publication of information relating to a cybersecurity incident, such as an attack, damage or illegal access to a network or information system, is subject to prior reporting to the public security organ above the prefecture level of the place where the incident occurred; and
- without the approval or authorisation of a government agency, enterprises, social organisations and individuals must not add the phrase 'early warning' to the title of the published cyberthreat information.

The Administrative Provisions on Security Vulnerabilities of Cyber Products issued on 12 July 2021 require that the release of security vulnerabilities information about cyberproducts to the public through cyber platforms, media, conferences, contests or otherwise, by any organisation or individual that discovers or collects security vulnerabilities of cyber products shall follow the principles of necessity, authenticity, objectivity and being conducive to preventing cybersecurity risks, and comply with the following provisions:

- it is not allowed to release vulnerability information before the cyber product provider provides remedial measures for security vulnerabilities of cyber products; the organisation or individual shall conduct joint assessment and consultation with the relevant cyber product provider if it or he or she deems it necessary to release such information in advance, and shall report the same to the Ministry of Industry and Information Technology and the Ministry of Public Security, which will release such information after organising assessment;
- it is not allowed to release the details of security vulnerabilities in the cyber information system and equipment used by network operators;

- it is not allowed to deliberately exaggerate the hazards and risks of security vulnerabilities of cyber products, or to carry out malicious speculation, fraud, extortion and other illegal or criminal activities by making use of information of security vulnerabilities of cyber products;
- it is not allowed to release or provide programs or tools specifically used for activities that endanger cybersecurity by taking advantage of security vulnerabilities of cyber products;
- it is required to release repair or preventive measures at the same time as releasing security vulnerabilities of cyber products;
- it is not allowed to release information of security vulnerabilities of cyber products without the approval of the Ministry of Public Security during major events held by the state;
- it is not allowed to provide undisclosed security vulnerabilities of cyber products to any overseas organisation or individual other than cyber product providers; and
- other relevant provisions of laws and regulations (not specified).

The right to freedom and confidentiality of private communications is a constitutional right. Article 40 of the Constitutional Law provides that no organisation or individual may, on any ground, infringe the right to freedom and privacy of citizens' private correspondences. The only limitation to this right is that the police or procurators may search and access private correspondence in accordance with the applicable rules for protecting state security or investigating criminal offences.

The law does not provide specific rules on the collection and processing of metadata. However, if metadata forms part of state secrets, important data or personal data, the collection and processing of it will be subject to the relevant rules applicable to the category of the data.

Law stated - 14 March 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The Criminal Law criminalises certain offences related to computers and computer networks that are commonly regarded as cybercrimes. Criminal activities include but are not limited to:

- illegally intruding into a computer system;
- illegally accessing or controlling data stored on a computer system;
- providing computer programs or tools to intrude into or illegally control a computer system;
- damaging a computer system;
- failing to fulfil the security management obligations for an information network; and

- illegally using an information network.

The Opinions on Several Issues Concerning the Application of Criminal Procedure in Information Cybercrime Cases issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on 30 August 2022 clarified the scope of cybercrimes as:

- endangering the security of computer information systems;
- refusal to fulfil the obligations of managing the security of information networks, illegal use of information networks and assistance in criminal activities involving information networks; and
- other criminal cases involving fraud, gambling and infringement of personal information of citizens etc, in which the main activities are conducted through information network.

Law stated - 14 March 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The providers of cloud computing services in China must comply with the laws and regulations on cybersecurity and data protection. There are various regulations, measures and national standards that are made specifically for cloud computing, which cover aspects ranging from the procurement of the cloud services, security and management measures for cloud services providers. For example, the Cyberspace Administration released the Opinion on Strengthening the Administration of the Cybersecurity of the Cloud Computing Services Used by Departments of the Party and Government on 30 December 2014 and jointly released the Measures for the Security Assessment of Cloud Computing Service on 2 July 2019 together with the National Development and Reform Commission, the Ministry of Industry and Information Technology and the Ministry of Finance. Government agencies and the CII operators must first assess the risks and assess the providers before using any cloud computing services that have passed the security assessment by the Cyberspace Administration. Use of public cloud computing services is prohibited if the network operator's information system stores any state secrets.

Where a network operator uses cloud computing services to store data, the network operator must also ensure that its cloud services providers comply with the technical and management measures under the MLPS regime so that the network operator can pass the annual testing of MLPS.

Law stated - 14 March 2025

Foreign organisations

12

> How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The CSL applies to network operators regardless of whether the companies are domestic companies or foreign-invested companies.

The CSL is silent on extra-territorial application and has no provision similar to article 3(2) of the GDPR. However, the view of the Cyberspace Administration seems to be that the CSL would have extra-territorial application.

Article 2 of the DSL provides for extra-territorial application of the DSL in certain circumstances; that is, if overseas organisations or individuals engage in the data processing activities that damage national security, the public interests of China or the legitimate interests of the citizens or organisations of China, such overseas organisations or individuals (or both) may be subject to the DSL.

The PIPL applies to the processing of individuals' personal data that takes place in China regardless of the nationality of such individuals. Unlike the CSL, which provides limited extra-territorial application, the PIPL proposes clear and specific extra-territorial application to overseas entities and individuals that process the personal data of data subjects in China for the purpose of provision of products or services (or both) to data subjects in China; for analysing or assessing the behaviour of data subjects in China; or in other circumstances as provided by China's laws and regulations.

According to article 2 of the newly released Network Data Regulations, any network data processing activities, as well as the security supervision and administration, conducted in China are subject to these regulations. With regard to the extraterritorial application, the provisions in Network Data Regulations are consistent with those in the PIPL, and further emphasise that any overseas network data processing activities that damage the national security, public interest, or the lawful rights and interests of citizens and organisations of China shall be held legally liable in accordance with the Network Data Regulations.

For foreign organisations doing business in China, one significant regulatory challenge that requires special attention is cross-border data transfers as these data transfers from Chinese subsidiaries to headquarters are generally inevitable for multinational companies. Since 2022, the Cyberspace Administration has made significant progress in formulating various rules on regulating cross-border data transfers, in particular the following:

- the Cyberspace Administration released the Measures on the Security Assessment of Cross-Border Data Transfer (Security Assessment Measures) on 7 July 2022, which came into force on 1 September 2022. The Security Assessment Measures are intended to implement the rules of security assessment for cross-border data transfers under the CSL, DSL and PIPL.
- the Cyberspace Administration, together with the State Administration for Market Regulation, released the Rules for Implementation of Personal Information Protection Certification (Certification Rules) on 4 November 2022, which provide implementation rules for cross-border transfer of personal data based on certification by a licensed agency (protection certification) as a legal mechanism recognised by the PIPL. The Certification Rules provide the relevant information on the certification model, the implementation process, the standards on certificates

and marks, etc, and also require that the licensed agencies can only provide a certification service after being approved. China Cybersecurity Review, Certification and Market Regulation Big Data Center (formerly named China Cybersecurity Review Technology and Certification Center, also known as CCRC), as officially licensed agency, has already issued China's first certificate of personal information protection in December 2023;

- the Cyberspace Administration released the Measures for the Standard Contract for Cross-border Transfer of Personal In formation (Standard Contract Measures), as well as the template of the Standard Contract for Cross-border Transfer of Personal Information(Standard Contract) on 22 February 2023. The Standard Contract Measures are intended to implement the rules of standard contract for cross-border transfers of personal data under the PIPL; and
- the concluded Standard Contract should be filed at the local Cyberspace Administration at provincial level within 10 working days of the effective date of the Standard Contract, together with a data protection impact assessment report in the context of cross-border transfer of personal data.

With regard to the regulations on cross-border data transfers, special attention should be paid to the Provisions on Promoting and Standardising Cross-Border Data Flows (Data Transfer Provisions) issued by the Cyberspace Administration on 22 March 2024. The Data Transfer Provisions aim to facilitate the free cross-border transfer of data and change the threshold stipulated by the Security Assessment Measures and the Standard Contract Measures released by the Cyberspace Administration previously.

Specifically, the Data Transfer Provisions have introduced relaxation and exemptions to the mechanisms for cross-border data transfer (ie, security assessment for cross-border data transfer ('security assessment'), filing of standard contract for cross-border transfer of personal information ('SCC filing') and personal information protection certification ('certification'), collectively referred to as 'cross-border data transfer mechanisms'):

- Company-wide exemption/de minimis exemption: if data handlers other than the CII operators have collectively shared less than 100,000 individuals' personal data (excluding sensitive personal data) outside of China since 1 January of that year, they are not obligated to follow the cross-border data transfer mechanisms.
- Scenario-based exemptions:
    - Exemption for cross-border nature business scenario: exemption for cross-border nature business scenarios includes situations where individuals need to provide personal information outside of China in order to enter into and fulfil a contract they are a party of. This includes activities such as cross-border shopping, mailing, fund transfers, payments, account opening, air ticket and hotel bookings, visa applications and taking exams.
    - Exemption for HR management necessity on employees' data: in cases where it is required to disclose employees' personal information outside of China for the purpose of managing cross-border human resources in compliance with labour laws and regulations, as well as collective contracts established by law.

- Exemption for protection of vital interest: in situations of emergency, where it is imperative to disclose personal information outside of China to safeguard the life, health and property of individuals.
- The Data Transfer Provisions have also made changes to the numerical threshold used to determine the applicable cross-border data transfer mechanism (see below). Additionally, the calculation period has been modified to start from 1 January of the current year.

Subject type	Number of cumulative data transferred overseas since 1 January of the current year	Applicable cross - border data transfer mechanism
CII operators	1 individual's personal information	Security assessment
Data handlers that are not CII operators	> 1 million individuals' personal information (excluding sensitive personal information)	Security assessment
> 10,000 individuals' sensitive personal information	Security assessment	
100,000—1 million individuals' personal information (excluding sensitive personal information)	Either SCC filing or certification	
1—10,000 individuals' sensitive personal information	Either SCC filing or certification	
<100,000 individuals' personal information without any sensitive personal information	Exempted from applying for any cross - border data transfer mechanism	

Law stated - 14 March 2025

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes, China has published various national standards and technical guidelines on cybersecurity and data protection, which mainly include GB standards (mandatory national standards that are compulsory for companies to adopt), GB/T standards (recommended national standards that are not compulsory for companies to adopt) and technical guidelines. These national standards and technical guidelines cover various issues related

to cybersecurity and data protection. For example, the Information Security Technology – Personal Data Security Specification (GB/T 35273-2020) provides various recommended rules on the protection of cybersecurity and personal data. Another example is that the Draft of Information Security Technology – Security Requirements for Processing of Important Data released on 25 August 2023 outline the various security requirements that information systems and platforms processing important data should comply with throughout the entire data processing lifecycle. The newly issued Information Security Technology – Implementation Guidelines for Notices and Consent in Personal Information Processing (GB/T 42574-2023) specify the methods and steps for notifying data subjects about personal information processing rules and obtaining their consent, and the Practice Guide for Cybersecurity Standards – Guidelines for Identifying Sensitive Personal Information further clarify the rules for identifying sensitive personal information, as well as its categories and examples, serving as a significant reference for enterprises.

Law stated - 26 December 2024

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

There is currently no specific monetary reward from the government to incentivise organisations to improve their cybersecurity. Protecting cybersecurity and data is an obligation for each network operator.

Law stated - 26 December 2024

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

China has published various national standards and technical guidelines on cybersecurity and data protection, which mainly include GB standards (mandatory national standards that are compulsory for companies to adopt), GB/T standards (recommended national standards that are not compulsory for companies to adopt) and technical guidelines. These national standards and technical guidelines cover various issues related to cybersecurity and data protection. For example, the Information Security Technology – Personal Data Security Specification (GB/T 35273-2020) provides various recommended rules on the protection of cybersecurity and personal data. In general, the national standards and technical guidelines are made by the National Cybersecurity Standardisation Technical Committee and are often published jointly by the State Administration for Market Regulation and the State Standardisation Administration. Various national standards can be found at www.tc260.org.cn. However,

these national standards are published in Chinese and there is no official translation for them.

Law stated - 26 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

China has released various rules on responding to data breaches and security incidents. In addition to relevant laws and regulations (eg, the Cybersecurity Law the National Emergency Response Plan for Cybersecurity Incidents and the Regulations on Network Data Security Management), there are also recommended rules for responding to data breaches and security incidents. For example, the Information Security Technology – Personal Data Security Specification (GB/T 35273-2020) provides relevant recommended rules on responding to and managing personal data breaches, in particular on notifying competent supervisory authorities and the affected data subjects.

The Cyberspace Administration of China released the Draft Administrative Measures for Cybersecurity Incident Reporting on 8 December 2023 together with the Guidelines on Grading of Cybersecurity Incidents (Guidelines) and the Reporting Form of Cybersecurity Incident Information (Reporting Form). According to the Guidelines, cybersecurity incidents are classified into 'extremely severe', 'severe', 'relatively severe' and 'general' categories by the impact degree of national security, social order, economic construction and public interest. Incidents classified as relatively severe, severe or extremely severe should be reported within one hour using the Reporting Form, which shall cover the company's basic information, a description of the affected information system, the incident background and preliminary investigation findings, as well as the contingency measures already adopted together with the next step plans.

Law stated - 26 December 2024

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

China supports cooperation between network operators in the collection, analysis and reporting of cybersecurity information and the response to emergencies for the purpose of improving their capabilities for cybersecurity protection. If the Draft Measures for the Administration of Publishing Cyberthreat Information are brought into force in their current form, the publication of cyberthreat information would be subject to prior reporting to relevant regulators, and the publication of cyberthreat information must not contain certain prohibited contents. The National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT), established in 2001, is a national cybersecurity emergency response agency established under the Cyberspace

Administration. The CNCERT initiated the establishment of the National Vulnerability Database, with information provided by various telecoms operators, cybersecurity companies and internet services providers. The database aims to proactively monitor cyberthreats and incidents, and provide information for network operators to take preventive measures against cybersecurity incidents.

Law stated - 26 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Other than the private sector giving comments on draft measures that are released for public consultation, the most common avenue of cooperation between government and the private sector is during the drafting of national standards on cybersecurity and data protection. Several members of the National Standardisation Committee (eg, TC260) will select a national standard and join a working group to initiate research and the drafting of the national standard. As a member of TC260, our experience has been that the private sector's comments and opinions are very much welcome and accepted, and the process of making various national standards is generally very collaborative.

Law stated - 26 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Insurance for cybersecurity breaches in China is available, and it is common practice for companies in China to have it.

Law stated - 26 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Various regulatory authorities enforce cybersecurity rules in China, in particular the primary regulators: the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security. Other sectoral regulators can also make rules to regulate data protection and cybersecurity issues in their respective

sectors, such as the People's Bank of China, the China Securities Regulatory Commission, the National Financial Regulatory Administration and the National Health Commission.

It is worth noting that according to Plan for Institutional Reform of the Party and State, the National Data Bureau (NDB), administered by the National Development and Reform Commission, was inaugurated on 25 October 2023 . The NDB is responsible for advancing the development of data-related fundamental institutions, coordinating the integration, sharing, development and application of data resources, and pushing forward the planning and building of a Digital China, the digital economy and a digital society.

Law stated - 26 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Chinese authorities in general have broad powers to monitor compliance, conduct government investigations, request cooperation and information, and impose penalties for violating laws according to various administrative laws, such as the Administrative Penalty Law.

For example, according to the Measures for Internet Security Supervision and Inspection issued by the Ministry of Public Security under the authorisation of the Cybersecurity Law (CSL), the Ministry may conduct on-site inspection and remote testing against certain types of network operators. During the on-site inspection, the Ministry may take certain measures to investigate cybersecurity incidents, such as entering the premises to inspect computer rooms and the workplace; interviewing the cybersecurity responsible person of the network operator; consulting and copying information required for the investigation; and checking the operation of technical measures for network and information security protection.

When the Ministry conducts remote testing to determine whether certain system vulnerabilities may exist on the network operator's network, prior notice will be given to the network operator concerned that will include the time of remote testing and the scope of testing. The Ministry generally should not interfere with the normal operation of the network of the network operator.

Law stated - 26 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The provisions under the Criminal Law against the infringement of the right to personal data protection and against cybercrimes have been actively enforced in China. There have been many cases where organisations and individuals that unlawfully collected and processed personal data have been investigated, prosecuted and convicted.

Aside from the active criminal law enforcement, there have been law enforcement actions against the violation of the CSL, such as failure to monitor and record network operation and cybersecurity incidents and maintain the network logs for no less than six months; take technical measures to prevent computer viruses, network attacks and network intrusion; and adopt online content moderation measures against the prohibited information released by app or website users. The unlawful use of virtual private networks has also been the subject of law enforcement in China.

As a coordinated law enforcement effort, the Cyberspace Administration, the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation (collectively, the Four Ministries) released a joint announcement of their law enforcement agenda on 25 January 2019, which aimed to curb certain privacy practices throughout 2019 and promote a certification scheme for personal data protection. The Four Ministries highlighted in this announcement that app operators must display a privacy notice for the collection and use of personal data in an easy-to-understand, clear and concise manner, and allow data subjects to give consent freely instead of coercing consent by way of pre-ticked consent boxes or bundled consent. Many app operators have been inspected and required by the Four Ministries to rectify non-compliance. The Four Ministries have repeatedly published a list of names of app operators that have not yet complied with the CSL and have even ordered certain apps to be suspended or temporarily removed from app stores.

App-related issues remain an enforcement focus for the authorities, with enforcement actions against illegal collection and use of user personal data becoming commonplace. Serious circumstances may also trigger the authorities' in-depth review of both cybersecurity and data protection status. On 6 September 2023, the Cyberspace Administration issued an announcement stating that based on the conclusions of the cybersecurity review against China National Knowledge Infrastructure (CNKI) and the relevant issues identified in this process, CNKI was ordered to cease its illegal processing of personal data and fined 50 million yuan (approximately US$7.1 million), which is the maximum amount of fixed fine under the Personal Information Protection Law. Previous to the penalty decision, the Cyberspace Administration had initiated an investigation into CNKI and found that 14 apps operated by CNKI were involved in illegal data processing activities such as collecting personal data without consent, failing to disclose or clarify collection and use rules, not providing account cancellation options, and not promptly deleting user personal data after account cancellation.

Law stated - 26 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

The law requires notification of security incidents to the relevant regulators as well as to the affected data subjects, for example:

- article 1038 of the Civil Code requires the handler of personal data to report a data breach to the affected natural persons and the competent supervisory authorities;

- articles 25 and 42 of the CSL require network operators to report security incidents to the competent supervisory authorities as well as to the affected data subjects whose personal data has been breached;
- article 29 of the Data Security Law requires companies that process data to report security incidents to the competent supervisory authorities as well as to the affected data subjects whose personal data has been breached;
- article 57 of the Personal Information Protection Law (PIPL) requires companies to immediately take remedial measures and notify the authorities and the data subjects concerned where personal data has been or may be divulged, tampered with or lost;
- article 14 of the Provisions on the Protection of Personal Data of Telecommunication and Internet Users provides that telecommunications business operators and internet information service providers must report security incidents that will or may have severe consequences to the competent telecommunications administration authorities;
- the National Emergency Response Plan for Cybersecurity Incidents defines and categorises cybersecurity incidents and provides the threshold for reporting to the regulatory authorities as well as the relevant procedural requirements;
- article 4 of the Draft Administrative Measures for Cybersecurity Incident Reporting requires the network operators to promptly initiate the emergency response plan for disposal when an incident occurs. For incidents classified as relatively severe, severe or extremely severe, the operators shall report to the local Cyberspace Administration within one hour; and
- the Regulations on Network Data Security Management again stress the obligations of network data handlers, including establishing and improving emergency response plans for network data security incidents, promptly initiating the plan when an incident is detected, and reporting the incident to relevant regulator in a timely manner.

Law stated - 26 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

To prevent cybersecurity breaches, network operators are required to adopt the necessary technical and management measures to safeguard data and for cybersecurity.

Failure to take technical and other measures to ensure cybersecurity and protect the personal data collected, which can lead to a cybersecurity breach, would render the network operator concerned subject to the administrative penalty imposed by the relevant regulators according to the CSL, including a rectification order, a warning, confiscation of illegal gains, a fine, suspension of business or operation of apps or websites, or revocation of the permit or business licence if it is a serious violation. The Cyberspace Administration

issued the Draft Decision on Amending the CSL (Draft Revised CSL) for soliciting public comments on 14 September 2022. The significant revisions mainly concern Chapter VI, Legal Liability of the current CSL, which provides a maximum fine of 1 million yuan (approximately US$140,000) for violations of the law. The Draft Revised CSL, however, increases the maximum fine to '5 per cent of the revenue of the preceding year' of a company to be consistent with the penalty under the PIPL. So far, the Draft Revised CSL has not been adopted by the Standing Committee of the National People's Congress of China, and hence is not in force for now.

In the event that the cybersecurity breach and serious consequences occur as a result of the network operator's refusal to adopt appropriate technical and other necessary measures to protect personal data as required by the relevant regulators in a rectification order, the refusal may further constitute the crime of 'refusal to perform security management obligations for the information network', as provided in article 286 of the Criminal Law.

Law stated - 26 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

There are legal ramifications for network operators that fail to report cybersecurity breaches to the relevant regulators and the data subjects whose personal data has been breached. Legal ramifications include rectification orders, warnings, fines, confiscation of illegal gains, suspension of business or operation of apps or websites, and revocation of the permit or business licence if it is a serious violation. These administrative penalties are imposed by the relevant supervisory authorities according to article 64 of the CSL.

Law stated - 26 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Data subjects may bring claims against organisations and individuals that unlawfully collect or process their personal data on the grounds of either tort or breach of contract (ie, a user agreement). A tort claim is more common as the data subjects can choose either the Civil Code or the Law on the Protection of Rights and Interests of Consumers as the legal basis to bring a claim. There is a provision in the latter that provides private redress for consumers similar to article 111 of the Civil Code.

Law stated - 26 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Cybersecurity Law (CSL) requires network operators to adopt security measures (ie, technical and organisational measures) for cybersecurity and data protection, such as:

- formulating internal security management systems and operation instructions concerning cybersecurity and data protection, and specifying the responsibilities of each relevant department;
- designating a cybersecurity responsible person;
- adopting technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitoring and recording network operation and cybersecurity events, and maintaining the cyber-related logs for no less than six months;
- adopting the rules of data classification and taking appropriate measures according to the data categories; and
- backing up and encrypting important data.

In the event that there is dissemination of prohibited content online, a massive data breach, loss of evidence for criminal investigation or other serious consequences as a result of a network operator's refusal to take appropriate technical and other necessary measures to protect information security as required by laws and regulations, and to rectify the situation as required by the relevant regulators, the failure may constitute the crime of 'refusal to perform security management obligations for the information network' according to article 286 of the Criminal Law.

The Administrative Measures for the Multi-level Protection of Information Security require that the information system operator or user shall take certain prescriptive measures to ensure the security of the information system according to the grade of information system. The Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019) has been implemented since 1 December 2019 to provide further clarity in conjunction with implementing the new Draft Regulations on Multi-level Protection System for Cybersecurity. It provides the following security measures:

- applying access control to the information systems;
- taking measures to protect the physical safety of information systems, such as anti-theft, fireproof and anti-invasion measures;
- ensuring the security of telecommunications;
- determining the safety parameters and taking appropriate protection measures accordingly;
- conducting identity authentication for the access of information systems;
- performing data backups;

- setting up internal company policies on security management and determining the responsible person or department;
- providing training to the employees on cybersecurity and data protection;
- grading the information systems and filing the grade of the information system with the local police if graded as Level II or above;
- designing a security plan for the information systems;
- ensuring the security of the products and services purchased for the information systems; and
- preparing a security incident response plan and protocol.

Chapter VI of the Data Security Law (DSL) stipulates various data protection obligations regarding data processing, as well as the principles of social morality and ethics applicable to data processing activity and the development of new technologies. The DSL also reiterates the importance of network protection, implementing the multi-level protection system, training and other technical measures (eg, risk monitoring and contingency measures) and other necessary measures.

The Administrative Provisions on Security Vulnerabilities of Cyber Products issued on 12 July 2021 requires that network product providers shall perform a series of network product security vulnerability management obligations to ensure that their product security vulnerabilities are timely patched and reasonably released, and guide and support product users to take preventive measures. Network operators are also required to take measures immediately after discovering or learning about network security vulnerabilities, and to verify security vulnerabilities and complete repairs in a timely manner.

Sectoral rules may provide more requirements on the protective measures for cybersecurity and data protection that apply to the network operators in certain sectors, such as banking and financial services.

Law stated - 26 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The CSL requires network operators to adopt technical measures to monitor and record network operation status, cybersecurity threat information and security incidents and to keep relevant logs for at least six months. There are other sectoral rules and circulars that require certain network operators in certain sectors to keep the logs for a minimum of one year.

The Information Security Technology – Personal Data Security Specification (GB/T 35273-2020) provides that records of data breach incidents must contain, at a minimum, who discovered the incident as well as when and where the incident was discovered, the categories of personal data affected, the number of affected data subjects, the names of the information systems involved and whether notification was made to the relevant regulators. The Specification is silent on the retention period of the records of data breach incidents.

Law stated - 26 December 2024

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There are various laws and measures that require network operators affected by cybersecurity incidents to report the incidents to the relevant regulators, such as the CSL-Law, the Civil Code, the E-commerce Law, the Provisions on the Protection of Personal Data of Telecommunication and Internet Users, the National Emergency Response Plan for Cybersecurity Incidents, the Draft Administrative Measures for Cybersecurity Incident Reporting, and the Regulations on Network Data Security Management, as well as relevant sectoral rules. The thresholds for reporting to different regulators are not the same; however, the reporting obligation under different rules is generally triggered by the occurrence or potential occurrence of a cybersecurity incident. The report must be in Chinese, and it must contain at least the following information: the time of occurrence of the incident; the scope of the impact and damage; remedial measures that have been taken; the details of the personal data and data subjects involved in the breach; and the contact details of the relevant responsible department or person of the network operator.

Law stated - 26 December 2024

Time frames

30 | What is the timeline for reporting to the authorities?

Upon the discovery of a cybersecurity incident, the network operator must immediately report the incident to the relevant regulators. Article 20 of the new Draft Regulations on Multi-level Protection System for Cybersecurity provides that a report of any online incidents must be made to the local public security organ within 24 hours. Article 4 of the Draft Administrative Measures for Cybersecurity Incident Reporting stipulates that the network operator shall report the cybersecurity incident within one hour when it reaches the level of relatively severe, severe or extremely severe. There are also sectoral rules that provide specific timelines for reporting the data breach to the authorities; for example, the new version of the Implementation Measures for the Protection of Rights and Interests of Financial Consumers, which was released by the People's Bank of China (PBOC) on 15 September 2020 and came into force on 1 November 2020, requires banking financial institutions and non-banking payment institutions to report a data breach that may damage financial consumers' life or property immediately to the local branch of the PBOC, and to report a data breach that may cause other negative influence on financial consumers within 72 hours to the local branch of the PBOC.

While there is no specific obligation to continue reporting after the initial report to the relevant regulators, in practice, once the regulators step in to investigate the incident, they will request cooperation and information from time to time until the closure of the investigation.

Law stated - 26 December 2024

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Network operators have specific obligations to notify the data subjects whose personal data has been breached. There is no specific data breach reporting obligation on a network operator to notify others in the same industry or sector as the reporting obligation is limited to the relevant Chinese authorities, should the cybersecurity incident meet the reporting threshold, and to the affected data subjects. The network operator can communicate with the affected data subjects using any of the following means: email, letter, telephone, in-app push notification and other proper means or announcement on the company website (if it is impractical to notify each of the affected data subjects).

Law stated - 26 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Although the Cybersecurity Law (CSL) is the primary law that provides rules on cybersecurity and data protection, its provisions are mostly high-level principles, and it is still very much dependent on implementation measures and regulations for consistent law enforcement. As the CSL authorises several ministries (as opposed to one specific ministry) to issue rules under the CSL and enforce them, the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security have been actively creating ministry-level measures since the passage of the CSL.

The Data Security Law (DSL) and the Personal Information Protection Law (PIPL), effective since 2021, together with the CSL, form the legal framework for cybersecurity in China. To supplement the CSL, the DSL introduced various new principles and rules regarding data processing and data protection. For example, the DSL stipulates various requirements for the processing of important data, including that important data processors must designate a specific individual or department in charge of data security and periodically file with the relevant authorities a risk assessment report regarding the processing of important data. The DSL also provides that data related to restricted items that are subject to export control

restrictions under Chinese law is also subject to export control, and without pre-approval by supervisory authorities of the Chinese government no organisation or individual in China may provide data stored on the territory of China to foreign authorities or judicial bodies. The DSL lays a good foundation for many rules to come. To strengthen the protection of personal data, the PIPL requires personal data handlers to take a series of protection measures that also touch on cybersecurity topics such as data encryption and categorisation.

The principal challenges to compliance with cybersecurity laws in China in 2024 are that companies have to meet various regulators' expectations and must dynamically adjust their compliance measures in response to rapid changes in regulatory requirements. Not only do the regulations and measures promulgated by different regulators require careful reconciliation by companies, but companies also need to consider certain recommended national standards that provide guidance. Companies may start taking a holistic and dynamic approach to harmonise these rules and build a comprehensive data protection programme to ensure continuous compliance with the CSL and implementation regulations and measures. Based on many law enforcement actions, it is easier to convince regulators that a company has taken sufficient measures for cybersecurity and data protection if they are shown evidence of compliance and a comprehensive data protection programme.

Take important data as an example: enterprises should pay particular attention to issues related to important data, as processing such data is subject to additional compliance requirements under applicable data protection laws. According to article 62 of the Regulations on Network Data Security Management (Network Data Regulations), 'important data' is defined as data in a specific field, a specific group, a specific region, or of a certain precision and scale, which, once tampered with, damaged, leaked or illegally obtained or illegally used, may directly endanger national security, economic operation, social stability, public health and safety. To identify important data, relevant Chinese regulators may either make the catalogue of important data to release or issue a circular or notice to notify specific companies and sectors. So far, Chinese regulators have already publicly released the catalogues of important data or the standards on the identification of important data of the automobile sector, the industry and information technology sector, the natural resources sector, as well as in certain free trade zones. Notably, the Network Data Regulations require data handlers who process personal information of 10 million or more individuals to fulfil additional responsibilities specific to important data handlers. Therefore, companies processing data in China should closely monitor updates to important data regulations and regularly assess their risk exposure to ensure the compliant business operations.

The year 2024 was a productive year for cybersecurity and data security with important regulations being finalised, such as the Provisions on Promoting and Standardising Cross-Border Data Flows and the Network Data Regulations (the latter coming into force on 1 January 2025).There is no doubt that active law enforcement agencies will follow the new regulations. At the beginning of 2025, after almost two years of public consultation, the Cyberspace Administration of China finally published the Compliance Audits Measures on 12 February 2025, which will come into force on 1 May 2025. According to the Compliance Audits Measures, an organisation that processes more than one million individuals' personal information should appoint a DPO and charge this DPO with audit responsibilities. Furthermore, if the organisation processes more than 10 million individuals' personal information, it must conduct a biennial audit, while there is no mandatory frequency for those who do not meet this threshold. Besides, in certain circumstances, such as a data

breach, the authorities may mandate an organisation to appoint an external auditor to conduct an audit.

In 2025 and the forthcoming years, it is expected that more important cybersecurity laws, amendments and regulations will be introduced as both the Legislative Plan of the Standing Committee of the Fourteenth National People's Congress and 2024 Annual Legislative Work Plan issued by the Standing Committee of the National People's Congress of China (NPC) highlighted the revision of the CSL. It was proposed that the Draft Decision on Amending the CSL be reviewed and passed during the office term of the current NPC (ie, 2023 to 2028). In addition, the Draft Administrative Measures for Cybersecurity Incident Reporting, which provide more specific requirements on organisations' cybersecurity obligations, may be finalised in 2025. As cybersecurity laws and policies continue to be developed and updated, law enforcement will also continue to be strong and active, and there may be more coordinated efforts in addressing cybersecurity and data protection practices in 2025.

Law stated - 14 March 2025

FANGDA PARTNERS
方達律師事務所

Kate Yin kate.yin@fangdalaw.com
Jeffrey Ding jding@fangdalaw.com
Patrick Guo patrick.guo@fangdalaw.com
Gil Zhang gil.zhang@fangdalaw.com

Fangda Partners

European Union

Kristina Schreiber, **Dennis Pethke**
Loschelder Rechtsanwälte

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The European Union developed several statutes and regulations over recent years to govern and promote cybersecurity. First came Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), which was repealed on 18 October 2024 Directive (EU) 2022/2555 (NIS2 Directive) took effect, even though several member states still had not implemented the NIS Directive into national law. The NIS2 Directive will also not apply in the member states until national law transposing the Directive enters into force. The NIS2 Directive expands the scope of the NIS Directive to include many more companies, and contains new obligations concerning the prevention and notification of cybersecurity incidents. Implementation has been delayed in 23 member states – namely, Austria, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Latvia, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden; the Commission opened infringement procedures against them on 28 November 2024 (-https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive).

Additionally, the Critical Entities Resilience Directive (EU) 2022/2557(CER Directive) obliges member states to ensure the provision of essential services through specific measures and critical entities to enhance their resilience.

Regulation (EU) 2019/881 Cyber Security Act) regulates the European Union Agency for Cybersecurity (ENISA) and the cybersecurity certification procedure for information and communications technology. In April 2023, the Commission proposed a targeted amendment for this Regulation on which the European Parliament has not yet decided.

For financial companies, Regulation (EU) 2022/2554 (also known as the Digital Operational Resilience Act or DORA) brings specific cybersecurity obligations directly in all EU member states from 17 January 2025.

The Cyber Resilience Act was published as Regulation (EU) 2024/2847 in the Official Journal of the European Union on 20 November 2024. The Regulation sets out the rules for more secure hardware and software products (eg, enforcing security updates for digital products). It entered into force on 10 December 2024 and will be is applicable as of 11 December 2027 (with some rules applicable from June and September 2026). The Commission proposed this Cyber Resilience Act (COM(2022) 454 final) in September 2022 to regulate horizontal cybersecurity requirements for products with digital elements as one core element of their EU-Cyberstrategy.

Regarding products and especially software, the renewal of the Directive on liability for defective products is relevant: Directive (EU) 2024/2853, based on the Commission proposal of September 2022 (COM(2022) 495 final). The updated directive also affects digital products such as software that may cause damage to a consumer. The directive

must be transposed to national law by 9 December 2026. The EU Commission is no longer pursuing the AI Liability Directive, which has also been discussed in the meantime.

The Cyber Solidarity Act was published as Regulation (EU) 2025/38 in the Official Journal of the European Union on 19 December 2024, based on the Commission Proposal (COM(2023) 209 final) from April 2023. This Act aims to improve the response to cyberthreats across the European Union. A European Cybersecurity Alert System shall be implemented, as well as a Cyber Emergency and a Cybersecurity Incident Review Mechanism.

Law stated - 1 April 2025

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The most affected economic sectors by cybersecurity laws and regulations in the European Union are the sectors with critical infrastructures. The NIS2 Directive defines these sectors as energy, transport, banking, financial market infrastructures, health, drinking and waste water, digital infrastructure, information and communication technology service management, public administration and space.

Other critical sectors are postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing (eg, of medical devices, computer products or transport equipment), digital providers and research (Annex II).

Specifically regulated are critical infrastructures, financial undertakings, telecommunications and energy undertakings.

Law stated - 1 April 2025

International standards

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The technical regulations, in particular DIN ISO 27001, have not been incorporated into the law, but are a central benchmark for interpreting and concertising the legal requirements.

Law stated - 1 April 2025

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Article 20 of the NIS2 Directive on essential and important entities and article 5 of DORA on the financing and banking sector set out clear and strict obligations of the management to ensure an appropriate level of cybersecurity within the company. The management itself has to approve the cybersecurity risk management measures taken by those entities, has to oversee its implementation and can be held liable for infringements. Training for the management to enable them to fulfil this task is obligatory under EU law. This is part of the governance obligations established by these EU Acts.

Law stated - 1 April 2025

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

'Cybersecurity' is defined in the Cyber Security Act (Regulation (EU) 2019/881) as ‘activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyberthreats (article 2(1)). Other EU Acts refer to this definition.

There is no explicit definition of 'cybercrime' in EU statutes.

Data privacy must be separated from this. Data privacy is regulated by the General Data Protection Regulation (EU) 2016/679 (GDPR) and includes the requirements for the processing of personal data. According to articles 25 and 32 of the GDPR, this also includes data security, which overlaps with cybersecurity.

Law stated - 1 April 2025

Mandatory minimum protective measures

6 | What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The GDPR sets out rules for data protection applying to all EU member states. The controller and the processor are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures could be the pseudonymisation and encryption of data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, or to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. The regulation also mentions a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32 of the GDPR).

In general, for critical sectors, important and essential entities, the NIS2-Directive sets out security requirements for network and information systems. Essential and important entities have to take appropriate and proportionate technical, operational and

organisational measures to manage risks posed to the security of the entities' network and information systems. The Directive defines the minimum requirements for these measures (eg, policies on risk analysis, incident handling, business continuity and supply chain security (article 21)). However, it does not specify any concrete measures, but requires risk-appropriate measures.

Law stated - 1 April 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure requires an adequate security of trade secrets. This covers protection against cyberattacks as well, but there are no specific obligations of cybersecurity in this regard.

Law stated - 1 April 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

There are regulations addressing specifically critical infrastructures. The NIS2 Directive in particular focuses on critical infrastructures. To protect critical infrastructure from cyberthreats, it sets out requirements for appropriate risk management and governance obligations. In addition, the CER Directive obliges operators of critical infrastructures to take measures to minimise the risk of failure of these facilities. Both directives need to be implemented into national law by the member states. The transposition period ended on 17 October 2024, but several member states have not yet completed transposition.

Law stated - 1 April 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Cyberthreat information can be very sensitive. If information about cyberthreats is personal, the protection framework of the GDPR applies. Disclosure (ie, processing) of personal data is permitted only on the basis of an authorisation – for example, to fulfil a legal obligation or due to predominant interests worthy of protection. However, there are no general bans on this.

Law stated - 1 April 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

In the European Union, ransomware attacks, distributed denial-of-service threats and malware are the most common types of cyberattacks. Criminal offences are prosecuted by the national authorities. Essential here is Directive 2013/40/EU on attacks against information systems.

Law stated - 1 April 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The obligations of the NIS 2 Directive also apply to cloud computing services belonging to the digital infrastructure sector with high criticality (Annex I).

ENISA is also in the process of developing a voluntary certification scheme for cloud services. This is based on the Cyber Security Act and aims to increase trust and protection for consumers and businesses across the European Union.

The Data Act (EU) 2023/2854 sets out, among other things, interoperability requirements for data processing services. A data processing service can also be a cloud computing service, which means that the provisions of article 35 of the Data Act can also be applicable in the context of cloud computing. The Data Act first requires that data processing services are interoperable (ie, that users can easily switch between different services of the same type and exchange data). The security and integrity of data processing services and data must not be compromised in the process.

With the Cyber Resilience Act (EU) 2024/2847 and the amendment of the Product Liability Directive (EU) 2024/2853, special obligations for security updates will become applicable in EU law for software and digital products, including the cloud. Application of those Legal Acts start in December 2026 (Product Liability Directive/December 2027 (CRA).

Law stated - 1 April 2025

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The impact of cybersecurity laws on foreign organisations depends on the territorial scope of the regulations and directives. The NIS2 Directive (applies to companies that provide their services in the European Union or carry out their activities in the Union, regardless of where they are based. Companies from third countries are also generally bound by the requirements. So there are no differences here. The only decisive factor is where the business activity takes place.

The territorial scope of application of the GDPR depends on the location of the controller or processor or the targets of processing. From either perspective there must be a direct link to the European Union. If this is the case, the GDPR is applicable also if the actual processing of personal data takes place outside the Union or the entity is located outside the Union (article 3 of the GDPR). If the establishment is located outside the European Union, the GDPR may still apply if the data processing is related to offering goods or services to data subjects in the European Union or their behaviour is to be monitored in the European Union.

Law stated - 1 April 2025

BEST PRACTICE

Recommended additional protections

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As the responsible authority for information technology security, the European Union Agency for Cybersecurity (ENISA) publishes various guidelines and recommendations about cybersecurity in companies in general or specialised on SMEs or certain topics. There are basic recommendations on how to implement cybersecurity in a company or technical guidelines describing special aspects of cybersecurity measures. These recommendations do not necessarily go beyond what is legally required. It is also often said that the legal obligations are thereby concertised. However, there are ENISA Cybersecurity Advices going into the details as password settings, authentication and so on.

Law stated - 1 April 2025

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

There are calls, information events and the like, but there is no specific monetary benefit.

Law stated - 1 April 2025

Industry standards and codes of practice

15 |

Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

Regulation (EU) 2019/881 (Cyber Security Act) brings significant certification opportunities for companies. ENISA furthermore publishes recommendations on a regular basis on its website.

Law stated - 1 April 2025

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

There are Guidelines on Personal data breach notifications under the General Data Protection Regulation (EU) 2016/679 (GDPR), published by the European Data Protection Board. ENISA publishes various details on incident reporting, but more in an analytic way than as recommendations on how to handle such a situation.

Law stated - 1 April 2025

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) obliges member states to create opportunities for the voluntary exchange of cybersecurity information. This includes various types of information on cyberthreats and their prevention. The exchange of information should aim to prevent or deal with cyber attacks or increase the overall level of cybersecurity (article 29). In addition, member states must set up a voluntary reporting mechanism for security incidents, cyberthreats and near-miss incidents (article 30). The directive was to be transposed into national law by 17 October 2024, but more than 20 member states have not done so on time. The Commission has already initiated various infringement proceedings in this regard.

Law stated - 1 April 2025

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Government cooperates within the European Governmental CERTs Group and ENISA.

Law stated - 1 April 2025

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Yes, there are insurances at national level from different providers. The conditions vary. We can see that the requirements have been increasing for some time. Insurance is only available on commercially reasonable terms if sufficient cybersecurity is guaranteed in the company.

Law stated - 1 April 2025

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and the Critical Entities Resilience Directive (EU) 2022/2557 (CER Directive) assign the task of enforcing cybersecurity requirements to the relevant national authorities (articles 32 and 33 of the NIS2 Directive and 21 of the CER Directive). There is no general EU authority. The requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR) are also enforced by the national supervisory authorities (article 57 of the GDPR).

Although ENISA is the EU agency for cybersecurity, it has only supporting and advisory functions to establish a high common level of cybersecurity in the Union (article 3 of the Cyber Security Act (EU) 2019/881). It is not responsible for enforcing security requirements or prosecuting cybercrime.

Law stated - 1 April 2025

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

According to the NIS2 Directive, the competent authorities monitor the application of the Directive at national level (article 8(2)). The various supervisory measures the authorities can take to fulfil this task include onsite inspections, safety audits, requests for information on risk management measures or other necessary data, documents or evidence (articles 32 and 33).

The data protection supervisory authorities may request the controller to provide relevant information, carry out data protection checks or request access to data in order to monitor the GDPR obligations (article 58 of the GDPR).

Law stated - 1 April 2025

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The EU requirements are enforced by the relevant national authorities. In cross-border cases regarding data protection, the data protection supervisory authorities will apply their national procedural rules. However, the differences in these rules hinder smooth and effective cooperation between the authorities. To counteract this problem, the Commission has proposed a new law with specific procedural rules for cross-border cases (COM (2023) 348). This is still being finalised; last discussions within the Council took place on 29 October 2024.

Law stated - 1 April 2025

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

According to the NIS2 Directive member states have to ensure that essential and important entities are obliged to report significant security incidents to the national competent authority (article 23). If necessary, they also inform the recipients of their services. A tiered reporting system applies: an early warning must be issued immediately, but at the latest after 24 hours. A security incident must be reported immediately and no later than 72 hours after becoming aware of it. A final report must be submitted no later than one month after the incident. The Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 specifies when a significant security incident has occurred.

In the case of data breaches, the controller must report these to the competent national supervisory authority immediately or within 72 hours (article 33 of the GDPR). This does not apply if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The data subject must be notified under the conditions of article 34 of the GDPR.

Law stated - 1 April 2025

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

According to article 36 of the NIS2 Directive, the member states are responsible for laying down rules on penalties applicable to infringements of the provisions adopted pursuant to the Directive. The penalties must be effective, proportionate and dissuasive. Regarding fines, the Directive regulates the general conditions that the member states have to follow. For example, any particularly important organisation that fails to take (appropriate) risk management measures is liable to a fine of up to €10 million or 2 per cent of its global annual turnover (article 34(4) of the NIS2 Directive).

The GDPR also leaves the regulation of sanctions for infringements to the member states. These sanctions must be effective, proportionate and dissuasive (article 84). However, the general conditions for the imposition of fines are governed by the GDPR. If, for example, the security requirements of article 32 of the GDPR are disregarded, a fine of up to €10 million or (as a company) up to 2 per cent of the annual turnover achieved worldwide must be paid.

Law stated - 1 April 2025

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

The NIS2 Directive contains more extensive provisions on fines than the previous directive. If an essential entity breaches its obligation to report a significant security incident (article 23 of the NIS2 Directive), it must expect a fine of at least €10 million or 2 per cent of its global annual turnover (article 34(4)). The amounts are lower for important organisations.

The general conditions for the imposition of fines are regulated by the GDPR. If, for example, the controller fails to report a personal data breach to the supervisory authority (article 33 of the GDPR), it has to pay a fine of up to €10 million or (as a company) up to 2 per cent of the annual turnover achieved worldwide (article 83(4)).

Law stated - 1 April 2025

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Affected persons can sue for damages or injunctive relief under national law. Collective actions are authorised for individual cases, in particular for injunctions, but not for individual claims for damages. The requirements for a claim for damages following a hacking attack were recently specified at EU level by the European Court of Justice in Case C-340/21, where it was stated in the case of a claim for damages under article 82 of the GDPR that fault is presumed and the controller can only exculpate itself if it demonstrates that it has taken all necessary measures to ensure adequate security.

Law stated - 1 April 2025

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

An appropriate risk management system must be in place, including an emergency plan. Article 30 of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) explicitly provides for this for important and essential entities.

Law stated - 1 April 2025

Record-keeping requirements

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

EU law does not provide any specific requirements in this regard. The General Data Protection Regulation (EU) 2016/679 (GDPR) recognises the general accountability obligation in article 5(2).

Law stated - 1 April 2025

Regulatory reporting requirements

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

According to the NIS2 Directive, member states should oblige essential and important organisations to report significant security incidents (article 23(1)). This includes security incidents that may cause serious disruption to services, financial loss to the organisation or significant harm to others. The organisations must first issue an early warning in which the suspicion of an unlawful or malicious act or cross-border effects is stated, if applicable. This is followed by a report on the incident with an initial assessment of its severity and impact. Lastly, a final report must be submitted describing the security incident in detail (article 23(4)).

With regard to cyberthreats, the member states are free to regulate a reporting obligation (article 23). However, member states must ensure that essential and important entities can also voluntarily report security incidents, cyberthreats and near-miss incidents (article 30).

The GDPR applies to security incidents that result in a personal data breach. According to article 33 of the GDPR, personal data breaches must be reported to the supervisory authority. This obligation does not apply if the data breach is not likely to result in a risk to the rights and freedoms of natural persons. The type of breach, contact details of the data

protection officer, a description of the likely consequences of the breach and the measures that have to be taken must be reported.

Law stated - 1 April 2025

Time frames

30 | What is the timeline for reporting to the authorities?

According to the NIS2 Directive, member states have to ensure that essential and important organisations are obliged to report significant security incidents to the national competent authority (article 23(4)). If necessary, these organisations should also inform the recipients of their services. A tiered reporting system applies: an early warning must be issued immediately, but at the latest after 24 hours; a security incident must be reported immediately and no later than 72 hours after becoming aware of it; and final report must be submitted no later than one month after the incident.

In the event of a personal data breach, the notification to the supervisory authority must be made without undue delay and, where feasible, within 72 hours of the controller becoming aware of the breach (article 33(1) of the GDPR). Any delay must be justified.

Law stated - 1 April 2025

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Under certain circumstances, customers (article 23(1) of the NIS2 Directive) or the public (article 23(7)) must also be informed. Where appropriate, the competent authority shall also notify other member states concerned and the European Union Agency for Cybersecurity of a significant security incident affecting two or more member states (article 23(6) of the NIS2 Directive).

In the event of a personal data breach, the data subject must be informed if there is likely to be a high risk to the personal rights and freedoms of natural persons. This does not apply if the controller has taken sufficient security measures or has ensured that the risk to the rights and freedoms of the data subject no longer exists. Notification is also not required if it involves a disproportionate effort (article 34 of the GDPR).

Law stated - 1 April 2025

UPDATE AND TRENDS

Recent developments and future changes

32 |

> What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

A number of new legal provisions that are intended to strengthen cybersecurity in the Union as a whole have been enacted in the European Union or are in the process of being politically agreed. At the centre is the EU Cybersecurity Strategy. Beneath this Strategy, numerous legal acts are pending, in particular the Digital Operational Resilience Act (Regulation (EU) 2022/2054, known as DORA), Directive (EU) 2022/20555 on measures for a high common level of cybersecurity across the Union (known as the NIS2 Directive), the Critical Entities Resilience Directive (EU) 2022/2557, the Cyber Security Act (EU) 2019/881, the Cyber Resilience Act (EU) 2024/2847 and the renewed Directive on liability for defective products (EU) 2024/2853, as well as the Cyber Solidarity Act Regulation (EU) 2025/38.

The goal is clear and convincing: better cybersecurity is needed. The challenge is to enact and implement the new legal legal framework in a coherent manner and thus enable companies to fulfil the requirements. Another important challenge is to also keep an eye on and strengthen the security of the administration.

Law stated - 1 April 2025

LOSCHELDER

Kristina Schreiber kristina.schreiber@loschelder.de
Dennis Pethke dennis.pethke@loschelder.de

Loschelder Rechtsanwälte

France

Claire Bernier
ADSTO

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Article L111-1 of the Code of Homeland Security provides that the state shall maintain security, which extends to cyberspace. It is in this regard that France has enacted not one specific law, but several acts and regulations promoting cybersecurity (some of the provisions of these acts and regulations have been integrated in the French Defence Code). They are as follows:

- The Military Programming Act No. 2013-1168 of 18 December 2013 for 2014 to 2019. Pursuant to this Act, the state has a duty and responsibility to take appropriate measures to protect essential sectors that are deemed 'of utmost importance for state survival', such as banks, hospitals and nuclear power plants.
- Decrees No. 2015-350 and 2015-351 of 27 March 2015, which enact the Military Programming Act of 2013. These decrees state that essential sectors deemed 'of utmost importance for state survival' are bound to:
    - adopt detection tools in their networks and IT infrastructures so as to prevent any cyberattack;
    - notify immediately any cybersecurity breach to the relevant authorities;
    - regularly audit their IT infrastructures; and
    - adopt specific measures requested by relevant authorities.
    - The law further provides that non-compliance may lead to a fine of up to €150,000.
- The Military Programming Act No. 2018-607 of 13 July 2018 for 2019 to 2024. The purpose of this act is to reinforce the national security level. A whole chapter is dedicated to cyber defence.
- Decree No. 2018-1136 of 13 December 2018, which enacts the Military Programming Act of 2018. This decree reinforces the collaboration between the authorities, electronic communications operators and web hosts to prevent any threat to the security of information systems. The decree provides measures regarding the implementation of detection tools in networks and IT infrastructures.
- Decree No. 2018-137 of 26 February 2018, regarding the hosting of personal health data. This decree establishes mandatory certification for health data hosting providers. Together with the Ministerial Order of 11 June 2018, which approves the certification reference framework drawn up by the Digital Health Agency (ANS), it refers to ISO standards and additional requirements such as encryption and authorisation management. A more stringent and restrictive certification reference framework drawn up by the ANS has been awaiting approval from the European Commission since 2022.
-

The National Information Systems Security Agency (ANSSI) is a governmental agency operating under the authority of the General Secretary for Defence and National Security to ensure correct application of the law and, more precisely, the security of the network and information systems. Its prerogatives have been extended by the Military Programming Act of 2018 and again by the Military Programming Act of 2023.

- The Military Programming Act No. 2023-703 of 1 August 2023 for 2024 to 2030. The purpose of this act is to strengthen three areas in cyber defence:
    - allow a specific budget for planned needs (personnel and technologies);
    - support ANSSI; and
    - strengthen its capacities for the analysis and detection of cyberthreats (notably by including an obligation for software publishers to inform ANSSI of any vulnerability of their products).
- Law No. 2022-309 of 3 March 2022, which came into force on 1 October 2023, on 'cyberscore' (similar to the nutriscore logo). The purpose of this Act is to provide internet users with clear information about the security of their data and 'cyber' quality of the sites they visit by making mandatory a cybersecurity certification for consumer digital platforms based on the number of their users. It should be noted that there is as yet no application decree, meaning that this law is not yet applicable.
- Even before the EU General Data Protection Regulation (GDPR) entered into force, the Data Protection Act of 1978 (modified by Ordinance No. 2018-1125 of 12 December 2018/Law No. 2022-52 of 24 January 2022) took into consideration cybersecurity, ensuring that when dealing with personal data, technical and organisational measures shall be implemented by data controllers and processors, either private or public, to ensure a level of security appropriate to the risk when processing personal data. These include protection from unauthorised access, alteration or theft. Additionally, internet service providers (ISPs) processing personal data are obliged to inform the French Data Protection Authority (CNIL) immediately in case of a breach. These ISPs are even compelled to keep records of cyberattacks. Under the GDPR, applicable since 25 May 2018, these obligations have been extended to all data controllers and processors, private and public. Failure by private and public data controllers and processors to take adequate security measures could have led to an administrative fine of up to €3 million according to the Data Protection Act of 1978. Since the entry into force of the GDPR, data controllers and processors may face an administrative fine of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million, whichever is higher, in case of failure to report and adopt appropriate security measures. By Act No. 2018-493 of 21 June 2018, France formally implemented the GDPR legal provisions.
- Reference shall be made to Directive (EU) 2016/1148 on Security of Network and Information Systems (the NIS Directive), adopted by the European Union on 6 July 2016. This Directive requires operators of essential services and digital service providers to adopt security measures and to report incidents affecting networks and information systems. The NIS Directive was transposed into French law by Act No. 2018-133 of 26 February 2018 and Decree No. 2018-384 of 23 May 2018.
- Lastly, reference shall also be made to:

- EU Regulation 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), which will come into force on 17 January 2025. The purpose of this act is to promote a common set of rules and standards aimed at investigation of information and communications technology risks for financial entities. This should allow for the first time a homogeneous application of the principles and rules of IT risk management in the financial sector.
- Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) is based on the achievement of the NIS Directive and broadens its objectives and scope of applicability to provide greater protection in terms of cyber regulation (to thousands of entities belonging to more than 18 sectors – 600 different types of entities, including administrations of all sizes and companies ranging from SMEs to CAC 40 groups). Its sanction regime will apply to all subject entities and may, depending on the offences, be based on a percentage of the global turnover of the entity considered.
- Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER Directive) deals with the physical security of legal entities or administrations critical to ensuring the functioning of essential services for the maintenance of vital societal functions or economic activities (internal market). These critical entities must carry out risk assessments, including IT risk assessments (as detailed in the NIS2 Directive).

It is worth noting that the French bill on the resilience of critical infrastructures and the strengthening of cybersecurity, which includes the transposition of the DORA Regulation and the NIS2 and CER Directives, was presented to the Council of Ministers on 15 October 2024. The text is expected to be reviewed and voted on by the French Parliament in the first half of 2025.

-
  - Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) entered into force on 10 December 2024. The Act enhances cybersecurity for internet-of-things devices, requires supply chains (manufacturers, importers and distributors) to take responsibility for security and compliance, and enforces mandatory requirements spanning the entire lifecycle of products. The main requirements introduced by the Act will apply from 11 December 2027.
  - Regulation (EU) 2024/1689 on artificial intelligence (Artificial Intelligence Act) entered into force on 1 August 2024. The Act establishes various cybersecurity requirements for high-risk artificial intelligence (AI) systems. These requirements are in addition to the security and resilience obligations fixed in other key EU regulations, such as the NIS2 Directive and the DORA Regulation.

Law stated - 9 January 2025

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Since the creation of ‘operators of vital importance’ in 2013, sectors have been added to the category to reach the current list of the following 12 sectors: healthcare products, water management, food, energy, transport, audiovisual and IT, electronic communications and the internet, industry, finance, nuclear, defence industrial activities and space.

The NIS Directive enlarged the scope of crucial sectors, establishing new categories of sectors concerned ('essential service operators' and 'digital service providers'), but with fewer obligations and restrictions than for operators of vital importance.

The NIS2 and CER Directives employ a modified approach to the classification of entities, this depending on their size, importance and activities rather than their sectors as such. Thus, the concepts of essential service operators and digital service providers are now merged, and entities are classified as ‘essential entities’ or ‘important entities’.

The sectors most affected by security laws and regulations are the sectors providing essential services for the functioning of society and include the energy, transport, water, banking, financial market and healthcare industries. An exhaustive list of those sectors is provided in Decree No. 2018-384 of 23 May 2018. Importantly, each entity must know to which classification it belongs (and thus respect the applicable rules), and no longer expect a ministerial order to declare its classification before respecting the applicable rules.

The list of entities affected by security laws will be extended with the transposition of the NIS2 Directive and will include entities in the following sectors: postal services, waste management, chemicals, research, foods and manufacturing.

On a more general aspect, every data controller and processor, whether private or public, is also bound by the Data Protection Act of 1978 and the GDPR to provide adequate security measures when collecting, processing, transferring and storing data. In this regard, to meet this obligation and comply with article 32 of the GDPR, data controllers must adopt cybersecurity measures.

Law stated - 9 January 2025

International standards

3 Has your jurisdiction adopted any international standards related to cybersecurity?

France acknowledges the ISO standards, and the French hosting health data certification is partially based on the ISO 27001 and ISO 20000-1 standards.

Regulation (EU) 2019/881 of 17 April 2019 set up an U-wide cybersecurity certification framework to prevent the risk associated with the use of information and communications technology (ICT) products, services and processes . The European Commission adopted on 31 January 2024 the first EU certification framework : the EU Cybersecurity Certification

Scheme on Common Criteria. ANSSI will be in charge of supervising the application of the scheme in France.

Law stated - 9 January 2025

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Pursuant to article 32 of the GDPR, data controllers and processors processing personal data shall implement adequate technical and organisational measures to ensure a level of security appropriate to the risk. These include protection from unauthorised access, alteration and theft. ISPs (extended to all data controllers and processors under the GDPR) processing personal data are also bound to inform CNIL immediately in case of a breach. They are also compelled to keep records of cyberattacks.

According to article 83 of the GDPR, non-compliant personnel and directors may be fined up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million by CNIL. Additionally, pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and be fined up to €300,000. This amount is multiplied by five for legal entities, pursuant to article 131-38 of the Criminal Code.

A relatively important act was adopted on 27 March 2017, namely Act No. 2017-399. This Act requires that firms with more than 5,000 workers in France undertake a mapping of the potential risks that may negatively affect public liberties, fundamental rights and health and security, and take appropriate measures to mitigate their effects. This mapping must identify the risks, categorise their level of importance and analyse their potential consequences.

The DORA Regulation requires financial institutions to regularly test and update their operational resilience plans and train their staff to be prepared to respond to operational disruptions. Article 5 of the DORA Regulation assigns responsibility to the managing body.

Law stated - 9 January 2025

Key definitions

5 How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Neither cybersecurity nor cybercrime has been precisely defined by a law in France.

In 2017, the concept of 'cybersecurity' was defined by the Ministry of Higher Education and Research in the Official Bulletin No. 36 of 26 October 2017 as the 'state of an information system that withstands cyberattacks and accidental failures occurring in cyberspace'.

Also, ANSSI published on 15 July 2024 its CyberDico, which gives definitions of words, expressions and acronyms in the field of cybersecurity. 'Cybersecurity' is defined as '[t]he desired state of an information system, enabling it to withstand events originating in

cyberspace that could compromise the availability, integrity or confidentiality of the data stored, processed or transmitted, and the related services that these systems offer or make accessible. Cybersecurity calls on information systems security techniques, and is based on the fight against cybercrime and the implementation of cyberdefence'. 'Cybercrime' is defined as the 'acts that contravene international treaties or national laws, using networks or information systems as a means of committing a crime, or targeting them'.

According to article 3 of Regulation (EU)2019/881 relating to ENISA (European Union Agency for Cybersecurity) and cybersecurity certification of information and communications technologies (Cybersecurity Act): ‘cybersecurity’ means 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'. The Cybersecurity Act also defines ‘cyberthreat’ as 'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons'.

A distinction must be made between cybersecurity and data privacy, as cybersecurity is considered to be a component of data privacy under French and EU law. As such, to have data privacy, cybersecurity measures would have to be implemented. In addition to this distinction, France’s cybersecurity and cybercrime policies are increasingly seen as sections of the cyber defence policy.

Law stated - 9 January 2025

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In September 2017, ANSSI published 42 measures to protect data and IT systems from cyberthreats. According to these measures, cybersecurity shall be seriously addressed and, therefore, ANSSI generally recommends to firms and organisations that they, among others:

- raise awareness;
- regularly update their IT systems;
- restrict access and encourage the use of strong authentication;
- conduct an audit;
- encrypt highly sensitive data and information when they are transferred; and
- decentralise their network.

The same measures have been recommended by CNIL to personal data controllers and processors, whether private or public. Regarding personal data, the GDPR requires a level of security adapted to the digital risk. It affirms the importance of assessing and dealing with risks to individuals. In particular, it requires organisations to implement appropriate technical or organisational measures, which may include encryption of data and tools to ensure confidentiality, integrity, availability and resilience.

Regarding essential sectors, several ministerial orders were adopted in 2016 and 2017. These orders provide for compulsory security measures, such as adopting detection tools, defensive tools, strong authentication and restricted access protocols that shall be taken by entities mainly operating in the electricity, maritime, finance, ISPs, space, gas, media, nuclear and arms industries.

In 2023, CNIL launched a new guide covering a range of measures, from basic precautions that 'should be implemented' to devices that strengthen data protection. The guide consists of 17 practical sheets covering aspects such as protecting the internal IT network, securing servers, protecting websites, backup and business continuity planning, secure archiving, monitoring IT developments and managing subcontracting. Although these recommendations are not mandatory, CNIL may consider a breach of security by referring to its guide and assessing non-compliance with these precautions as a criterion.

Lastly, the NIS2 Directive adopts a comprehensive 'all-hazards' approach and imposes a set of minimum measures on companies falling within its scope, as well as on their IT service providers. These measures include policies relating to risk analysis and the security of information systems, incident management, basic cyber hygiene practices and cybersecurity training (article 21). Although this directive has not yet been transposed in France, transposition should be completed during the first half of 2025.

Law stated - 9 January 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Naturally, any cybercriminal offence committed that has been catered for in the Criminal Code shall apply to intellectual property (see below). Similarly, any violation of intellectual property that has been catered for in the Intellectual Property Code shall apply to cyber acts or acts committed in cyberspace. However, and on a more specific note, the law better protects against copyright breach and counterfeiting of trademarks and patents on the internet. Counterfeiters may face a fine of up to €500,000 (multiplied by five for organisations) and up to five years of imprisonment.

Cybersquatting is amenable to a €15,000 fine (multiplied by five for organisations) and up to one year of imprisonment. Providing software for the purpose of encouraging copyright breach may lead to a fine of up to €300,000 (multiplied by five for organisations).

Article L335-3-1 of the French Intellectual Property Code could be invoked. This article sanctions, by fine and imprisonment, alteration of the protection of a work (effective technical measure) by decoding, decryption or any personal intervention intended to circumvent, neutralise or remove a protection or control mechanism for a purpose other than research.

Law stated - 9 January 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Pursuant to the Military Programming Act of 2013 for 2014 to 2019, the state has a duty and responsibility to take appropriate measures to protect essential sectors that are deemed 'of utmost importance for state survival'.

Pursuant to the Military Programming Act No. 2023-703 for 2024 to 2030, ANSSI's capabilities in addressing cyberthreats have been enhanced – notably, its detection capabilities of cyberattacks by accessing the content of communications and by being aware of the identity of presumed victims of cyberattacks for entities considered as 'operators of vital importance' . Also, its article 64 provides for mandating operators to filter domain names to counteract a potential threat to national security. Lastly, article 66 imposes on software publishers the obligation to notify ANSSI and users of any significant incidents or vulnerabilities concerning their products.

It should be noted that the NIS2 Directive provides for the creation of an EU vulnerability database, managed and updated by the EU Agency for Cybersecurity.

Additionally, the CER Directive, which will be transposed in France in the first half of 2025, aims to strengthen the resilience of infrastructures considered critical by member states, across a range of sectors (including energy, transport, banking, healthcare, water, food, digital infrastructure, public administration and space). The CER Directive introduces new obligations for these entities, including the requirement to conduct their own risk management assessments, implement resilience measures and report significant incidents.

Law stated - 9 January 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

France does not have any cybersecurity laws or regulations that specifically restrict the sharing of cyberthreat information. Such an approach will not be coherent and will surely hinder the proactive approach adopted to tackle cybercrime and cyberattacks. Article L2321-4 of the Defence Code even provides for the sole purpose of protecting an information system, namely that someone acting in good faith may inform ANSSI about a cyberthreat. The whistle-blower's identity is also protected. Moreover, dedicated websites have been set up to disclose cyberthreats and vulnerabilities.

Additionally, if every individual has a right to privacy, which entails the right to private communication, this right may be levied, and metadata can be accessed by the government in cases of terrorism and organised crime.

The European Union appears to be moving towards information sharing; indeed, the DORA Regulation aims to promote collaboration among financial entities by facilitating the sharing of information and intelligence on cyberthreats. Its goal is to leverage the knowledge and

practical experience of each entity at strategic, tactical and operational levels to enhance entities' ability to effectively assess and monitor cyberthreats.

Reference should also be made to the NIS2 Directive, which dedicates Chapter VI to information sharing and requires member states to ensure that companies can voluntarily exchange relevant information on cybersecurity. This includes data related to cyberthreats, averted incidents and vulnerabilities.

Law stated - 9 January 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

France has enacted laws regarding a wide range of cybercrime-related offences since 1988. In this regard, the following cyberactivities are criminalised:

- Any cyberattack on an information system (article 323-1 of the Criminal Code) through unauthorised access or maintenance is criminalised, and cybercriminals may face a fine of up to €60,000 and up to two years of imprisonment (this fine is multiplied by five for organisations, thus up to €300,000).
- Should this access or maintenance lead to the alteration or deletion of data contained in the system or alter the good running of the system, this will be constitutive of an additional offence amenable to a fine of up to €100,000 (multiplied by five for organisations) and imprisonment of up to three years.
- Attacking state-operated information systems may lead to five years of imprisonment and a fine of up to €150,000 (multiplied by five for organisations).
- Any cyberattack that disrupts or distorts the good running of an information system is sanctioned by up to five years of imprisonment and a fine of up to €150,000 (multiplied by five for organisations). Disrupting or distorting state-operated information systems is sanctioned with seven years of imprisonment and a fine of up to €300,000 (multiplied by five for organisations).
- Introducing, extracting, cloning, transferring, modifying or deleting data into or from an information system is sanctioned with a fine of up to €150,000 (multiplied by five for organisations) and up to five years of imprisonment. Should the above-mentioned acts be committed to a state-operated information system, contraveners will face a fine of up to €300,000 (multiplied by five for organisations) and up to seven years of imprisonment.
- Importing, proposing or possessing any equipment, software or other tool developed to commit cybercriminal activities is amenable to the same sentence as the act itself or whichever sentence is higher.
- The organised commission of cybercriminal activities is amenable to the same sentence as the act itself or whichever sentence is higher. However, the organised commission of cybercriminal activities against information systems operated by

the state is amenable to 10 years of imprisonment and a fine of up to €300,000. (Attempts are sanctioned in the same manner as the act itself.)

- Any unlawful collection, use, storage, transfer and processing of personal data, and failure to meet the security obligations and respect the right to object are also criminal offences amenable to a fine of up to €300,000 (multiplied by five for organisations) and up to five years of imprisonment.
- Impersonation or identity theft is amenable to one year of imprisonment and a fine of up to €15,000 (multiplied by five for organisations).
- Credit or debit card fraud is amenable to seven years of imprisonment and a fine of up to €750,000 (multiplied by five for organisations). Importing, proposing or possessing any equipment, software or other tool developed to commit credit or debit card fraud is amenable to the same sentence as the act itself or whichever sentence is higher.
- Cyber scams, such as phishing, are punishable by five years of imprisonment and a fine of up to €375,000 (multiplied by five for organisations).
- A breach of trust committed by means of accessing an information system is amenable to three years of imprisonment and a fine of up to €375,000 (multiplied by five for organisations).

The legislator has enhanced the investigatory powers of the police and established specialised cybercrime courts to deal in an efficient manner with cybercrime and attacks.

Additionally, dedicated institutional internet websites aiming to fight against unlawful cyber acts have been set up and allow the public to report such acts (eg, Pharos).

Law stated - 9 January 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

In December 2016, ANSSI published its binding guidelines on the minimum cybersecurity standards and requirements that businesses offering software as a service, platform as a service and infrastructure as a service must maintain(the SecNumCloud). As such, it provides for the basic security measures (physical, environmental and operational), update policy, internal risk management (before and after cyberattacks), database and network management and information security policies, among others. This SecNumCloud certificate ensures the resilience of the provider's solution against the most common cyberattacks. It thus represents an economic advantage, allowing the identification of the solution as robust, reliable and trustworthy. The requirements of the framework ensure the protection of the cloud service through three types of measures: (1) technical measures ensuring tightness; (2) operational measures limiting interventions; and (3) legal measures involving the exclusive application of European law. Access to the latest version of the framework is via https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-

exigences-v3.2.pdf. On 5 October 2020, ANSSI published a list of cloud computing providers that are certified, as they meet these security standards.

Annex 1 of the Military Programming Act for the years 2024 to 2030 reinforces the importance of the SecNumCloud certification. All sensitive data falling within its scope must be stored on servers compliant with this certification or with a European certification guaranteeing at least an equivalent level of security. In this regard, whether it be servers within operators of vital importance or those of their commercial partners, certification is now mandatory.

A European cloud certification project (EUCS: EU Cloud Services) is currently underway to align standards among EU member states. However, so far, the French SecNumCloud certification remains the most stringent in Europe.

Additionally, CNIL published its recommendations for businesses storing personal data on cloud service providers in 2012. CNIL is very clear about the matter: cloud computing firms shall guarantee their compliance with French and EU legislation on data protection laws. Security measures are a core subject in this recommendation. It has provided a template that consists of the essential clauses and aspects that must be covered in a cloud computing contract. In 2021, CNIL approved the first European code of conduct dedicated to infrastructure as a service providers (codes of conduct help streamline compliance and demonstrate adherence to prevailing regulations).

Lastly, a specific certification is mandatory for hosting personal health data. This certification (HDS) is governed by Decree No. 2018-137 of 26 February 2018. Any company seeking HDS certification must meet the criteria outlined in the certification framework published by the Digital Health Agency.

Law stated - 9 January 2025

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Data controllers and processors are bound by the obligation to secure the processing of personal data. In this regard, article 121 of the French Data Protection Act of 1978 and article 32 of the GDPR require that foreign organisations operating in France or offering goods or services (irrespective of whether a payment of the data subject is required) to such data subjects in France are bound by cybersecurity measures. The monitoring of their behaviour (as far as it takes place) within France is also bound by these measures.

Notwithstanding this particular case and, from a broader perspective, from the moment a cybercriminal offence is committed in the French territory, French law and French jurisdiction apply, pursuant to article 113-2 of the Criminal Code. In this regard, whether foreign organisations are the victims or perpetrators of cybercrime, they are bound by the Criminal Code if the offence is committed in France.

The Military Programming Act No. 2013-1168 of 2013 aims to ensure a broad application of the obligations it imposes on providers of information technology and telecommunications services.

Law stated - 9 January 2025

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The National Information Systems Security Agency (ANSSI) and the French Data Protection Authority (CNIL) recommend additional cybersecurity protections beyond those that are mandated by law. As such, 42 measures to protect data and IT systems from cyberthreats have been published.

According to these measures, cybersecurity shall be seriously addressed and, therefore, it is generally recommended that firms and organisations, among others:

- raise awareness;
- regularly update their IT systems;
- restrict access and encourage the use of strong authentication;
- conduct an audit;
- encrypt highly sensitive data and information when they are transferred; and
- decentralise their network.

The same measures have been recommended by CNIL to personal data controllers and processors, whether private or public. In 2023, CNIL launched a new guide covering a range of measures, from basic precautions that 'should be implemented' to devices that strengthen data protection. The guide consists of 17 practical sheets covering aspects such as protecting the internal IT network, securing servers, protecting websites, backup and business continuity planning, secure archiving, monitoring IT developments and managing subcontracting.

Regarding personal data, the EU General Data Protection Regulation (GDPR) requires a level of security adapted to the digital risk. It affirms the importance of assessing and dealing with risks to individuals. In particular, it requires organisations to implement appropriate technical or organisational measures, which may include encryption of data and tools to ensure confidentiality, integrity, availability and resilience.

ANSSI has set up a certification in the cloud domain (SecNumCloud). This certification is optional, except for operators of vital importance and their business partners.

Regarding essential sectors, several ministerial orders were adopted in 2016 and 2017. These orders provide for compulsory security measures, such as adopting detection tools, defensive tools, strong authentication and restricted access protocols that shall be taken

by entities mainly operating in the electricity, maritime, finance, internet service providers, space, gas, media, nuclear and arms industries.

Law stated - 9 January 2025

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

France is increasingly focusing on the cybersecurity challenges faced by businesses as part of its national strategy:

- The National Cybersecurity Strategy, led by the government and launched in February 2021, is now integrated into the France 2030 investment plan. The Strategy aims to double the employment and triple the turnover of the cybersecurity sector. To achieve these goals, the Strategy revolves around four major pillars: (1) developng new innovative solutions; (2) strengthening ties among stakeholders in this sector; (3) raising awareness among the French population; and (4) training the next generation in cybersecurity. As part of the Strategy, a cyber campus was inaugured on 15 February 2022, aimed at fostering collaboration among businesses, government services and associations. For instance, in December 2022 ANSSI and the Business Continuity Club organised a one-day simulation exercise of a cyber crisis. The goal was to prepare over 160 professionals for a worst-case scenario, enabling them to respond effectively in the event of a cyberattack. Moreover, thanks to the Strategy, several waves of support for innovative projects have already taken place, in 2022 and 2023. The third wave of the call for projects focused on one of the key 'gestures' contributing to digital sovereignty – namely, the assessment of cybersecurity.
- The French regulatory authorities, notably ANSSI for cybersecurity and CNIL for data protection, play a crucial role in strengthening cybersecurity in France and are particularly committed to training and raising awareness among stakeholders and users. Additionally, they develop guidelines and recommendations aimed at enhancing compliance and fostering a better understanding of issues for stakeholders.
- Incident response has improved, with mechanisms now implemented to assist businesses in addressing attacks and minimising damage. This involves close coordination between government authorities and private sector stakeholders: (1) implementation of a single point of contact, cybermalveillance.gouv.fr, connecting victims with local, competent service providers across the national territory; and (2) CERT-FR Technical Handling addresses, from a technical perspective, cybersecurity incidents for operators of vital importance, operators of essential services and digital service providers (which, under the NIS2 Directive ((EU) 2022/2555), will be designated as essential and important enterprises).

Law stated - 9 January 2025

Industry standards and codes of practice

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The 42 measures to protect data and IT systems from cyberthreats (which are very broad) can be accessed here.

A dedicated website has also been set up to help small and medium-sized enterprises, and can be accessed here.

CNIL has also released detailed guidelines and a checklist regarding the good safekeeping of personal data, available respectively here and here.

Law stated - 9 January 2025

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

France has adopted best practices and procedures. As such, ANSSI and CNIL recommend that the first step is to have recourse to a host-based intrusion detection system and a network-based intrusion detection system to identify in real time and certify the extent of the intrusion (compulsory for organisations identified as of essential importance).

If a breach is identified, it is recommended that the organisation should:

- disconnect the affected IT system from the network;
- inform the local computer emergency response team;
- make a clone copy of the hard disk drive;
- gather evidence and search for a digital footprint; and
- file a complaint to the police.

After the attack, it is recommended that, to analyse the intrusion, organisations should:

- search for any modifications made to the operating system and operating system files;
- analyse if there has been any alteration or modification of data;
- search for any data or tool that may have been introduced by the hacker;
- analyse the logs;
- look for any sniffer on the network; and
- analyse the other devices and hardware connected to the affected network.

For organisations of essential importance, notification shall be made to ANSSI. If required, for private and public data controllers and processors, notification shall be made to CNIL.

For healthcare professionals, the website cyberveille-sante.gouv.fr serves as a comprehensive resource providing in-depth information on potential threats and best practices in digital security. It offers reflex sheets and guides to assist in managing various incidents. Additionally, this portal provides a confidential space for the healthcare SSI community, fostering exchanges among cybersecurity experts.

Law stated - 9 January 2025

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Article L2321-4 of the Defence Code provides that, for the sole purpose of protecting an information system, someone acting in good faith may inform ANSSI about a cyberthreat. Further, the whistle-blower's identity is protected, and several websites have been set up to encourage the sharing of information.

In this regard:

- illegal internet content may be declared here;
- vulnerabilities may be declared here;
- information on cyberthreats and vulnerabilities is available here;
- a section dedicated to best practices is available here; and
- for healthcare professionals, best practices and information is available here.

Law stated - 9 January 2025

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The government and the private sector cooperate through non-profit organisations. As such, ANSSI (acting on behalf of the government) and large companies such as Thales, Airbus and Enedis form part of the European Cyber Security Organisation (ESCO). The ESCO combines public and private entities and aims to develop, promote and encourage European cybersecurity. Additionally, a public-private partnership on cybersecurity was signed on 5 July 2016 to better equip the European Union against cyberattacks and to strengthen the competitiveness of its cybersecurity sector. Naturally, these include, and will benefit, French industries and the government.

In 2022, a cyber campus was set up to bring together the main national and international cyber players to protect society at large. It allows companies (large corporations, SMEs and startups), state services, training organisations, research players and associations to

be hosted on the same site to develop synergies between these different actors. So far, more than 160 stakeholders are involved.

Law stated - 9 January 2025

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

A new law, No. 2023-22 of 24 January 2023 incorporated into the Insurance Code, introduced a new requirement for companies affected by a cyberattack: regarding the right to reimbursement by insurance for damages caused by cyberattacks, including ransoms paid by companies affected by ransomware, insurance compensation will be conditional on the victim filing a complaint with the competent authorities within 72 hours of the attack.

Law stated - 9 January 2025

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Military Programming Act No. 2013-1168 of 18 December 2013 for 2014 to 2019 defines the National Information Systems Security Agency (ANSSI) as the primary authority for enforcing cybersecurity rules when dealing with organisations of vital importance.

When dealing with personal data, the French Data Protection Authority (CNIL) is responsible for enforcing cybersecurity rules as well as prosecuting administratively, pursuant to the Data Protection Act of 1978 and the EU General Data Protection Regulation (GDPR).

Neither entity has the power to prosecute criminally since this falls within the sole jurisdiction of the public prosecutor.

Additionally, the Ministry of the Interior also contributes to cybersecurity management, particularly in the prevention of and response to incidents (its services investigate acts of malicious cyberactivity, identify perpetrators and then bring them to justice). The Ministry of the Interior's Programming Law for the years 2023 to 2027 (adopted on 24 January 2023) allocated a substantial budget to modernising the means of combating cybercrime. As a result, on 23 November 2023 a significant reorganisation in the field of cybercrime was carried out through the adoption of four new texts, establishing the creation of three new specialised services:

- Decree No. 2023-1084 established the Ministry of the Interior Command in Cyberspace (COMCYBER-MI). This team extends its mission to the entire national

territory to combat cybercrime, defined as any cyber violation of international treaties. COMCYBER-MI will also develop the ministerial strategy for combating cybercrime.

- Decree No. 2023-1083, along with its ministerial order, gave rise to the Anti-cybercrime Office, affiliated as of 1 December 2023 to the national director of judicial police.
- A ministerial order established a National Cyber Unit within the National Gendarmerie.

Law stated - 9 January 2025

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Anti-cybercrime Office and the National Cyber Unit (established by the aforementioned texts on 23 November 2023) operate at national level and are involved in the prevention and repression of organised or transnational cybercrime. Their tasks include conducting investigations and improving operational coordination between the services involved in the fight against cybercrime.

Regarding the enforcement of security measures provided in the Data Protection Act of 1978 and the GDPR, compliance, monitoring, investigations and administrative prosecution will be conducted by CNIL. As such, for monitoring and conducting investigations, CNIL can go on-site and search and seize any relevant documents and information. When an offence has been proved, it has the power to prosecute administratively, but most importantly, the power to impose fines, issue injunctions, remove authorisation for data processing, impose warnings and publish its decisions.

ANSSI is responsible for carrying out compliance monitoring and investigations for sectors of essential importance and any information system that is operated by the state.

The above-mentioned entities do not have the power to prosecute criminally and request criminal sanctions provided in the Criminal Code, as this power is vested in the public prosecutor only. However, ANSSI, with the transposition of the NIS2 Directive, will be able to issue injunctions and impose fines up to €10 million or 2 per cent of the annual turnover of the cybercriminal.

Law stated - 9 January 2025

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Concealment of data breaches is an important issue because organisations fear the negative impact that will follow and, given the particular consequences of cyberattacks (for the economy when speaking of sectors of essential importance or for personal data regarding the right to privacy), the legislator has imposed heavy fines for non-compliance to encourage enforcement. Additionally, the legislator has also encouraged whistle-blowers to inform ANSSI, but this information must be communicated in good faith. Dedicated websites have even been set up to facilitate notification to the respective authorities on cyberattacks, data breaches and incidents.

The creation of the Anti-cybercrime Office and the National Cyber Unit may have positive impacts on this matter.

Law stated - 9 January 2025

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Several actors are required to report incidents to ANSSI 'without delay':

- Operators of vital importance are compelled, under the Defence Code, to report any incident impacting on the operation or security of their industrial information systems. The types of incidents to be reported vary by sector and are detailed by ministerial order.
- Operators of essential services (soon to be replaced under the NIS2 Directive (2022/2555)must report any incident 'likely' to impact on the service's operation and any incident affecting the security of their industrial information systems.
- Digital service providers (soon to be replaced under the the NIS2 Directive must report any incident 'having a significant impact' on the service.
- Trusted providers of electronic identification and trust services for electronic transactions must report any security breach with a 'significant impact' on the service (according to the eIDAS Regulation (EU) 910/2014).

The relevant personnel dealing with products and services qualified by ANSSI must report any incident affecting or likely to affect the product or service.

In the event of a personal data breach (which includes deliberate security breaches by third parties and accidental loss or corruption of data) that may likely result in a risk to the rights and freedom of individuals, any 'data controller' businesses that are victims of such a breach must notify CNIL 'without undue delay and, where feasible, not later than 72 hours' after having become aware of the breach (article 33 of the GDPR and article 58 of the French Data Protection Act). Any 'data processor' businesses must notify the data controller without undue delay after having become aware of the breach (the notification to CNIL resting on the data controller once aware of the breach).

When a personal data breach is 'likely to result in a high risk for the rights and freedoms' of individuals, data controller businesses must inform the individuals without undue delay of the breach, unless:

- appropriate protection security measures or subsequent satisfactory measures to avoid such a risk have been taken;
- it would involve disproportionate effort (article 34 of the GDPR and article 58 of the French Data Protection Act) and so alternative solutions could be considered (public communication);
- the profile of the persons concerned is sensitive (police officer, military, civilian staff of the Ministry of Defence, customs officers); or
- such information may pose a risk to national security, national defence or public security.

Lastly, it is now imperative to respect the new mandatory 72-hour deadline, as stipulated in the Insurance Code, in order to qualify for insurance reimbursement.

Law stated - 9 January 2025

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Since 25 May 2018, the GDPR provides that non-compliance with personal data security measures may be subject to an administrative fine by CNIL of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million. Additionally, pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and face a fine of up to €300,000 (multiplied by five for organisations). Organisations of essential importance may be subject to criminal fines of up to €150,000 in cases of contravention of cybersecurity laws, pursuant to article L1332-7 of the Defence Code.

In addition, a section of the French Penal Code is specifically dedicated to offences against the rights of individuals arising from files or computer processing. However, the Penal Code refers to both the French Data Protection Act and the EU GDPR. Indeed, French law adds further provisions, in particular when it comes to the use of the social security number. Additionally to the fines provided for by the GDPR as penalty, the French Penal Code provides for imprisonment.

Law stated - 9 January 2025

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Pursuant to article 83 of the GDPR, personal data controllers and processors that fail to comply with the rules on reporting breaches (provided in article 33) may face an administrative fine by CNIL of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million. Organisations of essential importance may be subject to a €150,000 fine in the case of contravention of cybersecurity laws. Additionally, and pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and be fined up to €300,000 (multiplied by five for organisations).

The Military Programming Law No. 2013-1168 of 18 December 2013 provides that operators of vital importance are obligated to immediately report incidents affecting their information system. The same law introduced a sanction of €150,000 in case of non-compliance (after formal notice) with this notification obligation, as stipulated in the Defence Code.

Law No. 2018-133 of 26 February 2018 (transposing the original NIS Directive (2016/1148/EC)) imposed an obligation to notify ANSSI (under different conditions). This obligation is accompanied by a fine of €75,000 for executives of operators of essential services and €50,000 for executives of digital service providers, in case of non-compliance.

Law stated - 9 January 2025

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties can seek private redress for any unauthorised cyberactivity or failure to adequately protect systems and data under article 1240 of the French Civil Code. As such, and under the cause of action of negligence, parties may seek damages as a result of the damage suffered.

Law stated - 9 January 2025

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

It depends on whether the organisation is defined as an organisation of essential importance or whether the organisation is considered a data controller or processor.

For organisations of essential importance, rules and procedures are imposed on them by either decree, ordinance or ministerial orders. As such, since 2016, entities operating in the electricity, maritime, finance, internet service providers (ISPs), space, gas, media, nuclear and arms industries shall adopt compulsory security measures, such as detection tools, defensive tools, strong authentication and restricted access protocols.

The same cybersecurity measures have been recommended by the French Data Protection Authority (CNIL) regarding personal data on data controllers and processors, private or public. The EU General Data Protection Regulation (GDPR) has even provided, under article 32, security requirements that may be expected from data controllers and processors, namely:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Law stated - 9 January 2025

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

France has rules requiring organisations to keep records of cyberattacks. As such, pursuant to article 83 of the Data Protection Act of 1978 ISPs are required to keep records of cyberattacks. Article 33 of the GDPR extends this obligation to all data controllers and processors. The records are collected by way of audit and must specify how the attack happened, its consequences and the measures taken. The law does not specify for how long these records must be kept.

Law stated - 9 January 2025

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Pursuant to article 83 of the Data Protection Act of 1978, ISPs must report, without delay, data breaches to the CNIL. Under the GDPR, this obligation is now borne by every data controller and processor, private or public.

According to the guidelines on the notification of personal data breaches under EU Regulation 2016/679 (revised and adopted on 6 February 2018) established by the European Data Protection Board (EDPB), three types of incidents must be reported:

- confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data;
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and

- integrity breach – where there is an unauthorised or accidental alteration of personal data.

The EDPB fleshed out this definition by presenting concrete cases in the 'Guidelines 01/2021 on Examples regarding Personal Data Breach Notification', based on insights gained from the experiences of data protection authorities in recent years. The 18 listed practical examples cover various types of personal data breaches and outline the obligations to be followed depending on the circumstances. Each case specifies, among other things, whether notification to the authority is required and if the breach must be disclosed to the individuals concerned.

To facilitate reporting, dedicated forms have been provided online and, in the particular case of personal data, can be submitted online.

Regarding organisations of essential importance and in accordance with article L1332-7 of the Defence Code, they must report any cybersecurity breach or incident to the National Information Systems Security Agency (ANSSI).

Notification of violation and breach is followed by a report. Information required in reports of cyberthreats depends on the business sector of the organisation considered of essential importance. Regarding personal data, the GDPR is more precise on the matter: data controllers and processors must provide precise information on the time of the attack, its nature, the personal data affected, the remedies applied and the potential consequences of the breach, among others.

Incident notification forms can be found on the ANSSI website:

- for operators of vital importance, the form is available here;
- for operators of essential services, the form is available here;
- for digital service providers, the form is available here; and
- for qualified products and services (including qualified trusted service Providers and non-qualified providers of electronic identification, as well as trust services for electronic transactions), the form is accessible here.

It should be noted that the NIS2 Directive ((EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union) (not yet transposed into French law) requires for essential and important entities an initial notification called 'early warning' in case of a significant incident and an incident notification within 72 hours of becoming aware of the significant incident

Law stated - 9 January 2025

Time frames

30 | What is the timeline for reporting to the authorities?

Entities must report without any delay to CNIL when personal data is concerned, and to ANSSI if the entities affected are qualified as of essential importance. The GDPR provides

more precision about the timeline, namely that the incident must not be reported later than 72 hours (where feasible) after the entity has become aware of the breach.

To facilitate reporting, dedicated forms have been provided online and, in the particular case of personal data, can be submitted online.

Under the NIS2 Directive (not yet transposed in France), essential and important entities must proceed to an initial notification called 'early warning' in case of a significant incident without undue delay within 24 hours. They should also submit an incident notification within 72 hours of becoming aware of the significant incident

Law stated - 9 January 2025

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

According to article 83 of the Data Protection Act of 1978 and in the case of a personal data breach, ISPs are compelled to report, without any delay, to customers aggrieved by such breach. This obligation has been extended to all data controllers and processors under the GDPR. Such notification may be levied if CNIL certifies that appropriate measures have been taken to make direct or indirect identification impossible. According to article 29 of the Data Protection Working Party, in its guidelines on personal data breach notification for the new regulation, dedicated messages should be used when communicating a breach. These include, among others:

- direct messaging (eg, email, SMS and direct message);
- prominent website banners or notifications;
- postal communications; and
- prominent advertisements in print media.

Law stated - 9 January 2025

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The exchange of information between companies, state services and cyber players – notably when informed of cyberthreats or attacks – could improve the capabilities to react to an attack, and later hopefully to anticipate attacks.

Law stated - 9 January 2025

Claire Bernier clairebernier@adsto.legal

ADSTO

Read more from this firm on Lexology

Germany

Kristina Schreiber, **Dennis Pethke**
Loschelder Rechtsanwälte

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Cybersecurity in Germany is mainly governed by the Act on the Federal Office for Information Security (BSI Act). The Act regulates the tasks of the Federal Office for Information Security (BSI) to promote the security of information technology. Above all, certain obligations are laid down for a high level of information security for German critical infrastructure protection (KRITIS) operators. This includes, for example, state-of-the-art security, such as measures to detect attacks. In the event of incidents, there are reporting obligations and the authority has extensive powers to ensure security of supply. Exactly which KRITIS operators are regulated (the most important for supplying the population) depends on their size and is laid down in the KRITIS Regulation (BSI Kritis V). Around 3,000 undertakings are currently qualified as critical infrastructure entities in Germany.

The upcoming transposition of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) into national law will further tighten the material obligations of cybersecurity. Above all, the group of addressees will be considerably expanded (from 3,000 to around 30,000 entities). According to the first draft for the new law (the draft NIS2 Implementation and Cybersecurity Strengthening Act), this will also be implemented in the BSI Act. It is open at the moment until when NIS2-Directive will be transposed into national law due to the current political challenges and the still ongoing formation of a government after the early elections in February 2025. The new government should move quickly to implement this, as infringement proceedings are already pending.

Additionally, specific cybersecurity rules for specific sectors apply for telecommunication and telemedia undertakings, for energy undertakings in general and specifically for nuclear energy, for public health institutions, as well as for insurance, finance and banking. The requirements for all of these areas are enshrined in national law as part of sector-specific regulation.

Law stated - 1 April 2025

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The economic sectors most affected by cybersecurity laws and regulations in Germany belong to critical infrastructures. These are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences. According to the BSI Act, critical infrastructures appear in the following sectors: energy, health, IT and telecommunications, transport and traffic, water, finance and insurance, food and municipal waste disposal.

Law stated - 1 April 2025

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

The technical regulations, in particular DIN ISO 27001, have not been incorporated into law, but are a central benchmark for interpreting and enforcing the legal requirements. An important standard is the IT Basic Protection (IT-Grundschutz – A systematic basis for information security), which is published by the BSI.

Law stated - 1 April 2025

Personnel and director obligations

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Under general German company law, the management must ensure that the company acts in accordance with the law and that damage to the company is averted. This general compliance obligation may also include the obligation to ensure adequate cybersecurity. However, this is currently controversial for companies other than those in the critical infrastructure sector. A payment in response to a phishing email, for example, was not considered a breach of duty giving rise to liability by the Zweibrücken Higher Regional Court in a decision from 2023. Under current German law, the management is therefore responsible and liable for only a narrow core area of cybersecurity.

However, this will be intensified and strengthened with the implementation of article 20 of the NIS2 Directive into the German BSI Act. According to the draft NIS2 Implementation and Cybersecurity Strengthening Act, the obligation to approve and monitor risk management measures relating to cybersecurity is imposed on the management (section 38 of the draft Act). Training courses will become mandatory.

An earlier draft even stipulated that these duties may not be delegated. While this provision has been now been removed, the draft law still states that management remains ultimately responsible in all circumstances. This will remain the case in view of EU obligations.

Law stated - 1 April 2025

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

There is no exact definition for 'cybersecurity' but one for 'security in information technology'. It means 'compliance with certain security standards for the availability,

integrity, or confidentiality of information, by means of security precautions' either in IT systems or for the use of IT systems (section 2 II of the BSI Act). However, because the Cybersecurity Act (Regulation (EU) 2019/881 (the Act)) is a regulation that applies to the member states without any implementing act, its definition also applies in German law. The Act defines 'cybersecurity' as 'activities necessary to protect network and information systems, the users of such systems and other persons affected by cyberthreats'.

There is no definition of 'cybercrime' in German law. The Federal Ministry of the Interior and Community defines it as crimes in which the perpetrators use modern information technology and crimes that target computer systems and networks themselves.

Data privacy must be separated from this. Data privacy is regulated in Germany by the Federal Data Protection Act and by the General Data Protection Regulation (EU) 2016/679 (GDPR) and includes the requirements for the processing of personal data. Section 22 of the Federal Data Protection Act covers specific obligations of data security when processing special categories of data that are sensitive. This overlaps with cybersecurity.

Law stated - 1 April 2025

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The Federal Data Protection Act and the GDPR set rules for data protection including specific measures to protect data and IT systems from cyberthreats. The controller and the processor are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures could be the pseudonymisation and encryption of data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services or to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. The regulation also mentions a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32 of the GDPR). In the case of processing special categories of personal data, the controller has to implement suitable measures to safeguard the data subject's legitimate interests. Such measures could be i) technical organisational measures to ensure a GDPR-compliant data processing, and ii) measures to ensure that it is possible to subsequently verify and establish whether and by whom personal data have been entered, modified or removed and ensuring the capability, confidentiality, integrity, availability and resilience of systems and services relating to the processing of personal data, including the ability to restore availability and access quickly in the event of a physical or technical incident (section 22 of the Federal Data Protection Act). However, those regulations do not specify any concrete measures, but requires risk-appropriate measures.

The BSI Act obliges critical entities to take appropriate organisational and technical precautions to prevent disruptions to the availability, integrity, authenticity and confidentiality of their IT systems, components or processes that are essential for the functionality of the critical infrastructures they operate (section 8a of the BSI Act).

This also includes the use of attack detection systems. The draft amendments to the BSI Act implementing the NIS2 Directive (draft NIS2 Implementation and Cybersecurity Strenghtening Act) sets a minimum level for the necessary measures, which have to include, for example, policies on risk analysis, incident handling, business continuity and supply chain security (section 30 of the draft Act).

In practice, the technical regulations of the BSI are particularly important for concrete specifications. The IT-Grundschutz – A systematic basis for information security is not a law, but it does reflect the state of the art. It contains very specific guidelines on when, for example, two-factor authentication *must* be used and when it *should* be used. The document comprises many hundreds of pages and addresses the most diverse concerns in its technical guidelines. Authorities and courts use it as a guide, as do partners in contract negotiations.

Another typical and practical useful standard for SMEs is VdS 10000.

Law stated - 1 April 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Protection regulations for intellectual property can be found, for example, in the Trade Secrets Protection Act, in trademark and patent law, or in copyright law. The Trade Secrets Protection Act prohibits the unauthorised acquisition of trade secrets. As this can also happen through a cyberattack, there is an initial parallel to cybersecurity here, even if this is not explicitly mentioned (section 23 of the Trade Secrets Protection Act).

Law stated - 1 April 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The BSI Act specifically addresses cyberthreats to critical infrastructures. Operators of critical infrastructures must take technical and organisational security measures to prevent disruptions to the IT systems used (section 8a of the BSI Act). The BSI Act is substantiated by the KRITIS Regulation, which defines when a company is considered a critical infrastructure operator and is therefore subject to these obligations. Sector-specific standards developed by operators of critical infrastructures also help with the implementation of appropriate IT security measures. Such sector-specific rules can be found for telecommunication and telemedia undertakings, for energy undertakings in general and specifically for nuclear energy, for public health institutions, as well as for insurance, and finance and banking.

Section 206 of the German Criminal Code, which sanctions the violation of postal and telecommunications secrecy, is also worth mentioning. One company that is subject to telecommunications secrecy is Deutsche Telekom, which is also a KRITIS operator. This law protects information that is subject to telecommunications secrecy and is passed on without authorisation.

Law stated - 1 April 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

If information about cyberthreats is personal, the protection framework of the EU GDPR applies. Disclosure (ie, processing) of personal data is only permitted on the basis of an authorisation, for example, to fulfil a legal obligation or due to predominant interests worthy of protection.

The German Criminal Code also prohibits the unauthorised disclosure of information via telecommunications (section 206). However, justification can certainly be considered when ensuring cybersecurity or protecting personal data. Metadata can also be helpful in preventing and combating cyberthreats. In the case of metadata on geodata, for example, this can be obtained via the Geodata Access Act (section 7).

There is no general ban on sharing information about cyberattacks.

Law stated - 1 April 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

Section 202a et seq of the German Criminal Code criminalises the unauthorised access, procurement and disclosure of stored data, as well as the preparation required for this. Unauthorised disclosure to third parties is also punishable under the Federal Data Protection Act (section 42). No specific cyber activities are listed in the law. However, according to the BSI's status report (BSI Lagebericht 2024), the most common cybersecurity incidents at companies are attacks by ransomware or ransomware as a service.

Cyberattacks also often lead to criminal offences of extortion (section 253 of the Criminal Code) and fraud, including computer fraud (sections 263 and 263a of the Criminal Code) or damage to property (section 303).

There are centralised cybercrime contact points at police stations and with the criminal prosecution authorities.

Law stated - 1 April 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

National law implementing the obligations of the NIS2 Directive also apply to cloud computing services belonging to the digital infrastructure sector with high criticality (Annex I). The draft implementation law states that the risk management measures will primarily be defined by an implementing act of the Commission.

In its publication 'Secure use of cloud services – step by step from the strategy to the end of the contract', the BSI provides information on secure cloud use in companies. There is also a Cloud Computing Compliance Criteria Catalogue with minimum requirements for secure cloud computing. The BSI Basic Protection Compendium (IT-Grundschutz) also sets out requirements for the secure use of cloud services. With regard to applications in the healthcare sector, there is the technical guideline TR-03161 that refers to the above-mentioned BSI criteria catalogue for the security of cloud computing. The German Social Code now stipulatesC5 testing for the use of cloud solutions in the area of statutory health insurance (section 393 of the Code).

When it comes to B2C contracts, warranty law must also be observed. If there are no system updates to ensure IT security, this can be considered a product defect in a cloud application (sections 327f and 475b of the Civil Code) and lead to warranty claims by the consumer.

The Data Act (EU) 2023/2854 sets out, among other things, interoperability requirements for data processing services. A data processing service can also be a cloud computing service, which means that the provisions of article 35 of the Data Act can also be applicable in the context of cloud computing. The Data Act first requires that data processing services are interoperable (ie, that users can easily switch between different services of the same type and exchange data). The security and integrity of data processing services and data must not be compromised in the process.

Law stated - 1 April 2025

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The impact of cybersecurity laws on foreign organisations depends on the territorial scope of the regulations and directives. As a federal law, the BSI Act is applicable to operators of critical infrastructures within Germany. Foreign companies are affected if they operate a critical infrastructure in Germany.

The issue has recently become relevant with warnings from the BSI about certain applications, specifically Kapersky due to espionage concerns. There are more

far-reaching powers here because state security considerations can also be used as justification.

Law stated - 1 April 2025

BEST PRACTICE

Recommended additional protections

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As the responsible authority for information technology security, the Federal Office for Information Security (BSI) publishes various recommendations and tips for companies in general on its website, but also differentiated according to company size or sector. The recommendations range from basic measures such as updates, secure passwords and virus protection to measures specifically aimed at certain attacks or threats. The BSI also publishes technical guidelines on different cybersecurity aspects online. These guidelines shall spread appropriate IT-security standards. At the centre is a document called IT-Grundschutz – A systematic basis for information security, which reflects the state of the art in cybersecurity. It contains very specific guidelines on when, for example, two-factor authentication *must* be used and when it *should* be used. These recommendations do not necessarily go beyond what is legally required. It is also often said that the legal obligations are thereby implemented.

Law stated - 1 April 2025

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

There are calls, information events and the like, but there is no specific monetary benefit. The budget for the BSI's public relations work is currently being continuously increased (albeit still limited).

Law stated - 1 April 2025

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The most important industry standard is the IT-Grundschutz, which reflects the state of the art in cybersecurity and is published by the BSI. This is the standard work for checking whether a company's IT security is sufficient and appropriate. The BSI publishes many

checklists and compendiums for this purpose, from which the appropriate one can be selected on the BSI homepage.

Another very common standard is DIN ISO 27001, which provides general support in setting up cybersecurity management in organisations. If an organisation meets the standards and they are audited, the company can be certified under them. This is a widely recognised certificate. In addition, there are industry-specific standards that take into account the relevant particularities. For SMEs, the VdS10000 guideline, which provides assistance in setting up an information security management system, is particularly important. The BSI ISO 27001 standard can be accessed here and the VdS 10000 standard can be purchased here.

The standard data protection model is developed by the German supervisory authorities and sets standards for the protection of personal data.

Law stated - 1 April 2025

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

In Germany, different recommendations and guidelines exist. Helpful for data protection issues are those published by the data protection supervisory authorities on their websites (eg, for the whole country or for Niedersachsen). The BSI publishes numerous recommendations on its website on how to handle and react after attacks (eg, with the BSI Standard 100-4 for emergency handling).

Law stated - 1 April 2025

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

According to the draft amendments to the BSI Act implementing the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (draft NIS2 Implementation and Cybersecurity Strengthening Act), companies will be able to exchange information on cyberthreats via an online portal operated by the BSI (section 6 of the draft Act). An option for voluntary reporting of security incidents is also to be introduced (section 5 of the draft Act).

Law stated - 1 April 2025

Public-private cooperation

18

How do the government and private sector cooperate to develop cybersecurity standards and procedures?

At national level, government and private sector cooperate within the German CERT-Group (the Computer Emergency Response Team for Germany's federal authorities) and the Alliance for Cyber Security.

Law stated - 1 April 2025

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Yes, insurance policies are available in Germany from different providers. While the conditions vary, requirements have been increasing for some time. Insurance is only available on commercially reasonable terms if the company can guarantee sufficient cybersecurity. If cybersecurity insurance is in place, the insurance company usually must be involved at a very early stage in the event of an attack.

Law stated - 1 April 2025

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

At national level, the Federal Office for Information Security (BSI) checks compliance with the IT security requirements (section 8a of the BSI Act) and is the responsible authority in general. In the event of non-compliance with the obligations, the BSI can issue orders and enforce them in accordance with the general rules of the Administrative Procedure Act. According to the draft amendments to the BSI Act implementation Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)(draft NIS2 Implementation and Cybersecurity Strengthening Act) the BSI will have more specific supervisory and enforcement powers on compliance with IT security obligations (sections 62, 64 and 65). There are special competences for the sectors, in particular the Federal Network Agency for telecommunications and energy (Bundesnetzagentur - BNetzA).

The requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR) are enforced by the national data protection supervisory authorities (article 57 of the GDPR). In the case of cybercrime, the national law enforcement authorities take action.

Law stated - 1 April 2025

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The data protection supervisory authorities may request the controller to provide relevant information, carry out data protection checks or request access to data to monitor the GDPR obligations (article 58).

The BSI can check compliance with IT security requirements by operators of critical infrastructures. The BSI may request documents and information that are necessary for the inspection (section 8a (IV) of the BSI Act). According to the draft NIS2 Implementation and Cybersecurity Strengthening Act, this monitoring authorisation does not change under the implementation act. It no longer extends only to operators of critical facilities, but also to particularly important and important facilities (section 64 and 65 of the raft Act).

Law stated - 1 April 2025

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

To date, the requirements of the BSI Act have been enforced by the BSI using administrative measures in accordance with the general rules. Changes are expected following the extensive amendments to the BSI Act to implement the NIS2 Directive . The BSI will be given further-reaching powers so its remit includes more types of entities than at present. Public warnings about applications, etc, with security vulnerabilities are also a form of enforcement. Under German administrative law, these may be issued only under strict conditions due to the significant consequences.

The independent national data protection supervisory authorities enforce the data protection requirements. The most important instruments are requests for information, orders and fines.

Law stated - 1 April 2025

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Operators of critical infrastructures are obliged to report disruptions or significant disruptions to their information technology systems, components or processes that could lead to a failure or significant impairment of the functionality of the critical infrastructure (section 8b(4) of the BSI Act).

The draft NIS2 Implementation and Cybersecurity Strengthening Act, extends the reporting obligation to particularly important ('essential') and important entities in addition to operators of critical infrastructures. A tiered system will apply in accordance with the NIS2 Directive:

- an early warning must be issued immediately, but at the latest after 24 hours;
- a security incident must be reported immediately and no later than 72 hours after becoming aware of it; and
- a final report must be submitted no later than one month after the incident (section 32(1) of the Draft NIS2 Implementation Act).

In the event of a significant security incident, the BSI may instruct the company to notify its customers (section 35(1) of the DraftNIS2 Implementation Act).

In the case of data breaches, the controller must report these to the competent national supervisory authority immediately or within 72 hours (article 33 of the GDPR). This does not apply if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The data subject must be notified under the conditions of article 34 of the GDPR.

Law stated - 1 April 2025

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Violations of the provisions of the BSI Act can result in fines of between €100,000 and €2 million in accordance with section 14 of the BSI Act. For example, if operators of critical infrastructures do not take appropriate technical and organisational precautions to prevent IT disruptions, contrary to section 8a(1) of the BSI Act, this is an administrative offence that can be sanctioned with a fine of up to €1 million.

The sanctions will be adapted to the NIS2 Directive with the Implementation Act. Any particularly important organisation that fails to take risk management measures or does not take sufficient risk management measures is committing an offence and is liable to a fine of up to €10 million or 2 per cent of its global annual turnover (section 60(2) No. 2(7) of the BSI Act). The sanctions will be lower for important entities.

The Federal Data Protection Act contains sanction regulations for data protection violations in section 41 et seq. If, for example, the security requirements of article 32 of the GDPR are disregarded, a fine of up to €10 million or (as a company) up to 2 per cent of the annual turnover achieved worldwide must be paid.

Law stated - 1 April 2025

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Violations of the provisions of the BSI Act can result in fines of between €100,000 and €2 million in accordance with section 14 of the BSI Act. For example, if operators of critical infrastructures do not report a malfunction at all or not in time, contrary to section 8b(4) of the BSI Act, this can be sanctioned with up to €500,000.

The sanctions will be adapted to the NIS2 Directive with the Implementation Act. Any particularly important organisation that does not report a malfunction at all or not in time contrary to section 8b(4) of the BSI Act is liable to a fine of up to €10 million or 2 per cent of its global annual turnover (section 60(2) No. 3(7) of the draft NIS2 Implementation and Cybersecurity Strengthening Act). The sanctions will be lower for important entities.

The Federal Data Protection Act contains sanction regulations for data protection violations in section 41 et seq and refers to article 83 of the GDPR. If, for example, the controller fails to report a personal data breach to the supervisory authority (article 33 of the GDPR), he or she has to pay a fine of up to €10 million or (as a company) up to 2 per cent of the annual turnover achieved worldwide (article 83(4) of the GDPR).

Law stated - 1 April 2025

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Affected persons can sue for damages or injunctive relief under national law. Collective actions are authorised for individual cases, in particular for injunctions, but not for individual claims for damages. The requirements for a claim for damages following a hacking attack were recently specified at EU level by the European Court of Justice in Case C-340/21, where it was stated in the case of a claim for damages under article 82 of the GDPR that fault is presumed and the controller can exculpate itself only if it demonstrates that it has taken all necessary measures to ensure adequate security. There is a debate as to whether this now generally applies to claims for damages following cybersecurity incidents. The argument against this is that general German civil law does not recognise such a presumption of fault as article 82 of the GDPR.

Law stated - 1 April 2025

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

An appropriate risk management system must be in place, including an emergency plan. Currently, this is only an explicit legal obligation for critical entity operators. With the implementation of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the European Union (NIS2 Directive) into national law, this will also

become mandatory for important and essential entities. It is not yet clear when NIS2 Directive will be transposed into national law. The implementation deadline of the directive expired on 17 October 2024. Germany missed this deadline. The EU Commission has therefore already initiated infringement proceedings. Due to the current political challenges and the still ongoing formation of a government after the early elections, it is still unclear until when the transposition will be complete. The new government should move quickly to implement this, as infringement proceedings are already pending.

Law stated - 1 April 2025

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

National IT security law does not contain any explicit requirements in this regard. The requirements result from the possible claims. Due to claims for damages and official investigations, the documents must be kept in an audit-proof form until any claims for compensation become time-barred. It is important that they are suitable as evidence in court.

Law stated - 1 April 2025

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Operators of critical infrastructures are obliged to report disruptions or significant disruptions to their IT systems, components or processes that could lead to a failure or significant impairment of the functionality of the critical infrastructure (section 8b(4) Federal Office for Information Security Act (BSI Act). The companies must provide information on the disruption, possible cross-border effects and technical framework conditions.

In the new BSI Act (the NIS2 Implementation and Cybersecurity Strengthening Act), the reporting obligation will be extended to particularly important and important entities in addition to operators of critical infrastructures. The organisations must first issue an early warning in which the suspicion of an unlawful or malicious act or cross-border effects is stated. This is followed by a report on the incident with an initial assessment of its severity and impact. Lastly, a final report must be submitted describing the security incident in detail (section 32(1) of the draft NIS2 Implementation and Cybersecurity Strengthening Act).

In the event of a cyberthreat, only organisations from certain sectors are obliged to inform their customers of this threat. Customers and the BSI must be informed of possible measures that customers can take to avert the security incident. However, this obligation applies only if the interests of the customers outweigh those of the organisation when weighing up the interests (section 35(2) of the draft Act).

In addition, security incidents, cyberthreats and near-incidents can also be reported voluntarily to the BSI (section 5(2) of the draft Act).

The GDPR applies to security incidents that result in a personal data breach. According to article 33 of the GDPR, personal data breaches must be reported to the supervisory authority. This obligation does not apply if the data breach is not likely to result in a risk to the rights and freedoms of natural persons. The type of breach, contact details of the data protection officer, a description of the likely consequences of the breach and the measures that have to be taken must be reported.

Law stated - 1 April 2025

Time frames

30 | What is the timeline for reporting to the authorities?

According to the draft act implementing the NIS2 Directive, EU member states have to ensure that essential and important organisations are obliged to report significant security incidents to the national competent authority (section 32(1)). If necessary, they also inform the recipients of their services. A tiered reporting system applies: an early warning must be issued immediately, but at the latest after 24 hours; a security incident must be reported immediately and no later than 72 hours after becoming aware of it; and a final report must be submitted no later than one month after the incident.

In the event of a cyberthreat, only organisations from certain sectors are obliged to inform their customers of this threat. Customers and the BSI must be informed without undue delay of possible measures that customers can take to avert the security incident (section 35(2) of the draft Act).

In the event of a personal data breach, the notification to the supervisory authority must be made without undue delay and, where feasible, within 72 hours of the controller becoming aware of the breach (article 33(1) of the GDPR). Any delay must be justified.

Law stated - 1 April 2025

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

According to the draft NIS2 Implementation and Cybersecurity Strenghtening Act, the BSI can oblige particularly important and important entities to inform their customers of a significant cyber incident (section 35(1)t).

In the event of a personal data breach, the data subject must be informed if there is likely to be a high risk to the personal rights and freedoms of natural persons. This does not apply if the controller has taken sufficient security measures or has ensured that the risk to the

rights and freedoms of the data subject no longer exists. Notification is also not required if it involves a disproportionate effort (article 34 of the GDPR).

Law stated - 1 April 2025

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

At a national level in Germany, we currently see a high threat level, which was clearly identified in the Federal Office for Information Security (BSI) Situation Report 2024 (- BSI Lagebericht 2024). At the same time, countless new EU regulations need to be implemented and enforced. The BSI is increasingly positioning itself as an adviser and therefore publishes recommendations and guidelines, speaks at events and is active in the Alliance for Cyber Security, among other things.

Law stated - 1 April 2025

LOSCHELDER

Kristina Schreiber kristina.schreiber@loschelder.de
Dennis Pethke dennis.pethke@loschelder.de

Loschelder Rechtsanwälte

Greece

Dimitra Karampela
Karatzas & Partners Law Firm

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Greece, cybersecurity matters are regulated by Law No. 4961/2022, Law No. 4727/2020, Law 5160/2024, Law No. 5086/2024, Law No. 5002/2022, Regulation (EU) 2016/679, Law No. 4624/2019, Law No. 3471/2006 and ministerial decisions No. 1027/2019 and No. 1381/2025. The Greek cybersecurity laws, currently in force, strengthen security requirements, address supply chain security, streamline reporting obligations and introduce more stringent supervisory measures and enforcement requirements; notably, they also introduce personal liability for members of the management of entities within the scope of the law.

Law stated - 20 March 2025

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Law No. 5160/2024, which incorporates Directive 2022/2555 (the NIS 2 Directive) into Greek legislation and establishes cybersecurity measures and obligations, affects both public and private sector entities established or operating in Greece that provide their services or carry out activities in critical and highly critical sectors. In particular, entities doing business in energy, health, transport and banking sectors as well as in the food production or distribution and digital infrastructure (eg, cloud computing service providers and data centres) are the most affected by cybersecurity laws in Greece, especially in connection with the security measures to be taken to ensure compliance with the legislation.

Law stated - 20 March 2025

International standards

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Greece has established a new National Cybersecurity Authority to enhance its defences against cyberthreats and meet EU regulatory requirements. Greece follows European standards and methodologies for the development of the current strategic cybersecurity planning. Within the context of the evaluation of this strategic framework, the National Cybersecurity Authority (NCSA) has utilised the application of an evaluation tool, created by the European Union Agency for Cybersecurty (ENISA), which includes several objectives for evaluating national cybersecurity strategies. Furthermore, Greece

participates in NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), which supports its member nations (including Greece) and NATO with unique interdisciplinary expertise in the field of cyber defence research, training and exercises covering the focus areas of technology, strategy, operations and law.

Law stated - 20 March 2025

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Responsible personnel and directors should approve the cybersecurity risk-management measures and oversee the implementation of said measures, and they are liable for infringements of the relevant obligations (article 14 of Law 5160/2024). The NCSA may temporarily restrict the directors of an entity from performing their managing duties if the entity does not comply with the cybersecurity measures imposed on it by the NCSA (article 24 of Law 5160/2024).

Law stated - 20 March 2025

Key definitions

5 How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

In Greece, the term 'cybersecurity' has the meaning provided by Regulation (EU) 2019/881, that is, cybersecurity means the activities necessary to protect network and information systems, the users of these systems and other persons affected by cyberthreats. There is no specific meaning for the term 'cybercrime'. Cyberthreat also has the meaning provided by EU Regulation 2019/881, that is, any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of these systems and other persons.

Law stated - 20 March 2025

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

According to Greek cybersecurity legislation, essential and significant entities must take appropriate and proportional technical, operational and organisational measures to manage risks concerning the security of network and information systems they use for their activities or to provide their services and prevent or minimise the impact of incidents on their service recipients or other services and organisations. The measures are based

on a holistic risk approach aimed at protecting network and information systems and the physical environment of these systems from incidents and include, at least, the following:

- policies and procedures for risk analysis and information system security;
- incident management procedures;
- business continuity, such as backup management and disaster recovery, as well as crisis management;
- supply chain security, including security aspects related to the relationships between each entity and its direct suppliers or service providers;
- security in the acquisition, development and maintenance of network and information systems, including the handling and disclosure of vulnerabilities;
- policies and procedures for assessing the effectiveness of risk management measures in the field of cybersecurity;
- basic cyber hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where applicable, encryption in collaboration with the national authority;
- human resource security, access control policies and asset management; and
- use of multi-factor authentication solutions or continuous identity verification, secure voice communications, video and text communications and secure emergency communication systems within the entity.

Law stated - 20 March 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Greek copyright law (Law No. 2121/1993) has been amended to incorporate several EU directives that address digital copyright issues. For example, the implementation of Directive 2001/29/EC (the InfoSoc Directive) and Regulation (EU) 2019/790 (the Digital Single Market Directive) has strengthened the legal framework for protecting copyright in the digital environment. These amendments ensure that Greek law is aligned with EU standards in addressing cyberthreats. According to the Greek copyright legislation, it is prohibited, without the permission of the rights holder, to neutralise effective technological measures. 'Technological measure' can refer to any technology, mechanism or component that, in its usual mode of operation, aims to prevent or restrict actions, in relation to works or other protected objects, that have not been authorised by the copyright or related rights holder, including the special right of the database manufacturer. Technological measures are considered effective when the use of the protected work or other protected object is controlled by the rights holders through the application of access control or protection processes, such as encryption, transmission disruption or other transformation of the work or other protected object or protective copy control mechanism, which achieves the goal

of protection. If someone neutralises a technological measure on purpose, they may be punished by imprisonment of at least one year and a monetary fine.

Law stated - 20 March 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

In Greece, Regulation (EU) 2022/2554 (the Digital Operational Resilience Act) applies to financial entities such as banks, insurance companies and investment firms, aiming to strengthen their information technology security. Furthermore, in the energy sector, the Regulatory Authority for Energy has issued a risk preparedness plan (based on Regulation (EU) 2019/941) including provisions regarding cybersecurity threats.

Law stated - 20 March 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There are specific occasions in which sharing of cyberthreat information is restricted. In particular, under Law No. 5160/2024, no information must be disclosed in the context of the cybersecurity obligations whose disclosure would be contrary to essential national security interests, public order or the defence of the country. Furthermore, the exchange of information should consider the potentially sensitive nature of the information being shared as well as any restrictions under the data protection legislation.

Law stated - 20 March 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The Greek Penal Code provides penalties for cybercrimes. Activities such as hacking or phishing are considered criminal offences. Specifically, according to article 370B, electronic intrusion, that is, unauthorised access to information systems or electronic data (hacking), is punishable by imprisonment. Additionally, according to article 292 of the Greek Penal Code, piracy is a criminal offence punishable by one to five years, depending on the severity of the outcome. This applies if it causes serious obstacles to the operation of an information system or when the data has been modified or deleted as a result of the intrusion. Also, according to the Greek Penal Code (article 361), anyone who, except in cases of slanderous defamation (article 363), insults the honour of another by speech or

by deed or in any other way, with such a purpose, will be punished by imprisonment of up to six months or a fine. If a person commits the above act in public, including on the Internet, the person is liable to imprisonment for up to one year or a fine, and if the offence relates to relationships of private or family life, the person is liable to imprisonment for up to two years or a fine.

Law stated - 20 March 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Greece has implemented several measures to address challenges associated with cloud computing, mostly in relation to cybersecurity and data protection. Providers of cloud computing services fall, in principle, under Greek Law No. 5160/2024 (implementing the NIS 2 Directive) and therefore must comply with a wide set of cybersecurity obligations. Additionally, any processing of personal data that is involved in cloud computing must comply with the requirements of Regulation (EU) 2016/679 (GDPR) and Greek Law No. 4624/2019. Furthermore, we note that the Hellenic Data Protection Authority has participated in the coordinated enforcement action of the European Data Protection Board on the use of cloud-based services by the public sector.

Law stated - 20 March 2025

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

In Greece, cybersecurity legislation applies to organisations that are established in or provide their services or perform their activities within the Greek territory. The regulatory obligations are the same for local and foreign organisations doing business in Greece.

Law stated - 20 March 2025

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In Greece, the authorities do indeed recommend additional cybersecurity protections beyond what is mandated by law. The National Cybersecurity Strategy 2020-2025 outlines a comprehensive framework that includes not only compliance with legal requirements

but also the adoption of best practices and advanced measures to enhance cybersecurity. Furthermore, the incorporation of the NIS 2 Directive into Greek law emphasises the need for entities to adopt appropriate and proportional technical, operational and organisational measures to manage cybersecurity risks, taking into account the latest national, European and international standards. The strategy also encourages public–private partnerships (PPPs) and the use of innovative tools and techniques to strengthen cybersecurity resilience.

Law stated - 20 March 2025

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

The National Cybersecurity Strategy 2020-2025 of Greece sets incentives for organisations to implement organisational, technical and other measures to strengthen their cybersecurity profile and contribute to the successful response to incidents. For the effective financing of these interventions, the creation of an incentive toolkit in cooperation with competent bodies on a case-by-case basis is preferred, with the aim of motivating companies to invest in cybersecurity measures. This toolkit may include fiscal and financial incentives, such as reduced taxation, subsidy, etc. Furthermore, the development and utilisation of innovative financing mechanisms as well as mechanisms for optimisation, acceleration and simplification of procedures for the financing of cybersecurity actions, will make a key contribution to the fight against bureaucracy and the more efficient allocation of resources for the benefit of organisations.

Law stated - 20 March 2025

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In Greece, the NCSA formulates the National Cybersecurity Strategy, which provides for strategic objectives, the resources required to achieve them and the appropriate policy and regulatory measures, with the aim of establishing and maintaining a high standard of cybersecurity. The latest National Cybersecurity Strategy including these standards can be accessed at the website of the Ministry of Digital Governance. Furthermore, the department for NCSA requirements and cybersecurity architecture has published the Cybersecurity Handbook, which includes best practices for the protection and resilience of network and information systems. The set of best practices are divided into 18 chapters that correspond to security control families:

- inventory of hardware and software assets;
- secure configuration of devices and applications;
- application and services execution control;

- access control;
- user authentication;
- network security;
- malware protection;
- maintenance and analysis of event logs;
- web application security;
- teleworking;
- use of cryptography;
- cybersecurity skills and awareness training;
- supply chain risk management;
- cybersecurity technical assessments;
- physical security measures;
- data backups;
- incident handling; and
- business continuity and disaster recovery.

The Cybersecurity Handbook can be accessed at the website of the Ministry of Digital Governance.

Law stated - 20 March 2025

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

Yes, the recommended best practices for cybersecurity incident handling are included in the Cybersecurity Handbook, published by the NCSA department for requirements and cybersecurity architecture. Best practices refer to procedures for handling cybersecurity incidents to effectively protect the confidentiality, integrity and availability of network and information systems.

Law stated - 20 March 2025

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The NCSA, as part of its strategic planning evaluation, considers as one of its strategic priorities the sharing of information about cyberthreats. According to the current legislative framework in cybersecurity in Greece, legal entities may voluntarily exchange information

related to cybersecurity, including information about cyberthreats, incidents, vulnerabilities, techniques and procedures, indications of breach, malicious tactics, information about specific threat actors, cybersecurity warnings and recommendations on configuring cybersecurity tools to detect cyberattacks, to the extent that such information exchange aims to prevent, detect, respond to, or recover from incidents or mitigate their impacts, and enhances the level of cybersecurity, particularly through awareness of cyberthreats, limiting or preventing the ability to spread such threats, supporting a range of defensive capabilities, restoring and disclosing vulnerabilities, detecting threats, mitigation and prevention techniques, mitigation strategies or response and recovery stages and promoting collaborative research on cyberthreats between public and private entities. According to the legislation, key and significant entities promptly notify the NCSA of their participation in the information exchange framework as well as their withdrawal from participation, as soon as it occurs. Also, notifications can be submitted to the NCSA on a voluntary basis by key and significant entities regarding incidents, cyberthreats and near incidents. The NCSA ensures the confidentiality and appropriate protection of the information provided by the reporting entity.

Law stated - 20 March 2025

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Coordinating with government agencies regarding early self-reporting, remediation efforts and active collaboration may enable private sector companies to avoid prosecution and penalties for cybersecurity incidents. In Greece, the government and private sector cooperate to develop cybersecurity standards and procedures through a PPP framework. The NCSA plays a central role in this collaboration by defining requirements for cybersecurity service providers and establishing a registry of accredited private entities that meet specific conditions. These entities provide specialised services such as security consulting, technical inspections and threat intelligence. The NCSA also promotes networking and cooperation with academic and research institutions to foster innovation in cybersecurity. This collaborative approach ensures a harmonised and effective cybersecurity strategy that leverages both public oversight and private sector expertise.

Law stated - 20 March 2025

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Insurance for cybersecurity risks is available in Greece. Although an increasing number of organisations are affected by cybersecurity risks and are therefore interested in cyber insurance, there is no official data in relation to how common it is for organisations to obtain

such insurance. We note that some cyber insurance options address entities with specific criteria, for example, exclusively small and medium-sized enterprises with annual turnover of less than €2.5 million.

Law stated - 20 March 2025

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The NCSA, supervised by the Ministry of Digital Governance, is primarily responsible for enforcing cybersecurity rules.

Law stated - 20 March 2025

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The NCSA is the competent authority for supervision and monitoring of compliance with cybersecurity laws. Its designated employees have audit responsibilities and the authority, in particular to:

- visit, in the context of performing their duties and fulfilling their tasks, with or without prior notice, the entities that fall within the scope of cybersecurity requirements;
- inspect and collect information and data from mobile terminals, portable devices, servers and the cloud, in cooperation with the competent authorities, whether located inside or outside the premises of the entities;
- conduct searches in the offices and other premises of the entities;
- carry out seizures, take or obtain in any form a copy or extract of books, documents, as well as electronic storage and data transfer media, which relate to professional information and, when deemed appropriate, to continue the information search and select copies or extracts at the premises of the NCSA or other designated locations; and
- seal any professional space, electronic or non-electronic books or documents during the period of the audit and to the extent necessary for it.

Law stated - 20 March 2025

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

One of the most common enforcement issues is related to the fragmentation and complexity of structures and procedures related to cybersecurity, often leading to coordination challenges among various stakeholders, including public and private entities. The National Cybersecurity Strategy 2020-2025 highlights the need for clear roles, responsibilities and streamlined procedures to address this issue. Furthermore, financial constraints and complex procurement and service procedures are also common enforcement issues. These constraints can hinder the timely implementation of necessary cybersecurity measures and the acquisition of advanced technologies and services required to combat cyberthreats effectively. In addition to the above, rapid technological developments require continuous updates to cybersecurity measures, while resources and staffing within the regulatory bodies remain limited.

Law stated - 20 March 2025

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Businesses must immediately notify the recipients of their services who may be affected by a significant cyberthreat of measures or corrective actions that they can take to address the specific threat. They must report, among other things, any information that allows the NCSA to identify cross-border impacts of the incident. The mere act of notification does not imply liability on the part of the notifying entity. An incident is considered significant if:

- it has caused or may cause serious operational disruption of services or financial damage to the relevant entity; and
- it has affected or may affect other natural or legal persons causing significant material or non-material damage.

Businesses must report to the NCSA:

- without undue delay and in any case within 24 hours from the moment they became aware of the significant incident, a warning, which, where appropriate, indicates whether there is a suspicion that the significant incident was caused by illegal or malicious actions or could have a cross-border impact;
- without undue delay and in any case within 72 hours from the moment they became aware of the significant incident, an incident notification, which, where appropriate, updates the information referred to in the first point and, in addition, includes an initial assessment of the significant incident, including its severity and impact, as well as, if available, indications of the breach;
- upon request of the NCSA, an interim report on the relevant updates of the situation;
- a final report no later than one month after the submission of the incident notification, which includes:

- a detailed description of the incident, including its severity and impact;
- the type of threat or the root cause that may have caused the incident;
- applied and ongoing mitigation measures; and
- where appropriate, the cross-border impact of the incident.

Where appropriate, and especially when the significant incident concerns other member states of the European Union, the computer security incident response team of the NCSA must immediately inform the other affected member states and ENISA about the significant incident.

Law stated - 20 March 2025

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The supervisory or enforcement measures imposed on key or significant entities in relation to cybersecurity legislation must be effective, proportionate and dissuasive, taking into account the circumstances of each individual case. If a violation of articles 15 or 16 of Law No. 5160/2024 regarding security measures is found, a fine of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the business to which the significant entity belongs, whichever is higher, may be imposed on the key entities. As regards significant entities, if a violation of articles 15 or 16 of Law No. 5160/2024 is found, a fine of up to €7 million or up to 1.4 per cent of the total worldwide annual turnover of the business to which the significant entity belongs, whichever is higher, may be imposed on the significant entities.

Law stated - 20 March 2025

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

If a violation of article 16 of Law No. 5160/2024 regarding security measures is found, a fine of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the business to which the significant entity belongs, whichever is higher, may be imposed on the key entities. As regards significant entities, if a violation of article 16 of Law No. 5160/2024 is found, a fine of up to €7 million or up to 1.4 per cent of the total worldwide annual turnover of the business to which the significant entity belongs, whichever is higher, may be imposed on the significant entities.

Law stated - 20 March 2025

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

In cybersecurity incidents, entities may raise claims for damages based on tort law as well as compensation for damages against the attackers. Furthermore, if there is a contractual relationship and the failure to protect systems and data constitutes a breach of contract, the affected party can seek remedies under contract law. This may include specific performance, termination of the contract and damages.

Law stated - 20 March 2025

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Key and significant entities take appropriate and proportionate technical, operational and organisational measures to manage risks concerning the security of network and information systems they use for their activities or to provide their services, and to prevent or minimise the impact of incidents on their service recipients or other services and organisations. Taking into account the latest and, where applicable, relevant national, European and international standards, as well as the cost of implementation, the measures mentioned above will ensure a level of security of network and information systems proportionate to the respective risk. When assessing the proportionality of these measures, the degree of exposure of the entity to risks, the size of the entity, the likelihood of incidents occurring and their severity, including their social and economic impacts, are all taken into account. These measures are based on a holistic risk approach aiming at protecting network and information systems and the physical environment of these systems from incidents, and include at least:

- policies and procedures for risk analysis and information system security;
- incident management;
- business continuity, such as backup management and disaster recovery, as well as crisis management;
- supply chain security, including security aspects related to the relationships between each entity and its direct suppliers or service providers;
- security in the acquisition, development and maintenance of network and information systems, including the handling and disclosure of vulnerabilities;
- policies and procedures for assessing the effectiveness of risk management measures in the field of cybersecurity;
- basic cyber hygiene practices and cybersecurity training;

- policies and procedures regarding the use of cryptography and, where applicable, encryption, in collaboration with the national authority, where required;
- human resource security, access control policies and asset management;
- use of multi-factor authentication or continuous identity verification solutions, secure voice communications, video and text communications and secure emergency communication systems within the entity, where applicable.

Law stated - 20 March 2025

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

According to Law No. 5160/2024, in case of a cyberthreat or attack, the relevant entities should submit to the NCSA, among others, a final report no later than one month after the submission of the incident notification (which must take place not later than 72 hours after the organisation has become aware of it), which includes the following:

- a detailed description of the incident, including its severity and impact;
- the type of threat or the root cause that may have caused the incident; and
- the already applied and ongoing mitigation measures and, if applicable, the cross-border impact of the incident.

Law stated - 20 March 2025

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

According to Greek Law No. 5160/2024, key and significant entities notify, without undue delay, the computer security incident response team of the NCSA of any incident that has a significant impact on the provision of their services. Where applicable, the relevant entities notify, without undue delay, their service recipients of significant incidents that may negatively affect the provision of those services. These entities report, among other things, any information that allows the NCSA to identify cross-border impacts of the incident. The mere act of notification does not imply liability of the notifying entity. According to the legislation, an incident is considered significant if:

- it has caused or may cause serious operational disruption of services or economic damage to the relevant entity; and
- it has affected or may affect other natural or legal persons causing significant material or non-material damage.

For the notification of the incident as above, the relevant entities submit to the NCSA:

- without undue delay and in any case within 24 hours from the moment they became aware of the significant incident, a warning, which, where applicable, indicates whether there is a suspicion that the significant incident was caused by illegal or malicious actions or could have a cross-border impact; and
- without undue delay and in any case within 72 hours from the moment they became aware of the significant incident, an incident notification, which, includes an initial assessment of the significant incident, including its severity and impact, as well as, if available, indications of the breach.

The NCSA provides the notifying entity, without undue delay and if possible within 24 hours from the receipt of a response that includes an initial reaction to the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where applicable, and especially when the significant incident concerns other member states of the European Union, the computer security incident response team of the NCSA informs, without undue delay, the affected member states and ENISA about the significant incident. When public awareness is necessary to prevent a significant incident or to address a significant ongoing incident, or when the disclosure of the significant incident is in the public interest, the NCSA may, after consulting with the relevant entity, inform the public about the significant incident or require the entity to inform the public within a specified deadline.

Law stated - 20 March 2025

Time frames

30 | What is the timeline for reporting to the authorities?

Key and significant entities under Law No. 5160/2024 must proceed to a self-registration to the NCSA registry within two months from entry into force of the above legislation. This deadline has already been extended by the NCSA.

Law stated - 20 March 2025

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Key and significant entities notify, without undue delay, their service recipients, who may be affected by a significant cyberthreat, of measures or corrective actions they can take to address the specific threat. The entities also inform these recipients about the significant cyberthreat. The NCSA provides the notifying entity, without undue delay and if possible within 24 hours from the receipt of the timely warning, a response that includes an initial reaction to the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. The NCSA provides additional technical support, if requested by the relevant entity. When there are

suspicions that the significant incident is of a criminal nature, the NCSA also provides guidance on reporting the significant incident to the competent prosecutorial authorities or the competent Directorate of the Hellenic Police. Where applicable, and especially when the significant incident concerns other member states of the European Union, the computer security incident response team of the NCSA informs, without undue delay, the affected member states and ENISA about the significant incident. In this context, the NCSA safeguards, in accordance with EU and national law, the security and commercial interests of the entity, as well as the confidentiality of the provided information. When public awareness is necessary to prevent a significant incident or address a significant ongoing incident, or when the disclosure of the significant incident is in the public interest, the NCSA may, after consulting with the relevant entity, inform the public about the significant incident or require the entity to inform the public within a specified deadline.

Law stated - 20 March 2025

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The new legislation covers even more sectors and categories of businesses, including medium-sized enterprises (with 50–250 employees and having a turnover of up to €250 million), but also large enterprises in the sectors of energy, transport, health, cloud services and data centres, etc. Companies should implement stricter security measures to protect their networks and information, and should report major security incidents to competent authorities as soon as possible. This will strengthen cooperation between public and private sectors, as well as national strategic cybersecurity planning, while businesses will have to comply with the legislation and adopt risk-management measures. The rapid technological developments require continuous updates to cybersecurity laws and policies, so as to correspond to the new cyberthreats.

Law stated - 20 March 2025

Dimitra Karampela d.karampela@karatza-partners.gr

Karatzas & Partners Law Firm

Read more from this firm on Lexology

India

Sumit Ghoshal, **Aprajita Rana**, **Shagun Badhwar**, **Suyash Tiwari**
AZB & Partners

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

While India does not have a dedicated cybersecurity law, several statutes and sector-specific regulations among other things govern cybersecurity and promote the maintenance of cybersecurity standards. One of the primary pieces of legislation dealing with cybersecurity, data protection and cybercrimes is the Information Technology Act 2000 (the IT Act), read with the rules and regulations framed thereunder. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but also contains provisions that are aimed at safeguarding electronic data, information or records, and preventing unauthorised or unlawful use of a computer system. Some of the cybercrimes that are specifically envisaged and punishable under the IT Act are hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft.

In accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, the Computer Emergency Response Team (CERT-In) has been established as the nodal agency to deal with cybersecurity incidents and responding to these incidents. CERT-In is tasked with performing certain functions including collection, analysis and dissemination of information on cybers, issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, response and reporting of cybers. To perform these functions, CERT-In is empowered to call for information and issue directions to service providers, intermediaries, data centres, bodies corporate and any other person. Exercising such powers, CERT-In issued directions dated 28 April 2022 (CERT-In Directions) for strengthening cybersecurity in India. CERT-In clarified the Directions through frequently asked questions (FAQs) published on 18 May 2022.

In addition to the above, other relevant rules framed under the IT Act in the context of cybersecurity include:

- the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for the collection and processing of personal or sensitive personal data. Once the Digital Personal Data Protection Act 2023 (DPDP Act), which though notified is yet to become effective, comes into force the SPDI Rules will stand replaced. The DPDP Act stipulates that a data fiduciary is required to protect the digital personal data of an individual in its possession or under its control (including in respect of processing undertaken by it or on its behalf) by taking reasonable security safeguards to prevent personal data breach. While the draft of the Digital Personal Data Protection Rules 2025, released on 3 January 2025 for public consultation, provides clarity on minimum reasonable security safeguards that need to be implemented, this position will only be crystallised once the final rules are notified;
-

the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, which require specific information security measures to be implemented by organisations that have protected systems, as defined under the IT Act; and

- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (the Intermediaries Guidelines) require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein. The intermediaries are also required to report cybersecurity incidents (including information relating to such incidents) to CERT-In.

Other laws that contain cybersecurity-related provisions include the Bharatiya Nyaya Sanhita 2023 (BNS) (formerly referred to as the Indian Penal Code 1860), which punishes offences, including those committed in cyberspace (eg, defamation, cheating, criminal intimidation, obscenity and spreading false news), and the Companies (Management and Administration) Rules 2014 (the CAM Rules) framed under the Companies Act 2013, which require companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

In addition, there are sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India, the Department of Telecommunication (DOT) and the Securities Exchange Board of India (SEBI), which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecom service providers, and venture capital funds and stock exchange.

The proposed Digital India Act 2023 that will replace the IT Act can be expected to bring a robust and dedicated law dealing with cybersecurity.

Law stated - 5 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Regulated entities operating in sensitive sectors, such as financial services, banking, insurance and telecommunications, have exhibited higher standards of cybersecurity preparedness and awareness, partly because of regulatory intervention but also because of voluntary compliance with advanced international standards. Sectors such as e-commerce, IT and IT-enabled services that have seen an infusion of foreign direct investment have also proactively deployed robust cybersecurity frameworks and policies to counter the evolving nature of cyber fraud as they have borrowed advanced cybersecurity practices and procedures from their overseas parent entities in the United States, the European Union and other jurisdictions.

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased in numbers and become more complex. While the RBI has been active in requiring companies operating payment systems to build

secure authentication and transaction security mechanisms (eg, two-factor authentication, EMV chips, Payment Card Industry Data Security Standard (PCI-DSS) compliance and tokenisation), given that these payment companies often offer real-time frictionless payment experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyberthreats. In light of the above, there is an increased need for such entities to identify and develop cybersecurity standards commensurate with the nature of the information assets handled by them and evaluate the possible harm in the event of any cybersecurity attack to ensure that these emerging risks are mitigated.

Moreover, the covid-19 pandemic has led to increased dependencies on digital infrastructure for many organisations, as employees are being given the option of working remotely. This has led to enormous cybersecurity-related vulnerabilities and challenges for large and small organisations alike and made them rethink cybersecurity preparedness, policies and budgets.

We have already witnessed large-scale cyberattacks (eg, ransomware attacks) and disruption in sensitive sectors in India. As per the Annual Report for the year 2023-2024 released by the Ministry of Personnel, Public Grievances and Pensions Government of India, 2023 witnessed a ransomware attack on a crucial defence unit, a data breach impacting millions of Indian users, a malware attack in a ministry and a massive distributed denial-of-service attack on critical infrastructure and airports in India.

Additionally, CERT-In reported a possible intrusion and data breach at Bharat Sanchar Nigam Limited (BSNL), a popular telecom service provider that is a public sector undertaking owned by the government of India.

The demand for remote work, new technologies and vulnerabilities resulting therefrom will continue to exist and, accordingly, we expect cybersecurity standards to be given critical importance.

Law stated - 5 December 2024

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

Yes, the SPDI Rules require bodies corporate that handle sensitive personal data or information to implement 'reasonable security practices and procedures' by maintaining a comprehensively documented information security programme. This programme should include managerial, technical, operational and physical security control measures that are commensurate with the nature of the information being protected. In this context, the SPDI Rules recognise the International Standard ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements, as one such approved security standard that can be implemented by a body corporate for protection of personal information. All bodies corporate that comply with this standard are subject to audit checks by an independent government-approved auditor at least once a year or as and when they undertake a significant upgrade of their processes and computer resources.

The newly enacted, albeit yet to be notified, DPDP Act also puts an obligation on data fiduciaries to adopt reasonable security safeguards to prevent personal data breach. Unlike the SPDI Rules, the DPDP Act does not recognise any specific standards to be followed. That said, more clarity on specific security standards and safeguards to be implemented under the DPDP Act may emerge once the rules are framed and notified thereunder.

Sector-specific regulators have also prescribed security standards specifically applicable to regulated entities. For instance, the RBI guidelines mandate banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards for ensuring adequate protection of critical functions and processes. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to implement data security standards and best practices such as PCI-DSS and Payment Application Data Security Standard (PA-DSS) and implement checks to ensure that the merchants onboarded by them are compliant with such data security standards and best practices. The Master Directions on Cyber and Digital Payment Security Controls for Nonbank Payment System Operators, released by the RBI in July 2024, also mandate obtaining PCI-DSS certification and compliance with PCI-DSS guidelines for payment system operators storing card data. Similarly, SEBI requires stock exchanges, depositories, clearing corporations, etc, to follow best practices of standards such as ISO/IEC 27001, ISO/IEC 27002 or their subsequent revisions, if any, from time to time.

Law stated - 5 December 2024

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

While there is no specific statutory provision that requires information security personnel to keep directors informed of an organisation's network preparedness, in the event of a cybersecurity breach, the persons in charge of an organisation will be required to demonstrate before the regulators that they have implemented security control measures as per their documented information security programmes and information security policies. Therefore, it would be necessary for these persons to be aware of, and updated about, the information security preparedness of their organisation to effectively discharge their responsibilities.

Section 85 of the IT Act also specifically states that in case of any contravention of the provisions stipulated thereunder, any person who, at the time of contravention, was in charge of supervising the affairs of a company will be liable and proceeded against, unless he or she is able to prove that the contravention took place without his or her knowledge, or that he or she exercised all due diligence to prevent the contravention. Therefore, personnel can protect themselves from liability by being aware of and deploying adequate cybersecurity measures.

Separately, as per the CAM Rules, the managing director, company secretary or any other director or officer of the company (as may be decided by the board) is responsible for the maintenance and security of electronic records. This person is required, among

other things, to provide adequate protection against unauthorised access, alteration or tampering of records; ensure that computer systems, software and hardware are secured and validated to ensure their accuracy, reliability, and accessibility; and take all necessary steps to ensure the security, integrity and confidentiality of records. Any failure by such personnel in this regard may be construed to be a breach of their duties towards the organisation and is punishable with a fine. The CAM Rules also require an electronic voting system for companies with equity shares listed on a recognised stock exchange, and every company having not less than 1,000 members to have adequate cybersecurity in place.

It is also important to note that the CERT-In Directions now require service providers, intermediaries, data centres, bodies corporate and government organisations to designate a point of contact (POC) to interface with CERT-In. All communications from CERT-In seeking information and providing directions for compliance are to be sent to the said POC. The information relating to a POC is required to be sent to CERT-In, as well as kept updated from time to time. Accordingly, to demonstrate good-faith compliance with the CERT-In Directions, the management and persons in charge are to ensure such a POC is appointed and such details are communicated to CERT-In. Non-compliance with the CERT-In Directions is punishable with imprisonment and/or a fine.

Law stated - 5 December 2024

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Under the IT Act, 'cybersecurity' means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. 'Cybercrime', by contrast, has not been expressly defined under any central statute or regulations; however, the National Cyber Crime Reporting Portal (a body set up by the government to facilitate reporting of cybercrime complaints) has defined 'cybercrime' to mean 'any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime'. Further, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 define 'cybersecurity incident' as any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes in data, information without authorisation.

Under the CAM Rules, 'cyber' is defined as protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosures, disruption, modification or destruction.

Additionally, the Telecommunications (Telecom Cyber Security) Rules 2024 (Telecom Cyber Security Rules) issued by the DOT and effective from 21 November 2024, define 'telecom cybersecurity' as cybersecurity of telecommunication networks and telecommunication services which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance

and technologies that can be used to safeguard telecommunication networks and telecommunication services against relevant security risks in the cyber environment.

The RBI's Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices (Master Directions), which became effective in April 2024 and are applicable to regulated entities such as banks and non-banking financial companies, define 'cybersecurity' as preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. As per the definition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved in cybersecurity. Further, the Master Directions define a 'cyberincident' as a cyber event that adversely affects the cybersecurity of an information asset, whether resulting from malicious activity or not. Also, the Master Directions define 'cyberattack' as a malicious attempt (or more than one attempt) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorised access to assets.

Further, the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities released by SEBI in August 2024 defines a 'cyberthreat' as a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.

The courts in India have also dealt with various instances of cybercrime over the years. The Gujarat High Court, in the case of *Jaydeep Vrujlal Depani v State of Gujarat* (R/SCR.A/5708/2018 Order), recognised a publicly available definition of ‘cybercrime' to mean ‘the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)’.

While the IT Act does not make any distinction between cybersecurity and data privacy, in our view, these issues are distinct but also deeply interconnected, as ensuring the privacy of any data (whether of an individual or a corporate) requires adequate cybersecurity processes to be implemented by organisations. Further, cybersecurity and information security frameworks are developed by organisations at a broader level to build resilience against various forms of cyberthreat, including cybercrimes that entail more extensive engagement with regulatory authorities depending on the extent of the harm caused, the nature of the information handled by the body corporate, sector sensitivities, etc.

Law stated - 5 December 2024

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

As per the SPDI Rules, any body corporate that possesses, deals with or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements). The newly enacted, albeit yet to be notified, DPDP Act also puts an obligation on data fiduciaries to

adopt reasonable security safeguards to prevent personal data breach. While no specific standards are prescribed under the DPDP Act, more clarity may emerge once the rules are framed and notified thereunder.

Sector-specific cybersecurity measures have been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the RBI requires banks to undertake certain security measures, including, among other things, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security. The RBI also requires payment aggregators to implement data security standards and best practices such as PCI-DSS, PA-DSS, the latest encryption standards, transport channel security, etc as per the Guidelines on Regulation of Payment Aggregators and Payment Gateways. The Master Directions on Cyber Resilience and Digital Payment Security Controls for Nonbank Payment System Operators, released by RBI in July 2024, also mandate obtaining PCI-DSS certification and compliance with PCI-DSS guidelines for payment system operators storing card data.

Additionally, in the telecommunications sector, the licence conditions imposed by the DOT require every licensee to implement the following measures:

- ensure protection of privacy of communication so that unauthorised interception of messages does not take place;
- have an organisational policy on security and security management of its network, including network forensics, network hardening, network penetration tests and risk assessment; and
- induct only those network elements into its telecom network that have been tested as per relevant contemporary Indian or international security standards (eg, the IT and IT-enabled service elements against the ISO/IEC 15408 standards, the ISO 27000 series standards for information security management systems and the 3GPP and 3GPP2 security standards for telecom and telecom-related elements).

Also, the Telecom Cyber Security Rules issued by the DOT effective from 21 November 2024, mandate each telecom entity to ensure adoption of a telecom cybersecurity policy that provides for security safeguards, risk management approaches, actions, training, best practices and technologies to enhance telecom cybersecurity.

Further, critical information infrastructure (CII) is separately regulated by the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Guidelines for the Protection of National Critical Information Infrastructure (CII Guidelines). 'CII' has been defined under the IT Act to mean any computer resource, the incapacitation or destruction of which can have a debilitating impact on national security, the economy, public health or safety. Under the CII Guidelines, certain best practices and controls are provided as minimum recommendations to be implemented by the CIIs at different stages of CII functioning, to maintain safe and secure operations. In addition to the CII Guidelines, the NCIIPC in April 2020 also issued covid-19 guidelines titled 'Building Resilience

against Cyber Attacks during COVID-19 Crisis' that intend to provide guidance to CIIs on various issues, including managing email phishing risks, protection of organisational assets and enabling employees to work remotely. Further, the National Security Council Secretariat has released 'Cyber Security Audit – Baseline Requirements' (CSA-BR) for cyber information infrastructure prescribing minimum, common and harmonised baseline criteria for cybersecurity audits, which is to be mandatorily followed by all CIIs.

Law stated - 5 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The IT Act and related laws are equally applicable to cyberthreats involving intellectual property and grant similar protection.

Law stated - 5 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

As per section 70 of the IT Act, the government may notify any computer resource that directly or indirectly affects the facility of CII to be a 'protected system'. 'CII' means any computer resource of which the incapacitation or destruction can have a debilitating impact on national security, economy, public health or safety. Under the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, specific cybersecurity practices are applicable in the context of a protected system, such as setting up an information security steering committee (Committee) to approve all information security policies relating to the protected systems, designating a chief information security officer and carrying out vulnerability, threat or risk analysis on an annual basis and on a significant change or upgrade in the system, under intimation to the Committee. Significant changes in network configuration would need to be approved by the Committee, and organisations would need to ensure timely communication of cyberincidents to the Committee.

Under the provisions of the IT Act, a nodal body – the NCIIPC – has been set up to work in the interest of CII protection. The NCIIPC is authorised to reduce vulnerabilities of CII against cyberterrorism, cyber warfare and other threats. Certain identified CIIs are in sectors such as transport, telecoms, banking, insurance, finance, power, energy and governance.

The Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations 2023 prescribe measures to be taken by, among others, captive generating plants and energy storage systems to safeguard the national grid from spyware, malware,

cyberattacks and network hacking, and also include requirements for a security audit and a cybersecurity framework.

Sector-specific cybersecurity regulations are also available for sectors such as banking, telecommunications, finance and insurance.

Law stated - 5 December 2024

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

India does not have a dedicated cybersecurity law or regulation that restricts sharing of cyberthreat information. However, personal information and the right of privacy of an individual are protected under Indian law. In *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under article 21 of the Constitution of India and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence. Given that this issue is unsettled, the permissibility of recordings will need to be determined on a case-by-case basis.

In any event, the SPDI Rules require a body corporate to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the IT Act for the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes. The SPDI Rules also permit disclosure without consent in cases where the disclosure is made pursuant to an enforceable order under applicable law.

The SPDI Rules also allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer.

Under the DPDP Act, any processing (including disclosure) of personal data will require consent accompanied or preceded by a notice by the data fiduciary to the data principal (except in certain cases identified under the DPDP Act as legitimate use). However, disclosure of information may be done to the state or any of its instrumentalities, for fulfilling any obligation under any law for the time being in force in India. Further, disclosure may also be done for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution. Such disclosure will be subject to processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

Certain laws, such as the Telecommunication Act 2023 that was partially notified in June 2024 and the IT Act, permit governmental and regulatory authorities to access private communications and personally identifiable data in specific circumstances. The Telecommunication Act empowers the government to intercept messages in the interest of public order, national security or the prevention of crime, subject to certain prescribed safeguards. In that scenario, the telecom licensee that has been granted a licence by the DOT is mandated to provide necessary facilities to the designated authorities of the central government or the relevant state government for interception of the messages passing through its network.

The IT Act also grants similar authority to the government and its authorised agencies. Any person or officer authorised by the government (central or state) can, among other things, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event that it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data for cybersecurity incidents if they relate to contravention or investigation of any crime.

Law stated - 5 December 2024

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

Cybercrimal activities are specifically dealt with under the IT Act, which prescribes penalties ranging from fines to imprisonment for various types of cyberactivities, including hacking; tampering with computer source code; denial-of-service attacks; phishing; malware attacks; identity fraud; electronic theft; cyberterrorism; privacy violations; and the introduction of any computer contaminant or virus. Further, the CERT-In Directions also set out specific cybersecurity incidents, including targeted scanning/probing of critical networks/systems; attacks on internet-of-things devices and associated systems, networks, software and servers; attacks on servers, such as database, mail and domain name system, and network devices, such as routers.

Further, the BNS recognises cybercrime as an organised crime which is a continuing unlawful activity that involves use of violence, threat of violence, intimidation, coercion or any other unlawful means to obtain direct or indirect material benefit including a financial benefit, by any person or a group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate.

Law stated - 5 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

CERT-In Directions are applicable to cloud service providers as well. The CERT-In Directions have imposed certain obligations on cloud service providers, vis-à-vis data retention, and reporting. For instance, as per the CERT-In Directions, any attack or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing have to be mandatorily reported to CERT-In, within six hours of noticing such incident or such incident being brought to notice. Further, cloud service providers are required to register and retain certain mandatory data for their subscribers.

Further, given that cloud computing services are rendered and received over the internet or through the digital medium, certain other provisions of the IT Act, the SPDI Rules and the Intermediaries Guidelines may be relevant to these services.

For instance, the SPDI Rules allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer. Accordingly, in our view, any entity engaged in the cloud computing business will need to ensure that it maintains the same level of information security standards as that of the data controller (ie, the person collecting the information from the data subject).

Also, depending on the business model, a cloud services provider may fall within the definition of an 'intermediary' under the IT Act (defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cybercafes). As an intermediary, the cloud service provider will need to observe due diligence measures to claim safe harbour protection from liability arising from the content stored by it. These due diligence measures include taking all reasonable steps to secure its computer resource and the information contained therein by adopting the security practices prescribed under the SPDI Rules.

SEBI has also issued a Framework for Adoption of Cloud Services by SEBI Regulated Entities that is applicable to entities such as the Stock Exchange, clearing corporations and depositories and prescribes the framework for adoption of cloud services by entities regulated by SEBI. The Framework prescribes certain compliance requirements including mandating regulated entities to avail cloud services only from the Ministry of Electronics and Information Technology-empanelled cloud service providers.

The RBI also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways on 17 March 2020 and Regulation of Payment Aggregator – Cross Border (PA – Cross Border) on 31 October 2023, where it is mandated for all payment aggregators, and payment aggregators cross border, to adhere to the data-storage requirements applicable for payments data to ensure that all data is stored only in India for the RBI's unfettered supervisory access. Further, the Master Directions on Cyber Resilience and Digital Payment Security Controls for Nonbank Payment System Operators, released by the RBI in July 2024, mandates payment system operator availing cloud-based services to

have a cloud operation policy in place (as part of the board-approved information security policy) that must include provisions including role and responsibilities of cloud services providers, data localisation etc.

Law stated - 5 December 2024

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

As per section 75 of the IT Act, the IT Act also applies to any offence committed outside India if the act that constitutes the offence involves a computer, computer network or computer system in India. Hence, the applicability of this law is agnostic to the presence of foreign organisations in India so long as users in India can access the services provided by the organisations and the operation of the services amounts to the contravention of any provision described thereunder.

Further, in the context of applicability of the CERT-In Directions to overseas entities, the clarifications issued by CERT-In by way of FAQs suggest that the CERT-In Directions will apply to all entities in the matter of cyberincidents and cybersecurity incidents as long as the service is catering to users in India. This seems to indicate that CERT-In is of the view that CERT-In Directions would continue to apply as long as catering to Indian users, irrespective of fulfilment of the requirements of section 75 of the IT Act. We will have to await clarity on the interplay between section 75 of the IT Act and the position indicated by the FAQs issued on the applicability of CERT-In Directions.

Law stated - 5 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In addition to minimum statutory cybersecurity standards, various regulatory bodies have advised businesses to adopt more robust measures in areas of cybersecurity. For example, the Ministry of Communication and Information Technology released the National Cyber Security Policy in 2013, which recommended creating a secure cyberspace, strengthening laws and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy intended to encourage all organisations to develop information security policies integrated with their business plans and implement the policies in accordance with international best practices.

Under the Digital India initiative, the Ministry of Electronics and Information Technology (MeitY) has set up the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis

Centre), operated by the Computer Emergency Response Team (CERT-In), to work with internet service providers and product or antivirus companies to provide information and tools to users on botnet and malware threats. Similar proactive measures are deployed by sector-specific regulators from time to time.

Law stated - 5 December 2024

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

In recent years, the government has rolled out some beneficial measures to incentivise both public and private sector organisations to improve cybersecurity standards. One example is the Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products notified by MeitY on 2 July 2018, which was further revised by the Public Procurement (Preference to Make in India) Order 2019 for Cyber Security Products notified by MeitY on 6 December 2019, wherein cybersecurity was named as a strategic sector, and government procurement agencies will give preference to domestically manufactured or produced cybersecurity products.

Law stated - 5 December 2024

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In addition to the Information Technology Act 2000 and the applicable rules framed thereunder (including the CERT-In Directions, which prescribe specific obligations for maintenance of logs, information and communication technology clock synchronisation, and data retention requirements), industry-specific standards have been prescribed by specific regulators. Some examples are given below.

- Financial sector: the Reserve Bank of India has issued various guidelines for ensuring cybersecurity and the handling of cyber fraud within the banking sector. They can be accessed at www.rbi.org.in and include:
    - the Cyber Security Framework in Banks, prescribing standards to be followed by banks for securing themselves against cybercrimes;
    - the Basic Cyber Security Framework for Primary (Urban) Cooperative Banks, prescribing certain basic cybersecurity controls for primary urban cooperative banks; and
    - the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2023, effective from April 2024, that incorporates, consolidates and updates the guidelines, instructions and circulars on IT governance, risk, controls, assurance practices and business continuity/disaster recovery management.

- Insurance sector: the insurance sector is subject to the IRDAI Information and Cyber Security Guidelines 2023, issued by the Insurance Regulatory and Development Authority of India (IRDAI). These Guidelines are applicable to all insurers, including insurance intermediaries, brokers, corporate agents etc, regulated by IRDAI. The Guidelines apply to all data created, received or maintained by such entities in the course of, carrying out, their designated duties and functions, irrespective of the place of storage and form of such data. The Guidelines stipulate the organisational structure to be created for the governance, implementation and monitoring of information security.
- Telecommunications sector: the licence conditions for a unified licence granted by the Department of Telecommunication (DOT) prescribe various cybersecurity obligations on the licensee entity. For instance, the licensee is obligated to ensure the protection of privacy of communication and that unauthorised interception of messages does not take place; and the licensee is to be completely responsible for security of its networks and must have an organisational policy on the security and security management of their networks, etc. Due to the large surge in cybersecurity incidents fuelled by large-scale remote work adoption during the covid-19 pandemic, the DOT has issued, among others, various security-related circulars to update stakeholders, such as Best Practices – Cyber Security- , which provide protocols to be followed by organisations; and Unsafe Practices to be Avoided at Workplace for Cyber Security, which describe unsafe workplace practices that may be avoided, such as using common passwords, leaving devices unlocked, ignoring operating systems and software updates and downloading files without scanning. The Telecommunications (Telecom Cyber Security) Rules 2024 mandate telecommunication entities to implement certain measures such as the adoption of a telecom cybersecurity policy that includes security safeguards, risk management approaches, actions, training, best practices and technologies, to enhance telecom cybersecurity.
- Entities regulated by the Securities Exchange Board of India (SEBI): SEBI released the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities in August 2024, which requires regulated entities such as stock exchanges and mutual funds to, among other things, encrypt data and use layering of full-disk encryption along with file-based encryption.

Law stated - 5 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

Depending on the nature and the extent of the cybersecurity incident and the sensitivity of the sector, cyberincident response strategies may differ from one business to another. Some common measures that are recommended include:

- deploying a detailed information security policy to be approved by the board;

- conducting regular transaction monitoring;
- conducting information security risk assessments;
- setting up risk mitigation and transition plans;
- updating relevant stakeholders within the organisation on their role in advance; and
- allocating appropriate personnel to engage with regulatory authorities and to deal with clients, service providers, etc. For instance, the CERT-In Directions provide that service providers, intermediaries, data centres, bodies corporate and government organisations must appoint a point of contact to engage with CERT-In for certain compliance-related obligations.

Many companies also prefer to conduct regular assessments of the vulnerabilities in their systems, including by inviting focused hacking. Depending on the sector, organisations can also reach out to CERT-In and seek advice on incident recovery, containing the damage and restoring their systems to operation. From time to time, CERT-In also issues advisories on actions recommended for parties that have been affected by cybersecurity incidents.

Law stated - 5 December 2024

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

While there are mandatory reporting requirements under the CERT-In Directions, it is also possible for individuals and organisations to voluntarily report any other cybersecurity incidents and vulnerabilities to CERT-In and seek requisite support and technical assistance to recover from them. Whether timely and voluntary reporting will help mitigate the imposition of a penalty for failing to implement reasonable security practices will be a fact-specific assessment, given there is no formal guidance in this regard.

Moreover, the Ministry of Home Affairs has set up a toll-free National Helpline number '1930' (previously '155260') and an online reporting platform (the 'National Cyber Crime Reporting Portal') to enable persons to make immediate complaints of financial loss caused to such persons due to cyber financial frauds including debit or credit card fraud, e-wallet and internet banking related fraud. Further, the platform can be used to report other types of cybercrimes.

In addition, the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities, applicable on regulated entities such as alternative investment funds, clearing corporations and mutual funds requires such entities to submit quarterly reports to SEBI with information on cyberattacks and threats experienced by such entities and the corresponding measures that were taken to mitigate the vulnerabilities, threats and attacks.

Law stated - 5 December 2024

Public-private cooperation

.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The government issues consultation papers to invite feedback and suggestions from the private sector, which aids the formulation of policies and laws in respect of cybersecurity. For instance, presently, the government is working with the private sector to develop its 2020 cybersecurity strategy. In addition, in 2019 the National Cyber Security Coordinator and the Data Security Council of India launched an online repository on cybertech called 'Techsagar' to facilitate exchange and collaboration on matters of innovation and cybersecurity between businesses and academia. It is intended to provide an overview of India's cybersecurity preparedness and relevant stakeholders.

In 2018 MeitY launched the first-ever public-private partnership of its kind called 'Cyber Surakshit Bharat' to strengthen the cybersecurity ecosystem in India by spreading awareness about cybercrime and undertaking capacity-building for chief information security officers and IT staff across all government departments. The founding partners of the consortium are IT companies Microsoft, Intel, WIPRO, Redhat and Dimension Data. Additionally, knowledge partners include CERT-In and the National Information Centre, industry associations nasscom and the FIDO Alliance, and consultancy firms Deloitte and EY.

Law stated - 5 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Cybersecurity insurance has gained momentum in India. It is aimed at shielding online users against the damage and loss that may arise as a result of unauthorised disclosure of or access to personal and financial data. Cyber insurance is prevalent and common in the banking, IT and I-enabled services, retail and manufacturing sectors.

Furthermore, in 2023 a task force set up by government submitted recommendations for formulation of a National Cyber Security Strategy 2023, which can be expected to provide certain guidance on cyber insurance. However, the Strategy has not yet been released.

Law stated - 5 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Computer Emergency Response Team (CERT-In) is the nodal agency recognised under the Information Technology Act 2000 (IT Act) for the coordination of cyberincident

response activities and the handling of cybersecurity incidents. Further, the government has also established certain authorities and agencies for according protection specifically to the critical infrastructure of India, such as the National Critical Information Infrastructure Protection Centre, which was created to assess and prevent threats to vital installations and critical infrastructure in India. As and when a cybersecurity incident is determined, individuals and organisations can seek remedy from the adjudicating authorities appointed under the IT Act.

Sector-specific regulators have also attempted to enforce compliance with their respective information security standards. For example, the Reserve Bank of India (RBI) imposed a monetary penalty of 12.7 million rupees on the Bank of Maharashtra for non-compliance with the directions of the Cyber Security Framework in Banks.

In January 2020, the Union Minister for Home Affairs inaugurated the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime in a comprehensive and coordinated manner. One of the components of I4C is the National Cyber Crime Reporting Portal, which is a citizen-centric initiative that enables citizens to report all kinds of cybercrime online, with a specific focus on crimes against women and children – particularly child pornography, child sexual abuse material and online content pertaining to rapes, gang rapes and similar crimes. The complaints reported on this portal are dealt with by law enforcement agencies and the Police, based on the information made available in the complaints.

The Digital Personal Data Protection Act 2023 (DPDP Act) mandates a data fiduciary to have reasonable security safeguards in place to prevent breach of personal data. The Data Protection Board of India established by the central government under the DPDP Act can impose a monetary penalty of up to 2.5 billion rupees for breach in observing this obligation.

Law stated - 5 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Given that CERT-In is the national nodal agency responsible for cybersecurity, it has the authority to call for information and give directions to service providers, intermediaries, data centres, bodies corporate and any other person to perform their functions under the IT Act, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions. Failure to respond to CERT-In's information requests may lead to the imposition of monetary penalties as well as imprisonment for a term that may extend to one year, or both.

Further, the adjudicating authorities appointed under the IT Act have the powers of a civil court to call for evidence and documents, and summon witnesses in connection with an inquiry into any contravention under the IT Act.

As per the provisions of the IT Act, for national security and for investigation of any offence (including cybersecurity offences), authorised government officers can issue

orders to intercept, monitor or decrypt any computer resource, and ask intermediaries to provide access to any information or to block access to any information stored, received or generated in any computer resource. Additionally, law enforcement agencies can be authorised to monitor and collect traffic data or information generated, received or transmitted in any computer resource, and can confiscate any computer resource in respect of which any contravention of the IT Act has been carried out.

Indian law also provides law enforcement authorities with various other mechanisms to pursue, investigate and prosecute cybercriminals. For instance, the Bharatiya Nyaya Sanhita 2023 (BNS) (formerly referred to as the Indian Penal Code 1860) is a comprehensive code intended to cover most substantive aspects of criminal law. Criminal activities punishable under the BNS do extend to the online cyberspace infrastructure and will be dealt with in the same manner.

Under the DPDP Act, the Data Protection Board of India established by the central government can inquire into breach of personal data under certain circumstances and impose penalty.

Law stated - 5 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Regulators in India have relied on the provisions of the IT Act and the BNS to prosecute entities found to be non-compliant with mandatory information security requirements. However, from a practical perspective, enforcement agencies often face challenges in prosecuting offshore entities that do not have a business presence in India, as well as affixing liability in multi-layered business outsourcing structures. The absence of a comprehensive data protection law that allocates cybersecurity responsibilities between all relevant stakeholders is also a concern. Over time, the private sector and the government have felt the need to develop more cybercrime and prosecution expertise among the police personnel responsible for prosecuting offences under the IT Act, and specific local cyber cells have been set up to address this gap.

Law stated - 5 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

There is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. However, as per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions specific types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of

an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) have to be mandatorily reported to CERT-In by service providers, intermediaries, data centres, bodies corporate and government organisations within six hours of noticing the incident or being notified of the incident. As per the frequently asked questions issued for the CERT-In Directions, while the incidents specified in the Directions need to be mandatorily reported, it has been clarified that cybersecurity incidents not specified in the Directions or Rules also need to be reported considering the nature, severity and impact of the incident. If multiple parties are affected by a cybersecurity incident, any entity that notices the cybersecurity incident must report it to CERT-In.

In addition, sector-specific regulators have their own reporting requirements. For instance, the RBI requires banks to comply with the Cyber Security Framework in Banks, which, among others, requires banks to report cybersecurity incidents to the RBI within two to six hours. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to put in place a mechanism for the monitoring, handling and follow-up of cybersecurity incidents and breaches. These incidents and breaches must be reported immediately to the Department of Payment and Settlement Systems, RBI, Central Office, Mumbai, and reported to CERT-In.

As per the DPDP Act, a data fiduciary is required to notify the Data Protection Board of India (established by the central government) and the data principal affected by such breach. The form and manner of such notification will be prescribed in the rules to be formulated under the DPDP Act.

Law stated - 5 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The IT Act provides for penalties for varied instances of cybersecurity breaches, some of which are described here. Section 43 of the IT Act provides that any person accessing a computer or a computer system or network without permission of the owner, downloading copies and extracting any data or causing disruption of any system will be liable to pay damages to the person affected. Section 66 of the IT Act also provides for punishment of imprisonment for a term up to three years or with a fine of up to 500,000 rupees if the person dishonestly or fraudulently commits the offence.

Section 66C of the IT Act provides that a person who, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person will be punished with imprisonment of up to three years and will also be liable for payment of a fine of up to 100,000 rupees.

Additionally, the IT Act under section 70B provides for imprisonment of up to one year or a fine of up to 100,000 rupees, or both, for any failure by an entity (service provider,

intermediary, data centre, body corporate, etc) to provide requisite information requested by CERT-In. Furthermore, sector-specific authorities (eg, the RBI) may also levy penalties for non-compliance with their respective cybersecurity standards.

Further, under the DPDP Act failure to have reasonable security safeguards in place to prevent breach of personal data can result in imposition on the data fiduciary of a financial penalty of up to 2.5 billion rupees.

In addition, penalty can also be imposed by sector-specific regulators such as the RBI, the Securities Exchange Board of India (SEBI) and the Insurance Regulatory and Development Authority of India, depending on the nature of the violation.

Law stated - 5 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Any failure by intermediaries, service providers, data centres, bodies corporate and government organisations to mandatorily report a cybersecurity breach within the stipulated timelines or furnish any information to CERT-In, as per the process provided under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions, is punishable by imprisonment of up to one year or a fine that may extend to 100,000 rupees, or both.

In addition, sector-specific regulators have their own reporting requirements. For instance, failure to report within the timelines prescribed for banks under the Cyber Security Framework in Banks may result in the imposition of penalties by the RBI. For the telecommunications sector, the unified licence conditions stipulate that any failure by the licensee to comply with the obligations provided therein, including reporting of any intrusions, attacks and frauds on the technical facilities, may render the concerned licensee liable to a monetary penalty of up to 500 million rupees per breach.

Under the DPDP Act, a failure to notify the Data Protection Board of India or affected data principal of a personal data breach can result in a penalty of up to 2 billion rupees.

Law stated - 5 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The IT Act makes statutory remedies available to persons affected by a cybersecurity incident. Section 43A of the IT Act expressly provides that whenever a body corporate possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security practices and procedures that in turn cause wrongful loss

or wrongful gain to any person, the body corporate will be liable to pay damages to the person affected. Therefore, the affected party may initiate a civil action against the negligent body corporate, making it liable to pay damages.

Further, a civil action may also be brought against any person who, without permission of the owner of a computer or a computer system or network, does any of the acts mentioned under section 43 of the IT Act, including but not limited to accessing or securing access to the computer or computer system or network, downloading or extracting any data from it, contaminating it with a virus or other malware, or causing any damage to it.

In addition, SEBI's Guidelines (Cyber Security & Cyber Resilience Framework for Stock Brokers/Depository Participants) have mandated stockbrokers and depository participants to draft their cybersecurity and cyber resilience policy document and ensure provisioning of alternate services or systems to customers in the event of any security incident.

The Ministry of Home Affairs has set up a toll-free National Helpline number '1930' (previously '155260') and an online reporting platform (the National Cyber Crime Reporting Portal) to enable persons to immediately report financial loss caused to persons due to cyber financial frauds including debit or credit card fraud, e-wallet and internet banking related fraud, etc. This reporting platform can also be used by persons to report other kinds of cybercrimes, which include unauthorised access of data or data breach, ransomware, online and social media-related crimes, cryptocurrency related frauds, etc.

Under the newly enacted DPDP Act, a data principal has a right to readily available means of grievance redressal to be provided by the data fiduciary and/or consent manager. The right available to a data principal is for an act or omission by the data fiduciary and consent manager regarding the performance of their obligation under the DPDP Act or exercise of the data principal's rights under the DPDP Act. For instance, such acts or omissions can include failure to have reasonable security safeguards in place to prevent breach of personal data and failure to intimate the affected data principal of a personal data breach.

Law stated - 5 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Directions released by the Computer Emergency Response Team (CERT-In) (CERT-In Directions) prescribe certain compliance requirements for service providers, intermediaries, data centres, bodies corporate, virtual private server providers, cloud service providers, VPN service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations (individually and collectively, 'Entities'). These compliance requirements include the following:

- Reporting of a cybersecurity incident: specified cybersecurity incidents are to be reported to CERT-In within six hours of noticing such incidents or of being notified of such incidents.

- Appointment of a POC: a point of contact (POC) is to be appointed to engage with CERT-In in relation to the CERT-In Directions. Details of the POC need to be provided to CERT-In and should be kept updated.
- Maintenance of logs in India: logs of information and communications technology (ICT) systems are to be maintained for a rolling period of 180 days.
- ICT clock synchronisation: entities must connect to a network time protocol (NTP) server of the National Informatics Centre or National Physical Laboratory or with NTP servers traceable to these NTP servers, for synchronisation of the ICT systems clocks of such entities.
- Data retention: data centres, cloud service providers, virtual private server providers and virtual private network service providers are required to maintain certain data (eg, name of subscriber, email address and IP address, address and contact number, ownership pattern, etc) for five years or a longer duration as mandated by law after any cancellation or withdrawal of registration.
- Virtual asset service providers: virtual asset exchange providers and custodian wallet providers must maintain all information obtained as part of know your customer policy and records of financial transactions for five years.

In addition to the requirements mentioned above, CERT-In issued its Guidelines on Information Security Practices for Government Entities on 30 June 2023 for all the ministries, departments, secretariats and offices specified in the First Schedule to the Government of India (Allocation of Business) Rules 1961, their attached and subordinate offices, and all government institutions, public sector enterprises and other government agencies under their administrative purview. The Guidelines include guidelines prepared by the National Informatics Centre for Chief Information Security Officers and employees of central government ministries/departments for the purpose of enhancing cybersecurity and cyber hygiene.

In addition to the above, some specific requirements are mentioned below:

- Information Technology Act 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules): as per the SPDI Rules, all organisations handling sensitive personal information of natural persons (financial and health information, passwords, biometric data, etc) should, among other things:
    - have information security systems in place that are commensurate to the information assets sought to be protected;
    - appoint a grievance officer to address any discrepancies and grievances of the provider of such information;
    - have a privacy policy for providing information on how such information is used and disclosed, etc; and
    - audit the reasonable security practices and procedures that have been implemented at least once a year, or as and when the body corporate or a person on their behalf undertakes significant upgrading of their process and computer resources.
-

Companies (Management and Administration) Rules 2014: companies, when dealing with electronic records, are required to ensure the security of any such records, including:

- protection against unauthorised access;
- protection against alteration;
- protection against tampering;
- maintaining the security of computer systems, software and hardware;
- protecting signatures; and
- taking periodic backups; etc.

- The Reserve Bank of India (RBI) has issued a notification on 'Cyber Security Framework for Banks', which prescribes standards to be followed by banks for securing themselves against cybercrimes, including, for example, a mechanism for dealing with and reporting incidents, a cyber crisis management plan, and arrangements for continuous surveillance of systems and protection of customer information. A similar framework is applicable to non-banking finance companies. The Guidelines on Regulation of Payment Aggregators and Payment Gateways require payment aggregators to put in place a Board-approved information security policy for the safety and security of payment systems operated by them and to implement security measures in accordance with this policy to mitigate identified risks.
- The Insurance Regulatory and Development Authority of India (IRDAI) has issued the IRDAI Information and Cyber Security Guidelines 2023, which, among other things, mandate insurers to appoint a chief information security officer, formulate a cyber crisis management plan and conduct audits.
- In August 2024, SEBI released the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities that is applicable on regulated entities such as alternative investment funds, clearing corporations and mutual funds. This framework requires, among other things, for such regulated entities to document and implement a cybersecurity and cyber policy. Further, the framework requires such entities to have a cyber risk management framework in place for identification and analysis, evaluation, prioritisation, response and monitoring the cyber risks on a continuous basis.

Law stated - 5 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

CERT-In Directions prescribe that entities such as service providers, intermediaries, data centres, bodies corporate and government organisations (Entity) are required to maintain logs of information and communication technology (ICT) systems for a rolling period of 180 days. The logs to be maintained will depend on the sector in which an Entity is operating

and may include firewall logs, event logs of critical systems, application logs, VPN logs, etc. Relevant logs need to be provided to CERT-In when cyberincidents are reported or when so ordered by CERT-In. The frequently asked questions (FAQs) suggest that these logs can be stored outside India as long as a copy is retained within India. The FAQs also provide that logs for successful as well as unsuccessful events must be recorded.

Sector-specific regulators have prescribed storage requirements for regulated entities. For instance, IRDAI issued the IRDAI Information and Cyber Security Guidelines 2023, which require information and communications technology (ICT) to be maintained for a rolling period of 180 days and within the Indian jurisdiction.

Lastly, in accordance with the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities Securities Exchange Board of India Guidelines (Cyber Security & Cyber Resilience Framework for Stock Brokers/Depository Participants), stockbrokers and depository participants alternative investment funds, clearing corporations and mutual funds etc are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period not less than two years (at least six months in online mode and rest in archival mode).

Law stated - 5 December 2024

Regulatory reporting requirements

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Reporting under the IT Act

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 permit cybersecurity incidents to be reported by any individual organisation or corporate entity to CERT-In. In addition, as per the CERT-In Directions specified types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) must be reported to CERT-In by service providers, intermediaries, data centres, bodies corporate and government organisations within six hours of noticing the incident or the incident being brought to their attention. The Guidelines on Information Security Practices for Government Entities issued by CERT-In also require such entities to report a cyberincident to CERT-IN within six hours of noticing the incident or the incident being brought to their attention.

The Intermediaries Guidelines require the intermediaries, as part of their due diligence obligations, to notify CERT-In of security breaches. CERT-In publishes the formats for reporting cybersecurity incidents on its website from time to time. The Guidelines require

that incident reports mention the time of the incident, the type of incident, information regarding the affected systems or network, the symptoms observed, the relevant technical systems deployed and the actions taken, among others.

Reporting in other sectors

In addition to the reporting requirements under the IT Act, separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the Cyber Security Framework in Banks requires banks to inform the RBI of any cybersecurity incident within two to six hours of the breach and include details of it in a standard reporting template. Such report must include all unusual cybersecurity incidents (whether they were successful or were attempts that did not succeed). Similarly, the IRDAI Information and Cyber Security Guidelines 2023 require all insurers, including foreign reinsurance branches and insurance intermediaries regulated by IRDAI, to report cybers to CERT-In within six hours of noticing or being told about such incidents, with a copy to IRDAI and other concerned regulators/authorities.

As per the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, all listed entities need to submit a quarterly report of the details of cybersecurity incidents or breaches or loss of data or documents to the recognised stock exchange. Further, as per the Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities, entities such as stockbrokers, depository participants, alternative investment funds, clearing corporations and mutual funds etc need to report cyberattacks, cybersecurity incidents and/ or breaches falling under the CERT-In Directions shall be notified to SEBI and CERT-In within six hours of noticing/detecting such incidents using the email mkt_incidents@sebi.gov.in. The framework requires all other incidents to be reported within 24 hours.

In the telecommunications sector, every telecommunications licensee is required to create a facility (within 12 months of grant of authorisation) for monitoring intrusions, attacks and frauds on its technical facilities, and to provide reports of these intrusions, attacks and frauds to the Department of Telecommunications (DOT).

The Telecom Cyber Security Rules issued by the DOT effective from 21 November 2024 mandate telecommunication entities to report security incidents within six hours of becoming aware of such incidents affecting their telecommunication networks or services to the central government with relevant details of the affected system, including the description of the incidents. These Rules further require telecommunication entities to share information such as the number of users affected by the security incidents and the duration of the security incidents within 24 hours of becoming aware of such incident.

Law stated - 5 December 2024

Time frames

30 | What is the timeline for reporting to the authorities?

As per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions,

specific types of cybersecurity incidents (eg, target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/ suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) must be reported to CERT-In by service providers, intermediaries, data centres, bodies corporate and government organisations within six hours of noticing the incident or being told about the incident.

Separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the RBI requires banks to report cybersecurity incidents within two to six hours. Further, the RBI mandates non-bank payment system operators to report unusual incidents such as cyberattacks, outage of critical system/infrastructure, internal fraud, settlement delay, etc to the RBI and CERT-In within six hours of detection.

Similarly, the IRDAI Information and Cyber Security Guidelines 2023 require all insurers, including foreign reinsurance branches and insurance intermediaries regulated by IRDAI, to report cyberincidents to CERT-In within six hours of noticing or being told about such incidents, along with a copy to IRDAI and other concerned regulators/authorities.

The Telecom Cyber Security Rules issued by the DOT effective from 21 November 2024 mandate the telecommunication entity to report security incident within six hours of becoming aware of such incident affecting its telecommunication network or telecommunication service to the central government with relevant details of the affected system including the description of such incident. These Rules further require telecommunication entities to share information such as the number of users affected by the security incident and the duration of the security incident, within 24 hours of becoming aware of such incident.

Law stated - 5 December 2024

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Currently, there is no obligation to report cybersecurity threats or breaches to the general public or affected parties. However, under the Digital Personal Data Protection Act 2023 (DPDP Act), in the event of a personal data breach, the data fiduciary is required to notify each affected data principal of such breach. The draft of the Digital Personal Data Protection Rules 2025 (which is still in its consultation stage) provides that each data principal needs to be intimated of the data breach in a concise, clear and plain manner and without delay, through their user account or any mode of communication registered by them. However, this position will only be crystallised once the final rules are notified.

The Telecom Cyber Security Rules issued by the DOT effective from 21 November 2024, applicable on telecommunication entities, provide that if the central government determines that disclosure of a security incident having potential risk on telecom cybersecurity is in the

public interest, it can either by itself inform the public of such security incident, or require the affected telecommunication entity to inform the public.

Law stated - 5 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Various factors have contributed to the delayed formulation of cybersecurity regulations in India, including the rapid advancement of technology, which continues to outpace regulatory response; intermittent and ineffective reporting of incidents; the private sector's inability to accurately assess the criticality of available information and the likely harm that may be caused in the event of an incident; lack of cross-functional expertise on the nature of cybersecurity incidents that may be experienced by varied sectors; and government and private sector hesitation to mandate minimum standards for all categories of businesses, in view of the time and expense involved.

In the past year, however, there has been a renewed focus on the adoption of robust cybersecurity practices in India, from both the government and the private sector. Since the Covid-19 pandemic and the large-scale adoption of remote work and new technology resulting from it, the private sector has been quite vigilant in adapting its processing, updating its budgets and responding to cyberthreats in a timely and nuanced manner. Several organisations, such as the Data Security Council of India, have proactively issued advisories and assisted other private sector organisations to seamlessly transition to safer digital processes. We expect these initiatives to guide the government in terms of the level of cybersecurity preparedness expected from organisations, how the private sector has responded to cybersecurity threats, a renewed focus on the revision of policies and the diversified skill-set of response stakeholders, and testing the efficacy of protective technologies and strategies. Timely and descriptive cybersecurity reporting by the private sector will bring in more collaboration and clarity on better practices. The varied experiences of regulated businesses regarding cyberincidents will help guide policy, as it is likely that sensitive sectors such as healthcare and social security will require a higher standard of compliance in view of the nature of their operations and risk assessment.

We expect some regulatory developments proposed by the government to further energise compliance. In 2023, a task force set up by government submitted recommendations for formulation of a National Cyber Security Strategy 2023, which it is hoped will provide better security standards. However, the Strategy has not yet been released.

The proposed Digital India Act 2023 that will replace the Information Technology Act 2000 can also be expected to bring a robust and dedicated law dealing with cybersecurity.

The newly enacted Digital Personal Data Protection Act 2023 (DPDP Act) and the rules to be notified thereunder will also play a critical role in shaping the regulatory environment in relation to the protection of personal data, as they seek to prescribe certain obligations of

data fiduciaries (persons who determine the purpose and means of processing of personal data), which include among other things the use of reasonable security safeguards to prevent personal data breach, deletion of data after the purpose for collection is served, having a grievance redressal mechanism in place and processing of personal data only for lawful purpose for which appropriate consent has been received. Further, the data fiduciary and data processor need to notify the Data Protection Board of India (proposed to be constituted under the DPDP Act) in case of breach of this personal data. The Data Protection Board may in the event direct the data fiduciary to remedy this personal data breach or mitigate any harm caused to data principals.

Law stated - 5 December 2024

AZB & PARTNERS
ADVOCATES & SOLICITORS

Sumit Ghoshal sumit.ghoshal@azbpartners.com
Aprajita Rana aprajita.rana@azbpartners.com
Shagun Badhwar shagun.badhwar@azbpartners.com
Suyash Tiwari suyash.tiwari@azbpartners.com

AZB & Partners

Italy

Paolo Balboni, **Luca Bolognini**, **Francesco Capparelli**, **Giulia Finocchiaro**
ICT Legal Consulting

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Italy's cybersecurity landscape boasts a robust, multi-dimensional regulatory framework, seamlessly integrating EU directives with national legislation. This structure ensures high standards for data protection, operational resilience and security across critical sectors and services, from financial operations to public infrastructure. At the core of this framework is the General Data Protection Regulation (EU) 2016/679 (GDPR), which, alongside the Italian Personal Data Protection Code (Legislative Decree 196/2003), provides a stringent foundation for the protection of personal data. Article 32 of the GDPR mandates that data controllers and processors implement technical and organisational measures tailored to the level of risk involved in data processing. In Italy, article 2*septies* of the Personal Data Protection Code reinforces this, specifying additional protections for health-related personal data, reflecting the heightened sensitivity of this information.

To address sector-specific needs, Legislative Decree 51/2018, which transposes Directive (EU) 2016/680 (the Law Enforcement Directive), outlines specialised security measures for data handling by law enforcement agencies, ensuring secure data processing within judicial and police operations. Furthermore, Legislative Decree 231/2001, which focuses on the criminal liability of companies, indirectly promotes cybersecurity by mandating that companies establish protocols and control mechanisms to prevent computer crimes, thereby embedding cybersecurity as a core component of corporate governance.

A significant pillar of Italy's cybersecurity strategy is the National Cybersecurity Perimeter, established by Decree-Law No. 105/2019 and further defined by Prime Ministerial Decree No. 131/2020 and Presidential Decree No. 54/2021. This regulatory framework imposes stringent requirements on public admistrations and critical national entities, covering sectors such as telecommunications, energy, transportation and finance. It mandates robust procedures for managing supply chain security, continuous monitoring and incident reporting to prevent disruptions. Presidential Decree No. 54/2021 further specifies compliance and audit requirements, ensuring that entities within the cybersecurity perimeter meet Italy's standards for cyber risk management and resilience .

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), which was transposed into Italian law through Legislative Decree 138/2024, significantly extends the scope and stringency of its predecessor, the original NIS Directive (implemented in Italy through Legislative Decree 65/2018). NISNISni2 covers additional sectors such as energy, healthcare, transportation and financial services, mandating comprehensive risk assessments, incident response and cybersecurity controls to strengthen Italy's cyberdefences across essential and digital services. To support consistent implementation across member states, Implementation Regulation (EU) 2690/2024 specifies technical and methodological requirements for cybersecurity risk management under 2, harmosing measures with international standards such as ISO/IEC 27001 and ETSI EN 319401 .

For the financial sector, the Digital Operational Resilience Act (Regulation (EU) 2022/2554, known as DORA), approved on 10 November 10 2022, effective from 16 January 2023 and binding from 17 January 2025, mandates rigorous cybersecurity and resilience standards for banks, insurance firms and other financial institutions. DORA enforces stringent information and communication technology (ICT) risk management, incident response, resilience testing and governance over third-party digital service providers. Complementing this, Regulation (EU) 2024/1773 and Regulation (EU) 2024/1774 outline further operational and simplified risk management requirements, obligating financial entities to document and refine their cybersecurity policies regularly to address evolving threats .

Supporting operational security in information management, ISO/IEC 27002:2022 offers a control framework for cybersecurity practices applicable across various sectors, aligning with GDPR, NISnisni2 and DORA requirements. It emphasises controls in organisational security, technological safeguards and human factors, making it an essential reference for Italian organisations aiming to establish strong information security defences in compliance with national and EU regulations .

Italy also adheres to the eIDAS Regulation ((EU) 910/2014), which governs electronic identification and trust services across the European Union, essential for secure digital transactions. eIDAS mandates that trust service providers notify authorities of significant security incidents impacting service reliability or personal data protection, further bolstering Italy's secure digital ecosystem .

Lastly, the PSNC Cybersecurity Model (Modello Misure di Sicurezza 1.0.1) provides Italian entities with structured guidelines for implementing security controls, asset management and incident response processes. This model reinforces Italy's regulatory approach by promoting consistent updates, routine audits and robust threat detection mechanisms, aligning closely with both Italian and EU standards for cybersecurity .

Through this integrated framework, Italy is positioned to address evolving cybersecurity challenges comprehensively, protecting personal data, ensuring the resilience of critical infrastructures, and supporting secure digital transformation across sectors. Italy's cybersecurity regulatory structure exemplifies a proactive, harmonised approach, reflecting its commitment to safeguarding digital integrity and operational resilience on both a national and EU level.

Law stated - 2 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In Italy, the financial services sector is highly impacted by cybersecurity regulations due to the critical role it plays in the economy and the stringent requirements established by the GDPR, DORA and oversight bodies such as the Bank of Italy and the European Central Bank. These regulations mandate comprehensive standards for digital operational resilience, risk management and controls over third-party services, making cybersecurity a priority for financial institutions.

Healthcare is another sector where cybersecurity is paramount. The GDPR, along with national regulations such as article 2*septies* of the Italian Personal Data Protection Code, imposes strict measures to protect sensitive health data. This focus on security has intensified with the growth of digital health services and telemedicine, which bring additional cybersecurity challenges.

In the realm of critical infrastructure, energy and utilities are subject to extensive cybersecurity obligations. The sector must comply with the NIS2 Directive, recently transposed into Italian law by Legislative Decree 138/2024, as well as Italy's National Cybersecurity Perimeter. These regulations demand high levels of security to prevent and respond to potential disruptions that could impact on national stability.

Telecommunications and digital services are also heavily influenced by cybersecurity legislation, particularly the NIS2 Directive. In Italy, national communications authority AGCOM enforces sector-specific cybersecurity requirements, recognising the essential role of telecommunications in the digital economy and mandating measures to secure communication networks and protect data integrity.

The transport and logistics sector has seen an increase in cybersecurity requirements, especially under the NIS2 Directive. Given its importance to economic stability and national security, regulations ensure that this sector maintains resilient infrastructure capable of withstanding cyberthreats.

Lastly, the manufacturing sector, especially areas associated with Industry 4.0, is now more affected by cybersecurity regulations due to its increased digitalisation and exposure to cyber risks. The expanded scope of the NIS2 Directive covers certain critical manufacturing processes, acknowledging the sector's importance and potential vulnerability in the digital era.

Law stated - 2 December 2024

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

Yes, Italy has incorporated several international standards into its cybersecurity framework to align with global best practices and enhance regulatory compliance. Notably, Italy utilises ISO/IEC 27001 and ISO/IEC 27002 standards for information security management and controls, which serve as foundational benchmarks in Italian cybersecurity regulations, particularly within the context of the NIS2 Directive and Italy's National Cybersecurity Perimeter.

As of 30 July 2024, the National Cybersecurity Agency (ACN) is responsible for regulatory oversight of qualifying cloud services, having taken over from Agency for Digital Italy AgID. This move is part of a broader strategy to centralise national cybersecurity management. Concurrently, theACN's Directorial Decree of 2 January 2023 (from now, the Cloud Services Regulation) introduced new regulations defining the qualification path for cloud services in the public administration. This framework mandates public administrations to maintain and regularly update a catalogue of their data and digital services, categorised by characteristics as per article 3 of the Cloud Services Regulation. Cloud services are

required to meet different qualification levels (QC1 to QC4) based on the data processed and security measures implemented, with requirements ranging from ISO 9001 and ISO/IEC 27001 certifications to self-assessments aligned with ISO 22301 and ISO 20000 standards.

Law stated - 2 December 2024

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Directors and responsible individuals are held accountable through penalties that may be enforced if they fail to meet these obligations. The authority considers factors such as the severity of non-compliance, previous incidents and the organisation's overall security posture when determining the sanctions' severity .

A company's liability for failing to implement adequate cybersecurity measures is twofold, encompassing both administrative and criminal aspects. Administratively, the Italian Data Protection Authority (DPA) may impose fines for failing to implement sufficient security protocols, particularly in the event of a data breach. Criminally, under article 24*bis* on computer crimes and unlawful data processing of Legislative Decree 231/2001, liability extends to responsible employees and directors if the lack of appropriate measures leads to computer crimes.

The inclusion of computer-related offences in Legislative Decree 231/2001 requires a thorough risk analysis based on the company's activities and the proactive updating of the organisation and management model, as required by the Decree.

Directors also face civil liability for failing to take the necessary precautions. Individual employees can be held accountable for violating the company's code of ethics and organisational model, with potential disciplinary sanctions outlined within these frameworks.

Law stated - 2 December 2024

Key definitions

5 How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

In Italian legislation, 'cybersecurity' generally refers to measures, procedures and tools aimed at protecting networks, systems and data from unauthorised access, attacks or disruptions. According to Legislative Decree 138/2024, cybersecurity encompasses both technical and organisational actions necessary to manage and mitigate such risks to the security of information and communication systems. This aligns with the definitions in the NIS2 Directive, which emphasises a high level of security for network and information systems across critical sectors. However, it also refers to criminal activities

conducted through digital means or targeting information systems, as understood under both EU and Italian law. Legislative measures such as Legislative Decrees 231/2001 and 138/2024 address cybercrime indirectly by mandating that organisations implement robust cybersecurity protocols to prevent incidents such as data breaches or unauthorised access that could result in legal liability for the organisation or its directors.

Law stated - 2 December 2024

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In Italy, organisations are required to implement a range of fundamental protective measures to safeguard data and IT systems from cyberthreats. Defined under the NISnisni2 Directive (transposed through Legislative Decree 138/2024) and other relevant laws, these measures emphasise comprehensive risk analysis to identify and mitigate cybersecurity risks, supported by formal security policies that integrate technical, organisational and operational protections. Organisations are expected to have structured processes in place for managing cyber incidents, including detection, response and mandatory reporting, ensuring minimal disruption and rapid recovery.

Business continuity and disaster recovery plans are essential, with specific requirements for regular backups and operational resilience protocols that enable a swift response in the event of an incident. Supply chain security is another critical aspect, as companies are responsible for evaluating the cybersecurity practices of their suppliers and service providers, especially in sectors deemed essential or critical.

Minimum requirements also include securing network and information systems by adopting best practices in software acquisition, development and maintenance, particularly in vulnerability management and secure coding practices. Basic cyber hygiene, such as enforcing multi-factor authentication and controlling access to systems, secure communications and regular staff training, is also mandated. Encryption and cryptography play a key role in safeguarding sensitive data, ensuring it remains protected from unauthorised access throughout the organisation's digital infrastructure. Together, these measures establish a robust defence framework to counter cyberthreats and maintain high standards of cybersecurity resilience.

Law stated - 2 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The legal framework in Italy for addressing cyberthreats to intellectual property (IP) is multifaceted, blending traditional IP protection laws with modern cybersecurity and cybercrime provisions.

Firstly, there are foundational legal provisions for IP protection that were originally designed for traditional, offline scenarios but have become relevant in addressing cyberthreats as new technological means emerge to infringe upon IP rights. Key laws include the Italian Industrial Property Code, which governs patents, trademarks and industrial designs, and the Italian Copyright Law, which protects creative works. Additional protection is provided by IP-related sections in the Italian Civil Code and Italian Penal Code. These laws collectively cover actions such as the unlawful use of confidential information, unauthorised access to trade secrets, trademark infringements and counterfeiting of products, including those distributed online.

Secondly, the Italian legal system addresses certain cyber-related behaviours that, while primarily defined as administrative or criminal offences, may also result in the infringement of IP rights. The Italian Penal Code criminalises unauthorised access to computer systems, possession and distribution of access codes without authorisation, distribution of malware and computer fraud. These offences frequently overlap with IP violations when used to unlawfully access, alter or disseminate protected intellectual assets. Legislative Decree 184/2021 further modernised the Penal Code by introducing specific offences related to the misuse and counterfeiting of non-cash payment instruments and by adding an aggravating circumstance for computer fraud, reflecting the evolving threat landscape for IP-related cybercrime.

Additionally, Legislative Decree No. 231/2001 extends corporate criminal liability to companies that fail to prevent cybercrimes affecting IP rights, if these acts are conducted in the interest or for the benefit of the company. Under this Decree, organisations are encouraged to implement cybersecurity protocols and governance measures aimed at preventing unauthorised access, data leaks and cyberbreaches, which are essential for protecting sensitive IP assets such as trade secrets, proprietary research and trademarks.

This dual approach combines Italy's traditional IP protections with a modernised framework for cyberoffences, ensuring that IP rights are safeguarded against both conventional and emerging cyberthreats. This integration allows Italy to address cyberthreats to IP assets comprehensively, responding to both the technological sophistication of cybercriminals and the specific vulnerabilities of IP in the digital age.

Law stated - 2 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Italy has implemented specific laws and regulations addressing cyberthreats to critical infrastructure and essential sectors. A primary framework is Legislative Decree 138/2024, which transposes the NIS2 Directive. This Decree mandates stringent cybersecurity requirements for 'essential' and 'important' entities across critical sectors, including energy, healthcare, transportation, finance and digital infrastructure. These sectors must establish advanced risk management, incident handling and compliance monitoring protocols to prevent service disruptions and protect national security .

Additionally, Decree-Law No. 105/2019 establishes the National Cybersecurity Perimeter in Italy, applying heightened security measures to safeguard public administration networks and critical infrastructure against cyberthreats. It sets forth obligations for security assessments, reporting of incidents and protection against supply chain vulnerabilities for critical sectors such as telecommunications and utilities .

For the financial sector, DORA also imposes comprehensive requirements for managing ICT risks, especially in relation to third-party services. DORA ensures that financial entities, including banks and insurance firms, have robust cybersecurity frameworks to handle operational disruptions, safeguarding both financial stability and public trust .

Together, these laws represent a cohesive approach to protecting Italy's critical infrastructure from cyberthreats, encompassing sector-specific mandates and cross-sector cybersecurity standards.

Law stated - 2 December 2024

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In Italy, specific cybersecurity laws do not restrict the sharing of cyberthreat information outright but impose limitations and conditions to protect sensitive data, national security and business confidentiality. Legislative Decree 138/2024, implementing the NIS2 Directive, encourages cybersecurity information-sharing arrangements among essential and important entities to enhance cyberresilience. However, it mandates that information sharing respects the sensitive nature of data exchanged and that these arrangements are subject to specific protocols, especially for potentially sensitive information .

The ACN, as Italy's networks and information systems (NIS) competent authority, has the authority to facilitate such arrangements while setting conditions to safeguard the security and confidentiality of information. Information deemed sensitive for national security or business confidentiality reasons, such as trade secrets or critical infrastructure vulnerabilities, must be protected in compliance with both EU and national laws. For example, information with confidentiality concerns is only shared with the European Commission and other member state authorities when essential and under strict protective measures .

In the financial sector, DORA similarly supports voluntary threat intelligence sharing among financial entities, provided that such exchanges occur within trusted communities and adhere to data protection and business confidentiality rules to prevent unauthorised dissemination of sensitive operational information .

Law stated - 2 December 2024

Criminal activities

10

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The principal cybercrimes punished in the Italian Criminal Code concern abusive access to the computer system (under article 615*ter*), damage to computer systems (articles 635-*bis* and 635*quarter*) and computer fraud (article 640*ter*), also when committed with the alteration of the computer system that determines a transfer of money, monetary value or virtual currency. Under these provisions, the most important forms of cybercrimes that can be committed by company employees or by cybercriminals are criminalised, such as unauthorised access to an employee's email account, phishing or ransomware. The illicit use of payment instruments that could be the result of phishing activities and ransomware viruses is punished.

Other type of crimes are those provided for in articles 615*quarter* to 615*quinquies* regarding the possession, dissemination and unauthorised installation of equipment, computer program codes and other means of accessing computer or telecommunications systems, as well as in articles 617*quarter* and 617*quinquies*, which punish the unlawful interception, obstruction or interruption of computer or telematic communications.

Law stated - 2 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The adoption of new digital technologies, including cloud computing, in Italy is governed by EU regulations such as the GDPR and the free flow of non-personal data (Regulation (EU) 2018/1807). Additionally, national security legislation such as Law 133/2019 establishes the National Cybersecurity Perimeter, which includes provisions for cloud computing security. Concurrently, in Italy, theACN's Directorial Decree of 2 January 2023 (from now, the Cloud Services Regulation) introduced new regulations defining the qualification path for cloud services in the public administration

The Italian Standards Body has adopted key international ISO security standards, while AgID has elevated CSA STAR certification, integrated with ISO 27017 and 27018, as a viable alternative to ISO 27001 certification for validating the security of cloud services, particularly software as a service (SaaS), used within the Italian public administration.

As of 19 January 2023, regulatory oversight for the qualification of cloud services has been transferred from AgID to the ACN.

In parallel with this transition, the Cloud Services Regulation introduced a new regulation that defines the qualification path for cloud services within the public administration. This new framework requires public administrations to maintain and regularly update a catalogue of their data and digital services, categorised according to their characteristics, as described in article 3 of the Cloud Services Regulation. Depending on the data processed and the security measures implemented, cloud services require different levels of qualification, with each level mandating compliance with specific requirements.

Law stated - 2 December 2024

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Italian cybersecurity laws impose certain obligations on foreign organisations operating within the country, particularly in sectors deemed critical or essential, under regulations such as Legislative Decree 138/2024. This Decree transposes the NIS2 Directive, which requires that foreign providers of critical services, such as cloud computing, digital infrastructure and telecommunications, comply with Italian cybersecurity standards if they offer services in Italy. Foreign entities must also designate a representative within the European Union, typically in the member state where their primary E establishment is located, to ensure accountability and compliance with local cybersecurity obligations .

Additionally, the National Cybersecurity Perimeter framework, governed by Decree-Law No. 105/2019, imposes specific requirements on foreign companies involved in the Italian critical infrastructure. These companies are required to undergo risk assessments and implement secure data storage practices within the European Union, ensuring alignment with Italian data sovereignty and security regulations.

These regulations ensure that foreign organisations operate under the same cybersecurity standards as domestic entities, reinforcing the security of Italy's critical infrastructure and data protection framework.

Law stated - 2 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In Italy, authorities encourage additional cybersecurity protections beyond mandated legal requirements, particularly in the context of the National Cybersecurity Strategy. This strategy promotes several enhanced measures, such as advanced cyber hygiene practices and the integration of 'zero trust' principles, which include continuous network monitoring, software updates and secure identity management. The Italian framework, under Legislative Decree 138/2024, also supports information-sharing platforms and partnerships to facilitate proactive threat management and rapid response across sectors- .

Additionally, Italian regulations emphasise the adoption of ISO/IEC standards such as ISO 27002, which recommend strong controls, including vulnerability management and secure configuration practices that exceed baseline legal requirements. These practices

are suggested particularly for entities with critical infrastructure to ensure resilience against sophisticated attacks .

Law stated - 2 December 2024

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

The Italian government incentivises organisations to enhance their cybersecurity through a combination of strategic guidance, support programmes and public-private partnerships. Under Legislative Decree 138/2024 implementing Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Italy encourages entities to adopt advanced cybersecurity measures beyond the baseline requirements, such as using innovative technologies like artificial intelligence and automated tools for detecting and preventing cyberattacks. This approach aims to improve overall resilience, particularly in sectors critical to national security .

The government also promotes the adoption of open-source cybersecurity tools to reduce costs, particularly for small and medium-sized enterprises (SMEs). This initiative helps SMEs access affordable, community-driven tools, which can bolster their defences without significant financial strain . Additionally, Italy's National Cybersecurity Strategy encourages organisations to engage in information-sharing programmes and join public-private partnerships, facilitating knowledge exchange and best practices to fortify cybersecurity across sectors .

These measures are complemented by incentives for research and development in cybersecurity technologies and financial support for SMEs to improve their cybersecurity posture, creating an ecosystem where organisations are encouraged to actively enhance their security practices.

Law stated - 2 December 2024

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The main industry standards and codes of practice promoting cybersecurity in Italy include:

- ISO/IEC 27001 and ISO/IEC 27002 – these standards are central to information security management and cybersecurity practices across sectors. ISO/IEC 27001 provides a framework for setting up, implementing and maintaining information security management systems, while ISO/IEC 27002 offers guidance on specific security controls applicable across domains, such as access control, network security, and incident management ;
-

NIST SP 800-37 and NIST SP 800-63 – from the National Institute of Standards and Technology, these publications provide guidelines for risk management in information systems and digital identity. NIST SP 800-37 covers a lifecycle approach to security and privacy, while NIST SP 800-63 offers digital identity guidelines, focusing on authentication and identity lifecycle management; and

- OWASP Top Ten – published by the Open Web Application Security Project, the OWASP Top Ten highlights critical security risks for web applications. It serves as a valuable guide for developers and security teams in mitigating application-layer vulnerabilities.

Law stated - 2 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

Italy promotes best practices and procedures for responding to cybersecurity breaches through guidelines established by standards such as ISO/IEC 27002:2022 and regulatory frameworks such as Legislative Decree 138/2024. Key recommended practices include pre-incident planning, where organisations define roles, establish reporting protocols and prepare escalation procedures tailored to various incident scenarios. In the event of a breach, organisations are advised to execute rapid containment and mitigation measures, followed by a thorough root-cause analysis and documentation of all response activities .

CSIRT Italia, Italy's computer security incident response team, also provides specific guidance for organisations, offering support in handling incidents that could escalate or have cross-border impacts. Regular coordination with CSIRT Italia, as mandated under Legislative Decree 138/2024, ensures that organisations have access to mitigation support and incident response resources, including public guidelines on minimising and managing breach impacts. These practices are encouraged to strengthen organisations' resilience and prevent future incidents by integrating insights and lessons learned into security protocols .

Law stated - 2 December 2024

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

In Italy, voluntary sharing of cybersecurity information is encouraged to strengthen collective resilience across sectors, with specific practices and procedural support outlined under Legislative Decree 138/2024, which implements the NIS2 Directive. Essential and important entities, as well as other relevant organisations, can voluntarily exchange information on cyberthreats, vulnerabilities and near misses to enhance detection,

prevention and response capabilities. Such information-sharing efforts are designed to raise awareness of emerging threats, promote collaborative threat research and improve incident mitigation across public and private entities.

The National Cybersecurity Agency (ACN) facilitates and coordinates these information-sharing arrangements. ACN provides dedicated platforms and automation tools to support this exchange, ensuring that the sensitive nature of shared information is respected and that arrangements comply with both competition laws and data protection regulations .

Additionally, the Digital Operational Resilience Act (Regulation (EU) 2022/2554, known as DORA), encourages financial institutions to participate in trusted communities for sharing threat intelligence, which includes tactics, techniques and procedures for cyberdefence. This supports the resilience of financial entities against complex cyberthreats through structured information-sharing arrangements, governed by rules that protect business confidentiality and personal data .

These frameworks not only enable but actively promote voluntary cybersecurity collaboration, leveraging shared knowledge to mitigate risks more effectively. The Italian government, through the ACN, assists in implementing these arrangements by providing technical resources and ensuring compliance with regulatory requirements, which collectively serve as incentives for proactive threat information sharing.

Law stated - 2 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In Italy, voluntary sharing of cybersecurity information is encouraged to strengthen collective resilience across sectors, with specific practices and procedural support outlined under Legislative Decree 138/2024, which implements the NIS2 Directive. Essential and important entities, as well as other relevant organisations, can voluntarily exchange information on cyberthreats, vulnerabilities and near misses to enhance detection, prevention and response capabilities. Such information-sharing efforts are designed to raise awareness of emerging threats, promote collaborative threat research and improve incident mitigation across public and private entities.

The ACN facilitates and coordinates these information-sharing arrangements. The agency provides dedicated platforms and automation tools to support this exchange, ensuring that the sensitive nature of shared information is respected and that arrangements comply with both competition laws and data protection regulations .

Additionally, DORA encourages financial institutions to participate in trusted communities for sharing threat intelligence, which includes tactics, techniques, and procedures for cyberdefence. This supports the resilience of financial entities against complex cyberthreats through structured information-sharing arrangements, governed by rules that protect business confidentiality and personal data .

These frameworks not only enable but actively promote voluntary cybersecurity collaboration, leveraging shared knowledge to mitigate risks more effectively. The Italian government, through the ACN, assists in implementing these arrangements by providing technical resources and ensuring compliance with regulatory requirements, which collectively serve as incentives for proactive threat information sharing.

Law stated - 2 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

In Italy, cybersecurity insurance is available and increasingly common as organisations recognise the financial and operational risks associated with cyber incidents. The availability of such insurance extends to most organisations, including SMEs, particularly in industries identified as critical under the NIS2 Directive and the National Cybersecurity Perimeter. Policies typically cover a range of incidents, such as data breaches, ransomware attacks and business interruption, providing financial support for recovery and liability costs.

The Italian government, while not directly involved in the provision of insurance, indirectly promotes its adoption through regulatory frameworks that encourage robust risk management. For example, compliance with ISO/IEC 27002:2022 standards on risk and incident management can positively impact an organisation's insurability, as insurers view adherence to these standards as a demonstration of strong cybersecurity posture .

Additionally, the growing regulatory landscape, including requirements under Legislative Decree 138/2024 and DORA, incentivises organisations to seek insurance as a complementary layer of protection. These regulations increase the accountability of directors and organisations for cyber risks, driving demand for financial safeguards like insurance. While cybersecurity insurance uptake is growing, it remains concentrated among larger enterprises and regulated industries, with SMEs increasingly entering the market as awareness rises.

Law stated - 2 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In Italy, several regulatory authorities are responsible for enforcing cybersecurity rules, depending on the sector and the nature of the cybersecurity obligations. Key authorities include the following:

-

National Cybersecurity Agency (ACN): the primary authority overseeing Italy's cybersecurity framework, particularly for entities within the National Cybersecurity Perimeter and those governed by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), the ACN is responsible for setting national cybersecurity strategies, monitoring compliance and coordinating incident response for critical infrastructure.

- Data Protection Authority: the Authority enforces data protection rules under the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Italian Personal Data Protection Code. It oversees cybersecurity measures related to the protection of personal data, particularly for incidents involving breaches of confidentiality, integrity, or availability of personal information.
- Communications Authority (AGCOM): it supervises cybersecurity in the telecommunications and digital services sectors. AGCOM ensures compliance with specific security requirements for electronic communications, as mandated by national and EU regulations such as the NIS2 Directive.
- Bank of Italy and CONSOB (National Commission for Companies and the Stock Exchange): these authorities regulate cybersecurity within the financial sector and enforce the Digital Operational Resilience Act (Regulation (EU) 2022/2554, known as DORA) and sector-specific rules, requiring financial institutions to maintain robust information and communication technology (ICT) risk management practices.
- Computer Security Incident Response Team (CSIRT Italia): it operates under the ACN and coordinates cybersecurity incident management. It supports public and private organisations in handling breaches and reporting incidents as required under national and EU laws.

These authorities collaborate to ensure comprehensive enforcement of cybersecurity rules across sectors, leveraging Italy's integrated regulatory framework to enhance national resilience against cyberthreats.

Law stated - 2 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

In Italy, regulatory authorities are granted broad powers to monitor compliance, investigate violations and prosecute infringements related to cybersecurity laws. These powers include the following:

- Monitoring compliance:
    - ACN: as the primary authority for entities within the National Cybersecurity Perimeter, the ACN has the power to conduct audits, oversee compliance with security protocols and issue directives for corrective actions. Under the

NIS2 Directive, the ACN monitors compliance through risk assessments and ensures that essential and important entities adhere to mandatory cybersecurity requirements.

- Data Protection Authority: the Authority monitors compliance with the GDPR and national data protection laws. It has the authority to inspect data processing systems, verify the implementation of technical and organisational measures and issue administrative fines for breaches of data protection requirements.

- Investigative powers:
  - ACN: can conduct in-depth investigations into cybersecurity incidents affecting critical infrastructure. It collaborates with CSIRT Italia to analyse incidents, assess vulnerabilities and determine root causes.
  - AGCOM: investigates telecommunications and digital service providers for non-compliance with cybersecurity obligations, including failures in maintaining network integrity or reporting breaches as required by the NIS2 Directive.
  - Bank of Italy and CONSOB: investigate financial institutions for breaches of cybersecurity regulations under DORA, including failures in ICT risk management and incident reporting.

- Prosecution of infringements:
  - Data Protection Authority: imposes administrative sanctions for violations of the GDPR, with fines reaching up to 4 per cent of global annual turnover for severe breaches. It can also refer cases to judicial authorities for potential criminal prosecution.
  - ACN: refers serious cybersecurity infringements involving critical infrastructure to law enforcement for prosecution. In cases where breaches are linked to national security risks, the agency works with the judiciary and law enforcement agencies to pursue penalties under relevant criminal statutes.
  - Public Prosecutor's Office: handles criminal cases involving cybercrimes such as unauthorised access, data theft or computer fraud, often in collaboration with other authorities such as the ACN and CSIRT Italia.

These powers ensure that Italian regulatory authorities can effectively enforce cybersecurity laws, deter non-compliance and protect critical infrastructure, personal data and national security.

Law stated - 2 December 2024

Most common enforcement issues

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common enforcement issues in cybersecurity in Italy include inconsistent compliance across sectors, limited resources for smaller entities and delays in reporting cyber incidents. These challenges arise from the complexity of aligning various stakeholders, particularly in critical and essential sectors regulated by Legislative Decree 138/2024, which implements the NIS2 Directive.

The ACN and CSIRT Italia have addressed these issues by providing sector-specific guidelines, facilitating training and awareness programmes and developing automated tools for reporting and threat detection. Public-private partnerships have also been encouraged to foster collaboration, particularly in sharing threat intelligence and best practices. These partnerships allow private-sector expertise to support regulatory compliance, enabling smaller organisations to meet cybersecurity standards more effectively .

Moreover, regulatory frameworks have been updated to provide clarity on incident reporting and cybersecurity risk management obligations. These include tailored compliance requirements for different sectors, enabling a more practical and equitable application of cybersecurity laws . By integrating these measures, the Italian government seeks to mitigate enforcement issues and strengthen national cybersecurity resilience.

Law stated - 2 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Businesses are required to notify relevant authorities and, in certain cases, affected individuals following a cybersecurity breach. Under the GDPR, organisations based in the European Union must report breaches that pose risks to individuals' rights and freedoms to supervisory authorities within 72 hours of becoming aware of the incident. When the breach is likely to result in a high risk, such as potential identity theft or financial harm, individuals must also be informed without undue delay – unless the data was encrypted or other mitigating measures have reduced the risk.

The NIS2 Directive imposes obligations to notify national authorities of significant cybersecurity incidents that disrupt essential services. This notification must occur within 24 hours, with a comprehensive follow-up report submitted within one month. Users of the affected services must also be informed if their rights or access to services are impacted.

Other regulatory frameworks, such as DORA for the financial sector, require even more stringent timelines, with major incidents necessitating notification within four hours. In jurisdictions such as the United States, laws such as the California Consumer Privacy Act (CCPA) or the New York SHIELD Act emphasise notifying affected individuals when unauthorised access to personal data occurs, ensuring they can take steps to protect themselves.

These frameworks emphasise prompt action, requiring clear and factual communication to authorities and, where necessary, individuals. Organisations failing to meet these

requirements face significant penalties, underscoring the need for robust incident response mechanisms and compliance monitoring.

Law stated - 2 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Failure to comply with regulations designed to prevent cybersecurity breaches can result in severe repercussions for organisations, ranging from significant financial penalties to broader operational and reputational consequences. Under the GDPR, organisations that fail to implement adequate data protection measures or neglect their breach notification obligations may face fines of up to €20 million or 4 per cent of their global annual turnover, whichever is greater. Similarly, the NIS2 Directive imposes substantial fines for non-compliance with risk management or incident reporting requirements, with penalties scaled to reflect the size and economic impact of the offending entity.

Beyond financial sanctions, regulatory non-compliance often leads to operational constraints. Authorities may suspend business licences, enforce mandatory audits or require costly remedial measures to address security deficiencies. These actions can disrupt business continuity and impose a long-term financial burden. Furthermore, public enforcement actions frequently result in reputational harm, eroding customer trust and diminishing stakeholder confidence. This reputational damage can significantly impact market competitiveness and lead to the loss of contracts or partnerships, particularly in sectors reliant on robust cybersecurity credentials.

Civil liability is another consequence of non-compliance. Individuals or entities affected by a breach caused by insufficient security measures may seek compensation for damages, which can amplify the financial and legal exposure of the organisation. In cases of gross negligence or intentional misconduct, criminal liability may also arise, potentially leading to sanctions against executives or key personnel responsible for cybersecurity governance.

The cumulative effect of these penalties underscores the critical importance of adhering to cybersecurity regulations. Organisations must adopt proactive compliance measures, continuously assess risks, and align their security frameworks with evolving legal standards to mitigate the profound consequences of regulatory breaches.

Law stated - 2 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Under Legislative Decree 138/2024, which transposes the NIS2 Directive into Italian law, and DORA, the failure to comply with rules governing the reporting of threats and breaches

entails a robust framework of sanctions, reflecting the critical importance of timely and accurate incident reporting to ensure cybersecurity and operational stability.

Legislative Decree 138/2024 establishes penalties for entities failing to comply with reporting obligations related to significant cybersecurity incidents. The NIS2 Directive mandates that entities must notify their national competent authorities within 24 hours of becoming aware of an incident that has a significant impact on the provision of essential or important services.

Failure to comply with these obligations may result in administrative fines that are proportionate to the size and economic capacity of the entity. The fines aim to penalise the lack of timely notification or inaccurate reporting, which undermines the ability of authorities to respond effectively to threats. The decree also empowers national regulators to impose operational measures, such as mandatory cybersecurity improvements, where reporting failures reveal systemic vulnerabilities.

In cases of deliberate omission or negligence, the penalties may escalate, involving reputational sanctions, such as public notices of non-compliance, or suspension of activities, particularly for entities that fail to cooperate in addressing systemic threats or deficiencies exposed by their non-compliance.

DORA applies specifically to the financial sector and establishes stringent requirements for incident reporting. Entities regulated under DORA must report ICT-related incidents classified as 'major' to their financial supervisory authority within four hours of detection. A more detailed report is required within three days, covering root causes and mitigation measures.

Non-compliance with these reporting requirements triggers severe administrative fines. The regulation authorises supervisory authorities to impose penalties that may amount to millions of euros, scaled to the entity's turnover, reflecting the severity and potential systemic risk posed by non-reporting. The financial sector’s critical nature amplifies these penalties, with additional scrutiny applied to failures that expose interconnected systems to cascading risks.

DORA also grants supervisory authorities the power to enforce operational corrections. This includes mandating third-party audits, enforcing specific technology upgrades or, in extreme cases, suspending the use of specific third-party ICT services if their management poses unacceptable risks.

For entities subject to both Legislative Decree 138/2024 and DORA, overlapping obligations exist and compliance must align with the stricter of the two frameworks. Financial entities in particular are subject to dual scrutiny as they must meet sector-specific requirements under DORA, while also adhering to broader national obligations under Legislative Decree 138/2024. Authorities are equipped to enforce cumulative sanctions, leveraging both frameworks to address systemic and specific compliance failures.

The penalties for non-compliance under Legislative Decree 138/2024 and DORA are intentionally severe, aimed at deterring negligence and ensuring robust incident reporting practices. These frameworks underscore the importance of proactive compliance, requiring entities to implement robust monitoring, reporting and response mechanisms. Given the potential for compounded sanctions, organisations operating within regulated sectors must prioritise alignment with these regulations to mitigate legal, financial and reputational risks.

Law stated - 2 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Seeking private redress for unauthorised cyber or failures in protecting systems and data involves legal claims based on contract, tort or statutory frameworks. Contractual obligations, such as confidentiality or data protection clauses, are enforceable if breached, while tort claims, such as negligence, require proof of a duty of care, breach and resulting harm. Statutory provisions, such as the GDPR in the European Union or the CCPA in California, provide direct remedies for individuals harmed by inadequate cybersecurity measures, with the GDPR allowing compensation for material and non-material damages. Mass incidents often lead to collective actions, such as class lawsuits, which offer an efficient way to address widespread harm. Cross-border disputes, however, introduce complexities around jurisdiction and enforcement. Regulatory developments, such as DORA and the NIS2 Directive, emphasise managing third-party risks, reinforcing accountability across the supply chain. Success in such claims depends heavily on technical evidence, including forensic reports and breach logs. Standards such as ISO/IEC 27002 support evidence collection and risk management. Available remedies typically include monetary compensation, injunctive relief mandating security improvements and, sometimes, specific performance to fulfil contractual obligations. This legal framework reflects the growing interdependence of technology, regulatory compliance and legal accountability in the digital age.

Law stated - 2 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Organisations must adopt robust policies and procedures to protect data and IT systems from cyberthreats, ensuring compliance with regulations such as Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and the General Data Protection Regulation (EU) 2016/679 (GDPR), as well as adherence to standards such as ISO/IEC 27001. This includes defining governance structures, conducting regular risk assessments and implementing measures to mitigate vulnerabilities. Key areas include access control, with secure authentication and role-based permissions, and comprehensive incident response plans to manage and recover from breaches while complying with notification requirements. Data protection policies should enforce encryption, secure storage and adherence to data minimisation principles, while network security measures must address firewalls, intrusion detection and vulnerability

management. Staff training ensures awareness of risks and adherence to protocols, while third-party risk management extends security obligations to external providers. Logging, monitoring and regular security audits, including penetration testing, help identify and address threats effectively. These integrated measures enable organisations to maintain resilience and safeguard their systems and data against evolving cyber risks.

Law stated - 2 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Both Legislative Decree 138/2024, which implements the NIS2 Directive in Italy, and the Digital Operational Resilience Act (Regulation (EU) 2022/2554, known as DORA) establish clear obligations for organisations to maintain records of cyberthreats and attacks. These rules are crucial for enhancing organisational resilience, supporting compliance with incident reporting requirements, and enabling regulatory oversight.

Legislative Decree 138/2024 requires organisations within its scope, including operators of essential services and important entities, to maintain comprehensive records of cybersecurity incidents and threats. Specifically, organisation must maintain the following:

- Documentation of incidents: organisations must document all significant cybersecurity incidents, including their nature, causes and impact on services. This documentation is essential for the subsequent preparation of detailed reports to national competent authorities within the mandated time frames.
- Retention period: the Decree emphasises the necessity of retaining such records for a defined period, ensuring they are available for inspection by regulators and for analysis in case of subsequent related incidents. While the precise retention period may vary depending on the national implementation, it is typically aligned with the broader record-keeping obligations applicable to regulated entities.
- Audit and compliance: records of cyber incidents and threats must be sufficiently detailed to facilitate audits by regulatory authorities, demonstrating the organisation's adherence to risk management and reporting obligations.

DORA sets stricter record-keeping requirements for financial entities, reflecting the critical nature of the financial sector's reliance on information and communication technology (ICT) systems. Key obligations include the following:

- Incident logging: financial entities must maintain detailed logs of ICT-related incidents, including all major, minor and recurring threats or vulnerabilities. This includes the initial detection, response, mitigation measures and any lessons learned.
- Systematic record maintenance: DORA mandates the integration of record-keeping into an entity's operational resilience framework. This ensures records are

continuously updated and linked to broader ICT risk management practices, forming a comprehensive repository of historical and current threats.

- Third-party risks: records must also include incidents and vulnerabilities related to third-party ICT service providers, ensuring visibility across the supply chain.
- Retention period: the Regulation specifies a minimum period for which records must be kept, ensuring they are available for regulatory inspections, compliance audits and internal analysis. Although DORA does not prescribe a uniform period, financial regulators may establish sector-specific retention requirements.

Both frameworks align with international standards such as ISO/IEC 27001 and ISO/IEC 27002, which recommend systematic logging and maintenance of security-related incidents as part of an effective information security management system. These standards advocate for detailed record-keeping, including metadata such as time stamps, affected assets and mitigation actions, to support ongoing risk assessments and organisational learning.

Law stated - 2 December 2024

Regulatory reporting requirements

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Italy's Legislative Decree 65/2018, which transposes the NIS Directive ((EU) 2016/1148), establishes a notification requirement for digital service providers and operators of essential services. They are mandated to inform the Italian Computer Security Incident Response Team (CSIRT) and the relevant networks and information systems (NIS) authority about any incidents significantly impacting their service delivery. The assessment of an incident's significance considers various factors, including the number of users affected, especially those reliant on the digital service for their own services; the duration of the incident; its geographical spread; the degree to which the service's operation is disrupted; and the impact on economic and social activities.

While not being required to, companies that fall outside the scope of Legislative Decree 65/2018 may notify cybersecurity breaches to the CSIRT on a voluntary basis.

The NIS2 Directive requires affected organisations to notify the CSIRT or the relevant authority of significant incidents in a sequential manner. Firstly, a preliminary alert must be sent as soon as possible, within 24 hours of becoming aware of the significant incident. This alert should indicate, as appropriate, whether the incident is suspected to be the result of illegal or malicious acts or may have cross-border implications. Secondly, a detailed notification of the incident must then be issued within 72 hours of awareness, updating the preliminary information and providing an initial assessment of the severity and impact of the incident, together with any indicators of compromise. In addition, if requested by the CSIRT or an authority, an interim report is required with ongoing updates on the situation. Lastly, a comprehensive report must be submitted within one month of the incident notification, including a detailed description of the incident, its severity and impact, the likely threat

or cause, mitigation measures taken and in progress, and the cross-border impact of the incident, if relevant.

Entities subject to DORA are required to inform their clients of significant ICT-related incidents as soon as they become aware of them, and of the measures taken to mitigate the adverse effects of such incidents. Such entities shall classify cyberthreats as significant based on the criticality of the services at risk, including the transactions and operations of the financial entity, the number and/or importance of the customers or financial counterparties affected, and the geographical spread of the areas at risk.

Any cybersecurity breach that involves personal data shall be notified to the Italian Data Protection Authority (DPA), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Law stated - 2 December 2024

Time frames

30 | What is the timeline for reporting to the authorities?

The timeline for reporting cybersecurity incidents to authorities is defined by the specific regulatory framework and jurisdiction, with expectations emphasising promptness to ensure swift action and compliance. For instance, under the GDPR, personal data breaches must generally be reported to supervisory authorities within 72 hours of detection. The NIS2 Directive mandates a phased approach, requiring initial notification within 24 hours and a detailed follow-up within 72 hours, with potential for final reports as the incident resolution progresses. Other regulations, such as those under DORA for financial entities or sector-specific laws, also emphasise immediate reporting based on the severity of the incident. In jurisdictions such as the United States and Australia, reporting timelines are often framed around expediency, with obligations to notify authorities and affected individuals without undue delay. To meet these varied requirements, organisations must maintain effective incident detection, assessment and response systems, ensuring that reporting aligns with both regulatory obligations and the operational need for swift incident containment and resolution.

Law stated - 2 December 2024

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Organisations are increasingly required to report cybersecurity threats or breaches not only to authorities but also to customers, industry peers and sometimes the public, to enhance transparency and collective resilience. Under the NIS2 Directive, entities must report significant incidents and share information within their sectors to coordinate responses. The GDPR obligates organisations to notify individuals if a data breach poses a high risk to their

rights, providing actionable information promptly. Similarly, DORA in the financial sector emphasises informing ecosystem participants about incidents impacting on interconnected systems or third-party providers. In jurisdictions such as the United States, laws such as the California Consumer Privacy Act mandate notifying affected customers of breaches involving personal data, often with provisions for broader public disclosure in large-scale cases. Voluntary initiatives, such as Information Sharing and Analysis Centers, further facilitate threat intelligence sharing within industries, bolstering collaborative defences. These requirements collectively aim to mitigate risks, protect stakeholders, and maintain trust in interconnected digital environments.

Law stated - 2 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Developing cybersecurity regulations is challenging due to the rapid evolution of cyberthreats, jurisdictional fragmentation and the need to balance security with innovation. Laws often struggle to keep pace with emerging risks and international inconsistencies create compliance burdens for global businesses. Companies can influence regulation by engaging with policymakers, contributing industry insights and adhering to recognised standards such as ISO/IEC 27001 to set practical benchmarks. Over the next year, cybersecurity laws are expected to evolve, with frameworks such as Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union and the Digital Operational Resilience Act (Regulation (EU) 2022/2554 imposing stricter requirements on reporting, third-party risk management and operational resilience. Increased focus on supply chain security and critical infrastructure protection is also likely. Businesses must stay proactive, adapting to these changes and collaborating with regulators to ensure regulations remain both effective and feasible.

Law stated - 2 December 2024

Paolo Balboni paolo.balboni@ictlc.com
Luca Bolognini luca.bolognini@ictlc.com
Francesco Capparelli francesco.capparelli@ictlc.com
Giulia Finocchiaro giulia.finocchiaro@ictlc.com

ICT Legal Consulting

Read more from this firm on Lexology

Japan

Yasushi Kudo, **Tsubasa Watanabe**, **Hayato Maruta**
Nagashima Ohno & Tsunematsu

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The Japanese government has enacted the Basic Act on Cybersecurity (BAC), which defines cybersecurity and mandates that both national and local governments formulate and implement cybersecurity policies. The BAC also establishes an obligation on private businesses and citizens to make efforts to ensure cybersecurity.

The Act on the Protection of Personal Information (APPI) also imposes on business operators handling personal information the obligation to take security measures to prevent personal data leakage, loss or damage. These security control measures encompass technical, organisational, human and physical security control measures.

The Telecommunications Business Act (TBA) imposes on telecommunications carriers the obligation to establish rules for information handling, including security control measures to prevent incidents such as the leakage of users' information due to breach of communication confidentiality. These carriers must notify the Minister of Internal Affairs and Communications (MIC) of such rules.

These laws and other related laws and regulations ensure that businesses handling sensitive information adhere to stringent security standards to safeguard data integrity and confidentiality.

Law stated - 1 January 2025

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The most affected are the following 15 sectors, as designated in Annex 1 of the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP), developed by the Cybersecurity Strategy Center based on article 12 of the BAC:

- Information and communication
- Financial services
- Aviation
- Airports
- Railways
- Electric power supply
- Gas
- Government and administrative services

- Medical
- Water supply
- Logistics
- Chemical industry
- Credit cards
- Petroleum industry
- Port transport

The critical social infrastructure providers (CSIPs), as defined under article 3(1) of the BAC, doing business in these sectors are legally obliged to respond to a cybersecurity incident and report it to the competent regulatory authorities under business-related regulations established by the said authorities. The CSIPs are also obliged to make efforts 'to cooperate in the implementation of the cybersecurity policy that the national or local government implements' and ensure that they respond to the matters stipulated in the action plan established by the national government under article 6 of the BAC. Specifically, this efforts-based obligation encompasses strengthening systems for incident response, developing safety standards, strengthening information sharing systems and deploying risk management.

Law stated - 1 January 2025

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

Based on the Industrial Standardization Act, the Japanese government has established the Japanese Industrial Standards (JIS) as domestic standards for industry. The JIS refer to the standards established by the International Organization for Standardization (ISO) as the international ideal. Therefore, the JISs related to information security also reflect the international standards related to information security established by the ISO. JISs that refer to the information security management system (ISMS) standardised by ISO include JIS Q 27000:2019, JIS Q 27001:2023, JIS Q 27002:2024, JIS Q 27006:2018, JIS Q 27014:2020 as a standard for governance of information security and JIS Q 27017:2016 as a standard for security measures in response to cloud services.

Law stated - 1 January 2025

Personnel and director obligations

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The general interpretation in respect of directors' duty of care under the Companies Act is that it encompasses responsibility for managing cybersecurity risks through the

establishment and operation of an internal control system. Therefore, directors, including representative directors and chief information security officers, are obligated to establish and operate an appropriate cybersecurity system. Fulfilling this obligation entails managing and ensuring the adequacy of the organisation's cybersecurity defences.

In addition, in companies mandated to implement safety control measures and ensure the cybersecurity of their information based on the individual laws and guidelines, the person in charge of taking such measures and ensuring cybersecurity must evaluate and maintain the ISMS and overall cybersecurity system. This ensures ongoing compliance and the effectiveness of security measures.

Law stated - 1 January 2025

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Article 2 of the BAC defines 'cybersecurity' as the state whereby measures are taken for appropriate security management, including the prevention of leakage, loss or damage of information recorded or communicated electronically, and for ensuring the safety and reliability of information systems and networks, and which state is properly maintained and managed. In Japan, data privacy and cybersecurity are treated as distinct concepts, and the APPI covers data privacy. However, the above definition encompasses measures for appropriate security control of information and the proper maintenance of these measures, and overlaps with the obligation under the APPI to adopt security control measures for personal data. In addition, the National Police Agency, in Chapter 3 of its White Paper issued in 2024, defines 'cybercrimes' as 'violations of the Act on the Prohibition of Unauthorized Computer Access, crimes involving computer and electromagnetic records, and other crimes that use advanced information and communications networks as an essential means for their commission'.

Law stated - 1 January 2025

Mandatory minimum protective measures

6 | What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In Japan, while certain businesses are obligated to adopt safety control measures for cybersecurity pursuant to relevant laws and regulations, there is no rigid definition of specific methods as minimum requirements; rather, these methods are presented as reference information in the applicable guidelines. Each business entity is evaluated based on its implementation of measures deemed equivalent to or higher than a certain level, ensuring security in consideration of the associated risks. For instance, the APPI outlines specific methods for implementing security control measures against cyberattacks, and these methods are designed for business operators handling personal information. However, the methods are set forth as examples and their adoption is not compulsory.

For example, in the credit card business, a credit card operator that implements security control measures equivalent to or exceeding the measures outlined in the credit card security guidelines established by a professional body such as the Japanese Consumer Credit Association, a self-regulatory organisation for the credit card business, the operator is deemed to comply with the security standard mandated by the relevant laws and regulations.

In addition, entities designated as CSIPs under the BAC are mandated to implement certain safety control measures for cybersecurity. These measures are aligned with the laws governing their respective industries and are overseen by the relevant competent authorities.

Law stated - 1 January 2025

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

In Japan, the Unfair Competition Act (UCA) serves as the legislation governing cyberthreats to intellectual property, imposing criminal penalties for various acts, including the acquisition of trade secrets through unauthorised access with the intent to gain an advantage for oneself or to infringe upon the advantage of a third party.

According to the UCA, a 'trade secret' is defined as information meeting the following criteria:

- It must be kept confidential.
- It must consist of technical or business information that is beneficial for conducting business activities.
- It must not be publicly known.

Law stated - 1 January 2025

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The BAC has identified 15 sectors encompassing critical infrastructure projects such as gas and electricity. Operators within these sectors are designated as CSIPs under the BAC. CSIPs are subject to, among other requirements, the CPCIP and its associated guidelines for establishing safety standards, as outlined in the BAC. Additionally, each CSIP is obligated to adhere to the cybersecurity regulations stipulated by the corresponding competent authority overseeing its sector. They are also required to collaborate with such agencies to bolster cybersecurity efforts.

Law stated - 1 January 2025

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Under the TBA in Japan, criminal penalties are prescribed for actions that violate the secrecy of communications. Consequently, a debate arose about whether sharing cyberthreat information could potentially infringe upon this secrecy of communications.

In response to this issue, MIC, which supervises the telecommunications industry under the TBA, ed a study group to address the matter. This study group has compiled a report that concludes that, to enable internet service providers to effectively respond to cyberattacks, the sharing of specific information deemed necessary for cybersecurity measures by these providers does not constitute a violation of the secrecy of communications.

Law stated - 1 January 2025

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The principal criminal cyberactivities that are relevant to organisations are as follows:

- Unauthorised access to a computer system with restricted access via a network without legitimate authority, as provided in the Act on the Prohibition of Unauthorized Computer Access.
- Wrongfully creating electronic data used in processing a person's affairs, or using such data for illegitimate purposes, as provided in article 161-2 of the Penal Code.
- Creating or distributing malware without justifiable reason, as provided in article 168-2 and article 168-3 of the Penal Code.
- Interfering with a person's business by disrupting the operation of a computer used in the course of business, as provided in article 234-2 of the Penal Code. In addition, unjust economic gain by providing false information to a computer or by other means in relation to such a computer is punishable under article 246-2 of the Penal Code.

Law stated - 1 January 2025

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

To mitigate cybersecurity risks associated with the utilisation of cloud services, the Japanese government has implemented several measures. One of these measures is the establishment of JIS Q 27017:2016, which serves as the Japanese domestic standard for information security control measures specifically tailored for cloud services. This standard is based on the ISO framework. In addition, in response to these risks, the government has introduced the Information Security Management Assurance Program (ISMAP). ISMAP functions as a system to pre-evaluate and register cloud service providers that satisfy the security criteria set forth by the Japanese government. This initiative aims to provide assurance to users regarding the security posture of cloud service providers operating within Japan.

Law stated - 1 January 2025

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Japanese cybersecurity-related laws are applied consistently, regardless of whether the business entity is domestic or foreign. Therefore, such laws apply equally to foreign businesses operating in Japan.

For instance, provisions in the APPI concerning the transfer of personal data to third parties and the international transfer of personal data are applicable to foreign businesses operating in Japan, especially if they transfer personal data to their overseas parent companies. Moreover, if a foreign parent company provides goods or services to individuals in Japan from outside the country and handles personal information in the process, the APPI's extraterritorial clause directly applies to this parent company, thereby subjecting it to the provisions of the APPI.

Law stated - 1 January 2025

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency, Japan (IPA) have published the Cyber Security Management Guidelines (CMG). These guidelines summarise 'three principles' that management needs to be aware of and '10 important items' that should be directed to the chief information security officer (CISO).

In addition, the competent authorities that supervise the operations of critical social infrastructure providers (CSIPs) have issued guidelines concerning the CSIPs they supervise, outlining safety control measures for cybersecurity initiatives.

Law stated - 1 January 2025

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

The Japanese government has not implemented a system to incentivise cybersecurity enhancements.

Law stated - 1 January 2025

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The Japanese Industrial Standards have been established as the domestic standards in Japan equivalent to the standards of the International Organization for Standardization.

Further, METI and IPA have published the CMG and a collection of practices for its implementation of the CMG for cybersecurity. The three principles and 10 important items set forth by the CMG are outlined below, respectively.

The three principles that management should be aware of are as follows:

- Principle 1: management will promote measures under its own behest.
- Principle 2: attention must be paid to cybersecurity measures throughout the supply chain.
- Principle 3: proactive communication with stakeholders is necessary in both normal times and emergencies.

The 10 important items management should be aware of are as follows:

- Directive 1: recognise risks and develop an organisation-wide response policy.
- Directive 2: establish a risk management system.
- Directive 3: secure resources (budget, human resources, etc) for cybersecurity measures.
- Directive 4: identify risks and develop a plan in response to such risk.
- Directive 5: establish a mechanism to effectively respond to risks.
- Directive 6: continually improve cybersecurity measures through a plan-do-check-act cycle.
- Directive 7: establish an emergency response system in the event of an incident.

- Directive 8: establish a business continuity and recovery system in preparation for harm caused by incidents.
- Directive 9: assess the status of the entire supply chain and take countermeasures.
- Directive 10: promote the collection, sharing and disclosure of cybersecurity information.

Law stated - 1 January 2025

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

The CMG developed and published by METI and IPA also contain reference materials for incident response.

Moreover, businesses handling personal data are required to implement safety management measures outlined in the Guidelines Regarding the Act on the Protection of Personal Information, formulated under the Act on the Protection of Personal Information (APPI). In the event of a personal data breach, they must follow the procedures described in these guidelines.

Furthermore, the Japan Computer Emergency Response Team Coordination Center has issued an Incident Handling Manual to guide responses to incidents such as information leaks. Additionally, IPA has published a Security Incident Handling Manual specifically tailored for small and medium-sized enterprises.

For additional resources, the Japan Network Security Association, a non-profit organisation focusing on network security, maintains a list of security response providers and digital forensics companies that can offer assistance in the event of a cyber incident. This list serves as a valuable reference for businesses seeking support during such incidents.

Law stated - 1 January 2025

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Currently in Japan, there is no legal framework that provides incentives for sharing information on cybersecurity incidents. However, the Basic Act on Cybersecurity (BAC) led to the establishment of the Cyber Security Council, aimed at facilitating the prompt sharing of information to enhance cybersecurity.

In 2023, the Cyber Security Council issued the Guidance for Sharing and Publicizing Information on Cyber Attacks, aiming to promote information sharing in the event of cyberattacks. Moreover, in 2011, IPA initiated the Initiative for Cyber Security Information

Sharing Partnership of Japan (known as J-CSIP) as a platform for information exchange and early response, primarily among manufacturers of critical infrastructure equipment.

Law stated - 1 January 2025

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In general, when developing laws, regulations and guidelines, including those concerning cybersecurity, the Japanese government convenes a conference body made up of government and private-sector experts. These bodies formulate, publish and enforce regulations based on the outcomes of their deliberations.

For instance, the CMG and the collection of practices, which aid in implementing the directives outlined in the CMG, are crafted and published by METI and IPA. These documents are developed with the input of private-sector experts who participate as members of the study committee, incorporating the results of their discussions.

Law stated - 1 January 2025

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

In Japan, numerous insurance companies provide cyber insurance policies.

Law stated - 1 January 2025

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which was established as the secretariat of the Cybersecurity Strategy Headquarters under the Basic Act on Cybersecurity (BAC), is also tasked with formulating and operating the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP).

The competent authorities that oversee the CPCIP's operations, such as the Japan Financial Services Agency, the Minister of Internal Affairs and Communications (MIC), the Ministry of Health, Labour and Welfare, the Ministry of Economy, Trade and Industry and

the Ministry of Land, Infrastructure, Transport and Tourism, are tasked with developing and implementing cybersecurity guidelines for the businesses under their supervision.

By contrast, the National Police Agency and Public Prosecutor's Office possess criminal investigative authority over criminal acts, including cybercrimes. However, only the Public Prosecutor's Office has the authority to indict cybercrimes.

Law stated - 1 January 2025

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Under the BAC, NISC has the authority to request any person to provide materials, explanations or other cooperation as necessary to carry out its duties. These duties include investigations to determine the causes of serious cybersecurity events and the evaluation of countermeasures. However, such requests are voluntary, and a person who refuses to cooperate will not face any adverse consequences.

In addition, under the Act on the Protection of Personal Information (APPI), the Personal Information Protection Commission (PPC) is empowered to request reports from business operators handling personal information, request submission of documents and conduct on-site inspections. These actions are taken when there are concerns regarding safety management measures, including cybersecurity, implemented by such business operators.

Furthermore, each government agency possesses extensive administrative supervisory authority over businesses within its jurisdiction. For instance, MIC oversees telecommunications carriers, while the Ministry of Health, Labour and Welfare regulates pharmaceutical companies. Consequently, these administrative supervisory authorities may conduct investigations as needed, which may involve requesting reports and materials from businesses under their supervision, including matters related to cybersecurity.

Law stated - 1 January 2025

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

In 2024, numerous incidents of personal data breaches occurred due to cyberattacks including internal fraud and ransomware attacks, targeting companies that handle personal information. In response to this situation, the PPC has (1) emphasised that the companies responsible for the breaches handle significant volumes of personal information, (2) identified deficiencies in their safety management measures and their inadequate supervision of subcontractors regarding the personal information handling, both of which need to be appropriately taken under the APPI, and (3) issued guidance and other administrative measures against these companies.

Law stated - 1 January 2025

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Under the APPI, a business operator handling personal information is required to report an incident to the PPC within three to five days from identifying the incident and also to promptly notify the affected individuals if there is a breach of personal data (including leakage, loss or damage to personal data) or a threat of breach, and there is a risk of harm to individuals' rights and interests associated with the data. However, the PPC has delegated authority to the relevant authorities under the APPI, and such business operator must report to different parties depending on the type of business.

For example, banks and internet service providers are required to report personal data breaches to the Japan Financial Services Agency and MIC, respectively. Further, such business operators are generally required to report further details of the breach to the competent authorities within 30 days of learning about the personal data breach. In addition, under the Telecommunications Business Act (TBA), a telecommunications business carrier is required to 'promptly' report any incident of infringement of the secrecy of communications to the General Telecommunications Administration or the relevant authority having jurisdiction over the location of its headquarters. The carrier must also report additional details within 30 days of learning about the incident.

Law stated - 1 January 2025

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

In addition to the criminal penalties for the cyberactivities, violations of the safety control measures required under the APPI and other relevant laws and regulations such as the TBA may result in administrative penalties. These penalties can include business improvement orders against the violating business operator or the publication of the business operator's name by the relevant regulatory authorities.

Law stated - 1 January 2025

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

If there is a breach of personal data or a threat thereof, and there is a risk of harm to individuals' rights and interests associated with such data, a prompt report to the PPC and other relevant authorities is required, followed by a detailed report within a specified period. Additionally, notification to the affected individuals is also mandated. If the business operator handling personal information fails to meet these obligations, the PPC may request a report or conduct an on-site inspection of the business operator.

As a result of this investigation, the PPC may issue administrative guidance, recommendations or orders to the said business operator for improvement. If the said business operator makes a false report, refuses to report or fails to comply with the PPC's order, the business operator will be subject to criminal penalties.

If a telecommunications carrier fails to report a case or makes a false report in violation of the reporting obligation imposed on the said carrier when a case of infringement of the secrecy of communications occurs under the TBA, the telecommunications carrier will also be subject to criminal penalties.

Law stated - 1 January 2025

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

A lawsuit for damages may be possible based on tort law or for breach of contractual confidentiality obligations.

Law stated - 1 January 2025

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Personal Information Protection Commission (PPC) publishes security control measures that outline specific methods for business operators handling personal information, in accordance with the Act on the Protection of Personal Information (APPI) guidelines. However, these methods are provided as examples and are not mandatory. In Japan, certain business operators are required to implement safety control measures for cybersecurity pursuant to relevant laws and regulations. Nonetheless, there are no specific policies or procedures that organisations must put in place to comply with these safety control measures.

Law stated - 1 January 2025

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

In Japan, there is no explicit legal requirement mandating the retention of records, including logs, documenting cyberthreats and attacks. However, under the Basic Act on Cybersecurity (BAC), critical social infrastructure providers (CSIPs) are obligated to share information concerning cyberthreats and attacks with competent authorities, in accordance with the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP). Consequently, it is understood that CSIPs should maintain comprehensive records for a specified duration to facilitate the provision of such information and to address inquiries from competent authorities when deemed necessary.

Moreover, beyond entities covered by CSIPs, if a cyberattack leads to or is anticipated to result in an imminent breach of personal data, reporting to the PPC becomes obligatory. In such instances, the retention of information related to cyberthreats and attacks may be necessary to fulfil this reporting requirement adequately.

In addition, telecommunications service providers may be compelled by investigative agencies such as the National Police Agency, pursuant to the Act on Criminal Procedure, to maintain communication and other records pertaining to a specific individual or organisation for up to 60 days for criminal investigations. Consequently, it is customary for logs spanning this time frame not to be deleted.

Law stated - 1 January 2025

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Both the APPI and the Telecommunications Business Act (TBA) mandate expeditious reporting to the PPC or other competent authorities in the event that a breach or potential breach of personal data or an occurrence of the infringement of the secrecy of the communication meet specific criteria. It is important to note that this reporting requirement is triggered solely by the occurrence of a breach or the presence of a threat of breach or such occurrence, without necessitating an actual breach. Additionally, there exists no legal obligation for a company to report to authorities when it has experienced an attack that has not yet resulted in a breach or threat of breach or such occurrence, nor is there a requirement to report vulnerabilities to authorities.

Furthermore, the mandated report must encompass various details, including a summary of the incident, the nature of the leaked or potentially leaked information, pertinent information regarding affected individuals and the root cause of the incident, among other relevant information.

Law stated - 1 January 2025

Time frames

30 | What is the timeline for reporting to the authorities?

Under the regulations stipulated by the APPI, if a breach or a threat of breach of personal data occurs and there is a risk of harm to the rights and interests of individuals, business operators are obligated to expeditiously report the incident to the PPC or other relevant supervisory bodies within three to five days from the date of identifying the breach or potential threat. Further, they are generally required to provide an additional detailed follow-up report within 30 days of the initial identification date.

Under the TBA, a telecommunications carrier is required to 'promptly' report any incident of infringement of the secrecy of communications to the competent authority having jurisdiction over the location of its headquarters. The carrier must also report additional details within 30 days of learning about the incident.

Law stated - 1 January 2025

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

CSIPs defined under the BAC necessitate the dissemination of cyberthreat intelligence and information on cyberattacks to competent authorities, aligning with the guidelines set forth by the CPCIP.

Moreover, the APPI imposes distinct notification responsibilities on business operators handling personal data. Should there be a breach or a threat of breach of personal data meeting specific criteria, these operators are obligated to notify the individuals associated with said data.

Listed companies, as mandated by the Financial Instruments and Exchange Act, must disclose annual financial statements and related documents. These statements necessitate the comprehensive delineation of business risks, encompassing cybersecurity threats among them. Consequently, there has been a discernible uptick in the disclosure of cybersecurity risks by an expanding cohort of listed companies in recent years.

In cases of cybersecurity breaches such as information leaks, listed companies may find themselves obligated to promptly disclose the incident and their response measures, subject to meeting specific criteria outlined in the timely disclosure regulations established by each securities exchange. However, even if these criteria are not met, a listed company reserves the option to voluntarily disclose the security breach in a timely fashion.

Law stated - 1 January 2025

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The Personal Information Protection Commission (PPC) issued administrative guidance on 15 February 2024 in response to an incident involving a telecommunication carrier and significant volumes of personal information.

The telecommunications carrier had outsourced work related to its own internet service business, including the management of customer information for telemarketing, to a group company. A temporary worker at that group company at the time accessed a cloud service that he had a personal contract for without authorisation, using work PCs designated for managing the customer information related to the business. The temporary worker uploaded approximately 5.96 million pieces of personal information associated with the business to the cloud service, resulting in a data breach.

The carrier had assumed control of the business in this case following its merger with and acquisition of a group company. At the time of the succession, the telecommunications carrier had been aware of certain technical non-compliance issue with its established information management rules. These included unrestricted internet and email access on PCs used to handle customer information related to the business and lack of encryption for customer information. However, the carrier had faced challenges in taking immediate corrective action. Therefore, the carrier had permitted temporary exceptions to its rules, implementing alternative measures such as on-site self-inspections. During the period when the exceptions were in effect, the temporary worker engaged in the above misconduct.

In light of the above, it would be reasonable to advise companies contemplating the acquisition of a business that handles substantial volumes of personal information to conduct thorough due diligence regarding the target company's personal information and data management practices. They should also prepare to implement any necessary corrective measures post-acquisition based on the due diligence findings, considering the potential risk of administrative actions by the PPC.

Law stated - 1 January 2025

Yasushi Kudo yasushi_kudo@noandt.com
Tsubasa Watanabe tsubasa_watanabe@noandt.com
Hayato Maruta hayato_maruta@noandt.com

Nagashima Ohno & Tsunematsu

Netherlands

Robbert Santifort, **Ilham Ezzamouri**
Eversheds Sutherland

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The legal landscape for cybersecurity in the Netherlands can be divided into general and sectoral laws and regulations. The main general laws and regulations governing cybersecurity are as follows:

- Security of Network and Information Systems Act (Wbni): the Wbni implemented Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union (NIS Directive), aiming to enhance the Netherlands' digital resilience and prevent societal disruption caused by cyber incidents. Directive (EU) 2022/2555 (NIS2 Directive) came into force on 16 January 2023, requiring member states to transpose it into national legislation by 17 October 2024. The Netherlands missed this deadline, prompting the European Commission to initiate an infringement procedure. The NIS2 Directive will be implemented through the new Cybersecurity Act (Cbw), which will repeal the Wbni and is expected to come into force in the third quarter of 2025.
- Security of Network and Information Systems Decree (Bbni): introduced alongside the Wbni, the Bbni designates critical operators required to notify the National Cyber Security Centre (NCSC) of incidents. The Bbni and the Ministerial Regulation on network and information systems security (Regeling IenW) are expected to be repealed by the promulgation of new decrees that will supplement the Cbw to align with NIS2 requirements in more detail.
- Regulation (EU) 2019/881 (Cyber Security Act, CSA): the CSA is an EU regulation aimed at addressing cross-border cyberattacks more effectively. Its certification framework allows information and communication technology (ICT) products, services and processes to receive cybersecurity certification.
- Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA): on 10 October 2024, the Council of the European Union adopted the CRA, establishing cybersecurity requirements for products with digital elements. The regulation seeks to ensure the safety of digital products before they are introduced to the market.
- Regulation (EU) 2022/2554 (Digital Operational Resilience Act, DORA): DORA came into effect on 16 January 2023 and will apply from 17 January 2025. It aims to strengthen the IT security of financial entities, including banks, insurance companies and investment firms, ensuring the resilience of the financial sector during severe operational disruptions. DORA harmonises operational resilience rules for the financial sector, covering 20 types of financial entities and ICT service providers.
- Directive (EU) 2022/2557 (Critical Entities Resilience (CER) Directive): the CER Directive came into force on 17 October 2024, focusing on enhancing the resilience of critical entities that provide essential services. Member states are required to identify these entities by 17 July 2026. In the Netherlands, implementation of the

CER Directive has been delayed, with the Resilience of Critical Entities Act now expected to come into effect in the third quarter of 2025.

- Computer Crime Act III and Cybercrime Directive (2013/40/EU): these statutes empower the Dutch Public Prosecution Service and Police to effectively combat cybercrime in the digital realm.
- Temporary Cyber Operations Act: in March 2024, the Dutch Senate passed the Temporary Cyber Operations Act, expanding the powers of the General Intelligence and Security Service and the Military Intelligence and Security Service. The Act enables these agencies to respond more swiftly and effectively to cyberthreats posed by state actors. It aims to bolster the Netherlands' resilience against cyberattacks and includes temporary measures subject to evaluation for potential extension or amendment.
- EU Cybersecurity Certification Schemes: the European Union has introduced the EU Cybersecurity Certification Framework to ensure the security of ICT products, services and processes. Two key certification schemes under this framework are:
    - EU Common Criteria – based on international common criteria standards, this scheme provides a harmonised certification process for ICT products, such as hardware and software, allowing suppliers to demonstrate their products' cybersecurity under an EU-recognised standard; and
    - EU Cloud Services – focused on cloud services, this scheme is designed to evaluate and certify the cybersecurity of cloud service providers. Currently under development, the scheme aims to establish a uniform security standard for cloud services across the European Union.

Both schemes are voluntary, aiming to boost confidence in digital services while facilitating the free movement of ICT products and services within the European Union.

Law stated - 20 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In parallel with the impact of DORA for the financial sector, the NIS 2 Directive expands the scope of the NIS Directive to new sectors. These new sectors include space, postal and courier services, food, water waste management, public administration, managed (security) service providers, digital service providers and manufacturers of medical and electronic products and chemicals.

Results of the 'Cyber Security Assessment Netherlands 2024' (CSAN 2024) have shown an increasing interest from cyberactors in compromising operational technology (OT). This is, among others, due to the critical role OT plays in managing essential physical processes, such as the production and processing of raw materials, the purification of drinking water and the distribution of electricity. OT systems are foundational to these processes, making them attractive targets for malicious actors.

Large-scale failures or issues affecting the availability of OT systems could have severe consequences for Dutch society and the economy. These consequences include social unrest, significant economic damage and a decline of public confidence in digitalisation.

While there have been advancements in securing OT systems, CSAN 2024 highlights persistent challenges. These include the high costs associated with replacing or testing legacy systems, fragmented and incomplete information regarding vulnerabilities, and the potential risk of disrupting availability and interoperability during security upgrades.

The report further emphasises the growing interconnection between OT and IT systems, which increases the complexity of securing these environments and amplifies the potential impact of cyber incidents. Addressing these issues requires a coordinated and sustained effort to enhance the resilience of OT systems against evolving cyberthreats.

Law stated - 20 December 2024

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

The Netherlands has adopted the NEN-EN-ISO/IEC 27001:2023 standard, which aligns with the ISO/IEC 27001:2022 standard. This standard specifies requirements for establishing, implementing, maintaining and continually improving an information security management system. It replaces the earlier NEN-EN-ISO/IEC 27001:2017 version. However, there is no explicit evidence that this standard is obligatory for Dutch governmental institutions under a 'comply or explain' policy. The Baseline Information Security Government serves as the framework for information security within Dutch governmental institutions, aligning with international standards such as NEN-ISO/IEC 27001:2017 and NEN-ISO/IEC 27002:2017.

The healthcare sector in the Netherlands adheres to the NEN 7510 series, specifically NEN 7510-1:2017+A1:2020, which outlines information security requirements tailored for health data. These standards address the unique regulatory and operational challenges associated with safeguarding sensitive health information, ensuring that healthcare organisations implement robust security measures while maintaining patient safety and data privacy.

Beyond healthcare, various ISO and NEN standards are recognised as best practices across multiple sectors. While compliance with these standards may not be mandatory, regulators strongly encourage their adoption. Organisations in industries such as finance, energy and transport increasingly utilise standards such as ISO/IEC 27001 and ISO/IEC 62443 (for industrial control systems) to mitigate cybersecurity risks and ensure operational continuity. The implementation of these standards plays a key role in strengthening the Netherlands' digital infrastructure.

By ensuring adherence to internationally recognised frameworks, the Netherlands bolsters its cybersecurity position and enhances the resilience of its critical sectors, including public administration, digital service providers and energy networks.

In summary, the Netherlands demonstrates a strong commitment to cybersecurity standards through the adoption and implementation of both international and sector-specific frameworks. While the adoption of NEN-EN-ISO/IEC 27001:2023 reflects alignment with international advancements, its obligatory status for governmental institutions under a comply or explain policy is not explicitly confirmed. The healthcare sector continues to adhere to the NEN 7510 series, ensuring the protection of sensitive health information. Other sectors are encouraged to adopt relevant standards to mitigate cybersecurity risks and ensure operational continuity.

Law stated - 20 December 2024

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

For those entities covered under the NIS2 Directive (subject to implementation in the Cybersecurity Act in the Netherlands), article 20 of the NIS2 Directive stipulates that management bodies of essential and important entities should approve the cybersecurity risk management measures (see below) and are held responsible in this respect. Management bodies are furthermore required to follow training, and offer similar training to their employees on a regular basis, in order to gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity.

Article 21 of the NIS2 Directive outlines a set of measures for managing cybersecurity risks that essential entities (encompassing public and private companies in sectors such as transportation, finance, energy, water, space, health, public administration and digital infrastructure) and important entities (including companies in sectors such as food, digital providers, chemicals, postal services, waste management, research and manufacturing) must undertake to protect their networks and information systems. These measures encompass incident handling, business continuity and crisis management, basic practices of cyber hygiene, and policies and procedures regarding the use of encryption.

Natural persons who are responsible for or act as legal representatives of essential entities, possessing the authority to make decisions, represent the entity or exercise control over it, are entrusted with ensuring the entity's compliance with the Directive. These individuals bear a duty of care to guarantee that the essential entity complies with the requirements of the Directive. Failure to fulfil this duty may result in liability for breach of these responsibilities.

For DORA, see article 5 of the Cybersecurity Act.

Law stated - 20 December 2024

Key definitions

5 How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

The NCSC and the National Coordinator for Security and Counterterrorism (NCTV) define 'cybersecurity' as the ensemble of measures aimed at reducing relevant risks to an acceptable level. These measures focus on preventing cyber incidents and, when such incidents occur, detecting them, mitigating damage and facilitating recovery. Determining what constitutes an acceptable level of risk is the result of a comprehensive risk assessment.

According to the NCTV, cybercrime encompasses a wide range of illicit activities conducted through digital means. Common forms include:

- phishing – crafting fraudulent emails to extract personal information from users;
- identity theft – misappropriating personal data for unauthorised use;
- hacking – gaining unauthorised access to disrupt or exploit websites or computer networks;
- dissemination of extremist content – spreading hate speech or inciting terrorism;
- distribution of child pornography – circulating illegal content involving minors; and
- grooming – engaging minors online with the intent of sexual exploitation.

The pervasive connectivity of digital devices such as computers, tablets and smartphones to the internet amplifies the potential impact of cybercrime. The NCTV emphasises that cybercriminals have the capability to significantly disrupt Dutch society, potentially bringing critical sectors to a standstill. Recognising this threat, the Dutch government actively combats cybercrime through stringent measures and policies.

In recent years, the Netherlands has intensified its focus on improving cybersecurity and combating cybercrime. The 'Cybersecurity Assessment Netherlands 2024' (CSBN 2024) highlights the increasing complexity and interconnectivity of digital risks, which can lead to unforeseen and disruptive effects, thereby elevating risks to national security. The report advocates for a comprehensive approach to risk management to address these digital threats effectively.

Additionally, the 'Netherlands Cybersecurity Strategy 2022-2028' outlines the country's commitment to enhancing digital resilience across government, businesses and societal organisations. This strategy emphasises the importance of secure and innovative digital products and services, countering digital threats from state and non-state actors and strengthening the cybersecurity workforce and education.

Through these initiatives, the Netherlands aims to foster a secure digital environment, enabling society to fully benefit from digitalisation while safeguarding against the evolving landscape of cyberthreats. By prioritising cybersecurity, the country bolsters its resilience and ensures its ability to adapt to emerging challenges in the digital realm.

Law stated - 20 December 2024

Mandatory minimum protective measures

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

According to the NCSC, the following basic measures should be taken by every organisation to counter cyberattacks as recent digital incidents have shown that not taking these measures leaves organisations vulnerable:

- ensure every application and system generates sufficient log information;
- apply multi-factor authentication where necessary;
- determine who has access to data and services;
- segment networks;
- encrypt storage media containing sensitive business information or trade secrets;
- check which devices and services are accessible from the internet and protect them;
- regularly back up and test systems; and
- install software updates.

See the cybersecurity risk management measures of article 21 for those entities covered under the NIS2 Directive.

Law stated - 20 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The Netherlands has no laws or regulations that expressly address cyberthreats to intellectual property (IP). However, it is essential to recognise the potential risks posed by cybercriminals who may engage in activities such as the illicit acquisition of IP (including trade secrets) through hacking, often concealing their true motives behind ransomware tactics. The Dutch Trade Secrets Act states that 'reasonable measures' should be taken to protect its confidentiality in order to consider information a trade secret.

Despite the absence of dedicated legislation, legal recourse is available for victims of cyberthreats to IP. Individuals or entities whose IP, such as trade secrets or copyrighted material, has been compromised can leverage existing legal frameworks. For instance, the Trade Secrets Act and the Dutch Copyright Act provide avenues for legal action in cases where protected and valuable trade information or, for example, the source code of software is unlawfully accessed or stolen.

In addition to IP-specific legislation, victims may also pursue legal remedies based on charges related to computer intrusion. The Dutch Criminal Code, under article 138ab, addresses computer hacking, defining it as the intentional and unlawful intrusion into a computerised system. Perpetrators engaging in such activities are subject to punishment, reinforcing the legal consequences for those involved in unauthorised access to computer systems with the intent to compromise IP.

Lastly, the Netherlands is a signatory to international agreements, including the Convention on Cybercrime (Budapest Convention), underlining its dedication to combating cyberthreats across a range of areas, including IP protection. Adopted in 2001, the

Budapest Convention establishes an international framework aimed at harmonising legal approaches, enhancing investigative capabilities and fostering cross-border cooperation in addressing cybercrime. The Convention is particularly relevant to IP-related cybercrime as it covers offences such as unauthorised access, data interference and copyright infringement. These provisions enable measures to counteract threats such as the theft of trade secrets, unauthorised access to source code and other violations involving protected materials.

Law stated - 20 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Wbni, alongside the Bbni and Regeling IenW, focuses on enhancing the cybersecurity and resilience of critical infrastructure in the Netherlands. National laws – the Cbw for the NIS2 Directive and the Critical Entities Resilience Act (Wwke) for the CER Directive – are now expected to come into effect in the third quarter of 2025 and repeal existing decrees and regulations.

Law stated - 20 December 2024

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Police Data Act and the Criminal Data Act collectively govern the procedures and parameters associated with accessing data and communication in the pursuit of criminal prosecution. The Computer Crime Act III, which came into force on 1 March 2019, expanded the investigative powers of law enforcement agencies, particularly in the area of cybercrime. A significant addition was the authority granted to specially authorised investigators to covertly and remotely gain access to automated systems (hacking) with the objective of:

- identifying users or obtaining information about the system's configuration;
- intercepting communications transmitted through or stored on the targeted system;
- monitoring activities on the system over an extended period;
- copying or preserving data for investigative purposes; and
- removing or blocking harmful or illegal information.

These powers are deemed essential to address the complexities of both online and offline criminal activities.

A 2022 evaluation conducted by the Scientific Research and Documentation Centre concluded that the Dutch National Police has laid a solid foundation for a robust quality monitoring system to ensure these powers are exercised within legal boundaries. However, challenges such as limited capacity remain. A second evaluation report, which will assess the law's full implementation, is expected by the end of 2024.

In March 2023, a bill was introduced to establish a new Code of Criminal Procedure, aiming to modernise procedural laws and better align them with today's digital realities. The proposed code is expected to take effect on 1 April 2029, provided the legislative process proceeds on schedule.

Law stated - 20 December 2024

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

- Article 138ab of the Dutch Penal Code criminalises the intentional and unlawful intrusion into an automated system. This includes unauthorised access to computer systems, networks or databases. The Computer Crime Act III also specifically addresses hacking for the purpose of digital theft or using computers as listening or espionage devices.
- Articles 139c and 139d of the Penal Code prohibit the intentional and unlawful interception or recording of non-public communications, such as telephone conversations or digital data streams.
- Article 350a criminalises the intentional and unlawful destruction, damage, disabling or alteration of data stored in an automated system.
- The production, dissemination or provision of malicious software, such as viruses or malware, with the intent to cause harm, is punishable under various articles related to unauthorised access and sabotage. Specifically, article 139d addresses the creation and dissemination of tools used for unauthorised access.
- While there is no specific article addressing identity fraud, such acts can be prosecuted under offences such as fraud (article 326) and forgery (article 225).
- The creation, distribution, possession or access to child pornography is criminalised under article 240b of the Penal Code.
- Article 248e makes it an offence to use electronic communication to arrange meetings with minors for the purpose of sexual abuse. The Computer Crime Act III reinforces these provisions with specific measures targeting such behaviour.
- Since 1 January 2024, it is illegal to disseminate personal data with the intent to intimidate or harass someone. Offenders may face a prison sentence of up to two years or a fine in the fourth category. This legislation was introduced to provide better protection for victims of doxing (ie, the action or process of searching for and publishing online private or identifying information about a particular individual).
-

The Computer Crime Act III includes provisions that allow undesirable photographs or videos to be taken offline by court order. This mechanism is intended to protect individuals from harm caused by the unauthorised sharing of sensitive or damaging content.

Law stated - 20 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Cloud computing service providers are now explicitly in scope of the NIS2 Directive and the forthcoming Cyber Security Act. The Dutch government also revised its policy on cloud services for public institutions to address modern security and operational needs as follows:

- Expansion of permissible cloud services: public cloud services are now allowed, in addition to private cloud options, provided they meet stringent security requirements.
- Cybersecurity standards:
    - Providers must adhere to NIS2 security requirements, including incident reporting and risk management.
    - Certain cloud providers from high-risk countries are explicitly excluded based on geopolitical and cybersecurity considerations.
- Information categorisation:
    - All data must be categorised based on sensitivity to determine the appropriate cloud environment (public or private).
    - Highly sensitive data, particularly related to national security, is restricted from being processed or stored in public cloud environments.
- Cloud providers operating in the Netherlands face new responsibilities under these regulations:
    - Implementation of risk analysis procedures and secure data lifecycle management.
    - Compliance with stringent monitoring requirements and incident reporting obligations within defined time frames.
    - Alignment with both EU and Dutch cybersecurity standards to maintain operational legitimacy.

Law stated - 20 December 2024

Foreign organisations

.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations conducting business in the Netherlands are subject to the same set of cybersecurity laws and regulatory obligations as their Dutch counterparts. The legal framework is designed to create a level playing field, ensuring that all entities, regardless of their origin, adhere to the established cybersecurity laws. It is essential for foreign organisations to familiarise themselves with the specific cybersecurity laws and regulations applicable in the Netherlands to ensure compliance with the established standards. This equal treatment underscores the commitment of the Dutch authorities to create a secure and resilient digital landscape, irrespective of the organisational origin.

Law stated - 20 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In 2022, the Dutch government's National Cyber Security Centre (NCSC) published 'The Netherlands Cybersecurity Strategy 2022–2028', which provides for high-level and general policy initiatives.

The NCSC serves as the cybersecurity expertise centre in the Netherlands. When faced with threats and responsibilities, the NCSC issues security advice to organisations. The NCSC also provides guidance to the Dutch government and essential organisations on how to better protect themselves from digital threats by way of sharing information sheets, guidelines and handouts. The website veilginternetten.nl and the Alert Online campaign provide the public with tips on safe internet usage.

Law stated - 20 December 2024

Government incentives

14 How does the government incentivise organisations to improve their cybersecurity?

The Dutch government has reaffirmed its commitment to strengthening cybersecurity by significantly increasing investments in digital resilience and security in recent years. These investments aim to combat cybercrime effectively and enhance the country's overall digital security. To support organisations in their cybersecurity efforts, the government offers various grants and funding opportunities that have been updated and expanded.

REACT-EU (Recovery Assistance for Cohesion and the Territories of Europe) was established to address the economic impact of the covid-19 pandemic, providing additional funding to existing European Regional Development Fund and European Social Fund

allocations. These Funds were intended to be utilised until the end of 2023. Therefore, as of December 2024, REACT-EU is not an active funding source for new cybersecurity projects.

The Cybersecurity Innovation FundCIF-NL, managed by the Netherlands Enterprise Agency RVO, offers grants to Dutch companies and research organisations for developing cybersecurity solutions. In 2023, the Fund had a budget of €930,000, with grants ranging from €25,000 to €75,000 per project. The application period for this funding was from 2 October to 2 November 2023. There is no publicly available information indicating that the scope of this Fund was expanded in 2024 to include projects focusing on artificial intelligence-driven cybersecurity tools.

The Digital Trust Centre (DTC), part of the Ministry of Economic Affairs and Climate Policy, supports partnerships between businesses in non-essential sectors through various grant schemes. While the DTC has prioritised projects focusing on cross-sector collaboration and scalable solutions, specific details about grants of up to €250,000 for initiatives providing long-term cybersecurity improvements in 2024 are not corroborated by available sources. Additionally, while the DTC offers support for small enterprises, information regarding funding for projects focusing on advanced threat intelligence sharing and securing supply chains in 2024 is not specified in the available data.

'The Netherlands Cybersecurity Strategy 2022-2028' outlines the government's approach to enhancing digital resilience across various sectors. However, there is no specific information available about the launch of a National Cybersecurity Collaboration Programme in 2024 that provides grants for developing technologies related to cyberthreat prediction, secure cloud computing and post-quantum cryptography.

Recognising the challenges SMEs face in implementing robust cybersecurity measures, the Dutch government has introduced funding streams, including grants for cybersecurity audits, training programmes and tools designed to address specific vulnerabilities. The focus is on developing scalable solutions that can be adopted across similar organisations, ensuring that smaller businesses can enhance their cybersecurity posture.

Law stated - 20 December 2024

Industry standards and codes of practice

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In the Netherlands, NEN-EN-ISO/IEC 27001:2023, the Dutch adaptation of ISO/IEC 27001 published on 1 August 2023, serves as the primary standard for information security, providing a robust framework for establishing, implementing, maintaining and improving an information security management system. While this standard ensures the confidentiality, integrity and availability of sensitive business information, organisations may need to adopt additional controls or standards to comprehensively address cybersecurity and privacy protection. In the financial sector, De Nederlandsche Bank (DNB) has issued the 'Good Practice Information Security 2023', a guideline tailored for institutions under its supervision to manage information security risks effectively. This aligns with EU regulations, such as those from the European Insurance and Occupational Pensions Authority, and addresses

the evolving cyberthreat landscape. Additionally, the Threat Intelligence-Based Ethical Red Teaming (TIBER-NL) programme, led by the DNB's Cyber Unit, strengthens the resilience of financial institutions by simulating cyberattacks, enabling organisations to test their defences and improve overall readiness. While NEN-EN-ISO/IEC 27001:2023 is applicable across industries, sector-specific frameworks such as the DNB's guidelines and TIBER-NL focus on the financial sector. Organisations in other industries should consult their respective regulatory bodies for guidance on cybersecurity and information security.

Law stated - 20 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

In 2024, the NCSC reinforced the importance of organisations maintaining robust incident response plans to effectively address cyber incidents, such as ransomware attacks. Recognising that every incident and organisation is unique, the NCSC emphasises that a well-structured incident response plan is essential for initiating prompt action, mitigating damage and enhancing overall cyberresilience. Key recommendations include integrating comprehensive cybersecurity measures into continuity management plans, such as maintaining regularly tested and verified backup facilities to ensure data integrity and confirm they are free from malware or unauthorised encryption. Organisations are also advised to conduct full restoration tests of systems or data volumes to establish realistic recovery times and validate the effectiveness of restoration processes under real-world conditions. Additionally, the NCSC highlights the importance of regularly reviewing and updating incident response plans to align with evolving cyberthreats and organisational changes. Recent developments include the publication of the guide '*Incidentresponse: waar begin ik?*' in October 2024, which provides practical steps for organisations to formulate and refine their incident response strategies, and the findings of 'Cybersecurity Assessment Netherlands 2024', which underscore the growing complexity of digital threats and the need for advanced risk management measures. By adopting these practices and adhering to the latest guidance, organisations can strengthen their preparedness, minimise disruptions and safeguard critical systems and data in an increasingly volatile digital landscape.

Law stated - 20 December 2024

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

In the Netherlands, several public-private initiatives facilitate the voluntary sharing of information about cyberthreats. A key example is the Electronic Crimes Taskforce (ECTF), a collaborative effort involving the Netherlands Police, ABN AMRO, ING, Rabobank, the Dutch Banking Association, the Public Prosecution Service and the Centre for Protection of National Infrastructure. Operational since 2011, the ECTF focuses on tactical-level

information sharing concerning (financial) cybercrime, aiming to strengthen the intelligence capabilities of all partners and develop innovative intervention strategies. The taskforce is hosted by the Dutch National Police, leveraging its organisational, technical and communication resources.

Other significant initiatives include the Financial Intelligence Unit Netherlands, the Schiphol Public Security Platform, the Information Sharing and Analysis Centres and the National Detection Network. Additionally, entrepreneurs can engage with the DTC, which supports businesses in improving their digital resilience. The DTC encourages collaboration within and between sectors, regions and industries, offering information and advice to bolster cybersecurity. It also disseminates two types of cyberalerts: general information on severe vulnerabilities in widely used enterprise software and ICT systems, and company-specific threat notifications.

Recent developments highlight an increased focus on thematic calls for public-private collaboration. In early 2024, the Netherlands Organisation for Scientific Research launched five new calls under the Mission-Driven Knowledge and Innovation Covenant programme. These calls address societal challenges, including the development of data structures for the energy transition and influencing consumer behaviour for a circular economy. These initiatives aim to foster impact-driven research through consortia comprising knowledge institutions, businesses and societal organisations, further enhancing collaboration and information sharing on cyberthreats.

Law stated - 20 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In the Netherlands, the collaboration between the government and the private sector in developing cybersecurity standards and procedures has been further strengthened through recent initiatives. In May 2024, the Dutch government introduced the draft Cybersecurity Act. This legislation seeks to enhance cybersecurity resilience across various sectors by establishing clear guidelines and standards, developed in consultation with both public and private stakeholders.

Additionally, the 'International Cyber Strategy of the Netherlands 2023–2028', published in September 2023, outlines the country's commitment to international cooperation in the cyber domain. This strategy emphasises the importance of public-private partnerships in developing and implementing effective cybersecurity measures, recognising that collaboration is essential to address the evolving cyberthreat landscape.

These developments build upon existing frameworks, such as the 'Netherlands Cybersecurity Strategy 2022–2028' and the Cyber Security Council, and initiatives by the NCSC and the DTC, which continue to play pivotal roles in fostering collaboration between the government and private sector to enhance the nation's cybersecurity position.

Law stated - 20 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Cybersecurity insurance has been available in the Netherlands since the early 2000s, marking its presence as a crucial risk mitigation tool in the evolving digital landscape. Over the past two decades, the cybersecurity insurance market in the country has evolved into a mature and well-established sector. It has become a standard policy offering, reflecting the recognition of the pervasive and evolving nature of cyberthreats.

Most cybersecurity insurance policies in the Netherlands are designed to provide comprehensive coverage on a cyber incident basis, addressing both first-party and third-party damages. First-party coverage protects the policyholder against damages resulting from a cyber incident directly affecting their organisation. By contrast, third-party coverage extends protection to damages incurred by external entities as a consequence of a cyber incident for which the policyholder is held accountable.

These insurance policies typically offer a range of coverage, including incident-response services aimed at effectively managing and mitigating the aftermath of a cyber incident. These services often include IT-forensic research, legal expertise and public relations support. The inclusion of incident-response services underscores the proactive approach taken by insurers to help organisations respond promptly and effectively to cyberthreats.

Moreover, cybersecurity insurance policies commonly cover damages arising from criminal activities or fraud, addressing the financial impact of incidents such as ransomware attacks and digital theft. This coverage ensures that organisations have financial protection in place to navigate the potentially devastating consequences of cybercriminal activities.

The prevalence of cybersecurity insurance has grown significantly, making it an integral component of risk management strategies for organisations across various industries. As the frequency and sophistication of cyberthreats continue to increase, cybersecurity insurance has become a critical tool for businesses to mitigate the financial and reputational risks associated with cyber incidents.

Law stated - 20 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The primary regulatory authority responsible for enforcing cybersecurity rules in the Netherlands is the Dutch Digital Infrastructure Authority (Rijksinspectie Digitale Infrastructuur, RDI). The RDI plays an important role in safeguarding the availability, continuity and reliability of the digital infrastructure within the country. Established to

address the evolving challenges of the digital landscape, the RDI operates at the intersection of legislative guidance, independent oversight and impartial enforcement.

One of the key functions of the RDI is to provide guidance and recommendations to the Dutch legislator regarding laws and regulations related to cybersecurity. This advisory role ensures that the legislative framework remains adaptive and effective in addressing emerging cyberthreats. The RDI's insights contribute to the development of policies that promote a secure and resilient digital environment for businesses, organisations and the broader society.

In addition to its advisory role, the RDI is vested with the authority to enforce and supervise compliance with cybersecurity rules. This encompasses overseeing adherence to information security standards, ensuring that organisations and entities operating within the digital realm comply with established protocols and measures. The enforcement activities of the RDI are characterised by independence and impartiality, emphasising a commitment to fair and equitable treatment in the pursuit of cybersecurity objectives.

By actively engaging in enforcement and supervision, the RDI seeks to create a robust cybersecurity ecosystem. This involves monitoring and assessing the implementation of information security standards, identifying potential vulnerabilities and taking corrective actions when necessary. The overarching goal is to enhance the overall cyberresilience of the nation's digital infrastructure.

Law stated - 20 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Despite the absence of implementation law in the Netherlands, based on Directive (EU) 2022/2555 (NIS2 Directive), the following applies: competent authorities, in their supervisory role concerning 'essential entities', possess a range of powers to monitor compliance, conduct investigations and prosecute infringements related to cybersecurity; these powers include on-site inspections and off-site ex post supervision conducted by trained professionals, as well as regular and targeted security audits carried out either by an independent body or the competent authority; and ad hoc audits may be initiated, especially in response to a significant incident or an infringement of the Directive by the essential entity.

Competent authorities, in the execution of their supervisory responsibilities concerning 'important entities', are empowered to apply a range of measures, including on-site inspections and off-site ex post supervision conducted by trained professionals, targeted security audits performed by an independent body or a competent authority and security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria. Cooperation with the concerned entity may be necessary for security scans. Furthermore, authorities have the right to request information for assessing cybersecurity risk management measures adopted by the entity, including documented cybersecurity policies and compliance with the obligation to submit information.

They also have the authority to request access to data, documents and information essential for carrying out their supervisory tasks, as well as evidence demonstrating the implementation of cybersecurity policies, such as the results of security audits conducted by a qualified auditor and the underlying evidence.

Law stated - 20 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Various enforcement issues have emerged prior to the implementation of the NIS2 Directive The most common issues were:

- insufficient cyberresilience – many businesses struggled to meet the required cybersecurity standards, leading to inconsistent resilience across sectors and member states;
- inconsistent incident reporting – there were variations in how and when incidents were reported, leading to delays and inefficiencies in response;
- lack of joint crisis response – coordination between member states and businesses was often lacking, hindering effective crisis management;
- limited focus on the cybersecurity of supply chains, leaving vulnerabilities unaddressed; and
- leadership accountability – cybersecurity was often not a priority at the executive level.

The NIS2 Directive addresses these issues, which should enhance the overall cybersecurity position and resilience of organisations across the European Union, ensuring they are better prepared to handle evolving cyberthreats. It also introduces harmonised penalties across the European Union, with fines up to €10 million or 2 per cent of a company's global annual turnover for non-compliance.

Meanwhile the RDI and the NCSC are publishing more enhanced guidelines and provide support to help organisations comply with the various EU directives.

Also in the private sector, we see improved cybersecurity measures, with companies investing in advanced security technologies, regular system updates and employee training to meet evolved international standards. Organisations are also developing and refining incident response protocols to ensure rapid and effective responses to cyber incidents, while conducting thorough evaluations of their supply chains to mitigate risks associated with third-party providers.

Law stated - 20 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Based on the NIS2 Directive, which has yet to be implemented in the Netherlands, we can conclude the following: essential and important entities have an obligation to promptly report any significant incident to the competent national authorities, including the national Computer Security Incident Response Team (CSIRT) (in the Netherlands, the NCSC); a 'significant incident' is defined as one capable of causing serious operational disruption or financial losses in the specified sectors or subsectors, or inflicting considerable material or non-material damage on other individuals or entities; and the reporting process involves the following stages:

- early warning – to be submitted no later than 24 hours after learning of the incident, providing minimal information such as the potential spread to other sectors or abroad and any suspected malicious intent;
- complete incident report – to be filed within 72 hours of learning about the incident, offering comprehensive details;
- interim or progress reports – these may be requested by the national CSIRT, providing updates as necessary during the incident; and
- final report – to be submitted within one month of the incident report.

If the incident is ongoing after one month, an interim report is expected at that point, followed by a final report once the incident concludes.

In cases where contractually committed to do so, entities should promptly notify their customers of significant incidents that could adversely affect their services. Additionally, beyond mandatory reporting, both essential and important entities have the option to voluntarily submit reports on non-significant incidents, cyberthreats and prevented incidents. This option also extends to entities outside the essential and important categories, regardless of whether they fall within the Directive's scope.

Law stated - 20 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

While specific penalty guidelines have not yet been established in the Netherlands, the NIS2 Directive provides clear indications regarding the sanctions that may be imposed for non-compliance with regulations aimed at preventing cybersecurity breaches. This Directive addresses both essential and important entities.

Essential entities, encompassing public and private companies in sectors such as transportation, finance, energy, water, space, health, public administration and digital infrastructure, may face fines up to €10 million or 2 per cent of their global annual revenue, whichever is higher.

Important entities, including companies in sectors such as food, digital providers, chemicals, postal services, waste management, research and manufacturing, could incur fines up to €7 million or 1.4 per cent of their global annual revenue, again dependent on whichever amount is greater.

The specific penalty levels, established as a percentage of the global annual revenue, underscore the seriousness of non-compliance with cybersecurity regulations, with higher fines applicable to essential entities compared to important entities. The penalty framework is designed to act as a deterrent, encouraging organisations to implement adequate measures to safeguard their networks and data against potential cyberthreats.

Law stated - 20 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In expectation of the fining policy rules of the RDI, based on the NIS2 Directive, the penalties would be similar to those for non-compliance (see above).

Law stated - 20 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Private redress for unauthorised cyber activity or failure to adequately protect systems and data in the Netherlands is primarily sought through civil law actions. The Dutch legal system provides avenues for parties to address such issues, drawing on principles established in the Dutch Civil Code.

One approach to seeking redress is through civil actions grounded in the concept of wrongful acts. Individuals or entities adversely affected by unauthorised cyber activity can initiate legal proceedings, alleging that the responsible party committed a wrongful act. In this context, a wrongful act refers to any action or omission that causes harm or damage to another party. By pursuing a claim under the Dutch Civil Code based on a wrongful act, the aggrieved party seeks compensation for the losses incurred due to the unauthorised cyber activity.

Another avenue for seeking private redress is through claims based on the breach of contract. In situations where there is a pre-existing contractual relationship between parties, the failure to adequately protect systems and data may constitute a breach of the terms and conditions outlined in the contract. Parties affected by such breaches can file legal actions to claim damages for the breach of contract, holding the responsible party accountable for failing to fulfil its contractual obligations related to cybersecurity.

These civil law actions provide a framework for individuals and organisations to seek compensation for the financial, reputational or other losses suffered as a result of unauthorised cyber activity or inadequate protection of systems and data. The legal system in the Netherlands allows for the pursuit of remedies through the courts, where judges evaluate the evidence and legal arguments presented by the parties involved.

It is important to note that the specific circumstances of each case may influence the choice of legal actions, and parties may choose to pursue multiple legal avenues simultaneously.

Law stated - 20 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Under Directive (EU) 2022/2555 (NIS2 Directive) and its Dutch implementation in the forthcoming Cybersecurity Act, organisations must implement several key policies and procedures to protect their data and IT systems from cyberthreats. Here are some of the main requirements:

- Risk management: organisations must conduct regular risk assessments and establish security policies for their information systems.
- Incident handling: there should be clear procedures for managing and responding to security incidents, including crisis management and vulnerability disclosure.
- Corporate accountability: management must oversee and approve cybersecurity measures, ensuring they are trained to address cyberrisks.
- Reporting obligations: organisations must have processes for promptly reporting significant security incidents, with specific notification deadlines.
- Business continuity: plans must be in place to ensure business continuity during and after major cyber incidents, including system recovery and emergency procedures.
- Supply chain security: security protocols must be established for the procurement and operation of systems, including assessing the security of suppliers.
- Access control and encryption: policies for access control, the use of cryptography and encryption must be implemented to protect sensitive data.
- Employee training: regular cybersecurity training and basic computer hygiene practices should be enforced for all employees.

These measures aim to enhance the overall cybersecurity position of organisations and ensure they are better prepared to handle cyberthreats.

Law stated - 20 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The key rules around record keeping of cyberthreats or attacks are in the context of the NIS2 Directive are as follows:

- Incident reporting: organisations must report significant cybersecurity incidents within 24 hours of detection, followed by a detailed report within 72 hours. This ensures timely communication and allows for swift response and mitigation.
- Record keeping: organisations are required to keep comprehensive records of all cybersecurity incidents, including the nature of the threat, the impact on their systems,and the measures taken to address the incident. These records must be maintained for a specified period to facilitate audits and reviews by regulatory authorities.
- Documentation of risk assessments: regular risk assessments must be documented, detailing identified vulnerabilities, potential impacts and the steps taken to mitigate these risks. This documentation helps in understanding the evolving threat landscape and improving security measures over time.
- Supply chain security: records of cybersecurity assessments and measures related to third-party suppliers and service providers must also be maintained. This ensures that the entire supply chain adheres to the required security standards.

Law stated - 20 December 2024

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The Dutch Cyber Security Act implementing the NIS2 Directive is not into effect yet, therefore the Security of Network and Information Systems Act, known as Wbni, still applies. Vital providers and providers of essential services have a reporting obligation to the National Cyber Security Centre when serious incidents occur. From 17 October 2024, other organisations can voluntarily report an NIS2 incident via this form.

Under the NIS2 Directive, reportable 'significant incidents' are defined as those causing severe operational disruption to services, leading to financial losses for the organisation and having the potential to inflict substantial material or non-material harm on individuals or entities. This reporting obligation encompasses incidents that pose a tangible threat to the organisation's operations and may have repercussions for a broader ecosystem.

Additionally, the Computer Security Incident Response Team (CSIRT), or the competent authority where applicable, is obligated to report incidents to the European Union Agency for Cybersecurity (ENISA) every three months, providing anonymised information. ENISA, utilising this collective data, will subsequently issue comprehensive reports every six months on incidents across the European Union.

Law stated - 20 December 2024

Time frames

30 What is the timeline for reporting to the authorities?

The NIS2 Directive has introduced a revised timeline for incident reporting, requiring essential and important entities to promptly notify any incident with significant impact without undue delay. Within the initial 24 hours, an early warning, along with preliminary presumptions regarding the nature of the incident, must be communicated to the CSIRT or competent authority. Following this, a comprehensive notification report, encompassing the incident assessment, severity, impact and indicators of compromise, is mandated to be submitted within 72 hours. A final report, summarising the incident's details, is required to be communicated after one month. Updates are to be provided for ongoing incidents.

Law stated - 20 December 2024

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, the supervisory authorities may, after consulting the organisation concerned, inform the public about the significant incident or require the organisation to do so.

Additionally, organisations may submit notifications to the supervisory authorities in respect of incidents, cyberthreats and near misses on a voluntary basis. This aims to collectively leverage the individual knowledge and practical experience of the organisation in order to enhance cybersecurity risk management.

Law stated - 20 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Developing effective cybersecurity regulations in the Netherlands presents several challenges, including the rapid pace of technological advancements, the evolving nature of cyberthreats and the necessity for harmonisation with EU directives. The implementation of Directive (EU 2022/2555) (NIS2 Directive) and the proposed Cyber Resilience Act (EU) 2022/2557 exemplify the European Union's commitment to enhancing cybersecurity across member states. However, aligning national regulations with these directives requires

significant effort and coordination. Additionally, the Critical Entities Resilience Directive and the Digital Operational Resilience Act (Regulation EU) 2022/2554, known as DORA) introduce further complexities, necessitating that organisations adapt to a multifaceted regulatory environment.

Companies can play a pivotal role in shaping a favourable regulatory landscape by actively engaging with regulatory authorities and participating in public consultations. By implementing robust cybersecurity best practices and collaborating with industry peers, organisations can contribute valuable insights that inform the development of practical and effective regulations. Engagement through industry associations and public-private partnerships facilitates a collaborative approach to cybersecurity, ensuring that regulations are both comprehensive and adaptable to emerging threats.

Looking ahead, the cybersecurity regulatory framework in the Netherlands is poised for significant transformation. The Dutch government has introduced a draft Cybersecurity Act. This legislation will impose enhanced cybersecurity obligations on essential and important entities, including stringent security measures and incident reporting requirements. Organisations must proactively prepare for these changes by aligning their cybersecurity strategies with the forthcoming legal requirements.

Lastly, predicting specific changes in cybersecurity laws and policies over the next year in a particular jurisdiction is challenging and highly dependent on the geopolitical and technological landscape. It is advisable to monitor government announcements, legislative proposals (with our country-by-country guide to the NIS2 Directive) and industry trends to stay informed about potential changes. Additionally, engaging with industry associations, legal experts and regulatory bodies can provide insights into anticipated developments in cybersecurity regulations.

Law stated - 20 December 2024

EVERSHEDS SUTHERLAND

Robbert Santifort robbertsantifort@eversheds-sutherland.com
Ilham Ezzamouri ilhamezzamouri@eversheds-sutherland.com

Eversheds Sutherland

Read more from this firm on Lexology

Singapore

Lim Chong Kin, **Anastasia Su-Anne Chen**
Drew & Napier LLC

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The primary cybersecurity legislation in Singapore is the Cybersecurity Act 2018-. Subsidiary legislation includes the Cybersecurity (Critical Information Infrastructure) Regulations 2018, Cybersecurity (Confidential Treatment of Information) Regulations 2018 and Cybersecurity (Cybersecurity Service Providers) Regulations 2022. The licensing framework, which currently covers cybersecurity service providers providing penetration testing services and managed security operations centre monitoring services, aims to improve the standard of cybersecurity service providers and address the information asymmetry between consumers and service providers.

The Cybersecurity Act seeks to:

- create a framework for the protection of designated critical information infrastructure (CII) against cybersecurity threats;
- authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore; and
- regulate providers of licensable cybersecurity services in Singapore – namely, managed security operations centre monitoring services and penetration testing services.

On 7 May 2024, the Cybersecurity (Amendment) Bill was passed. The Cybersecurity (Amendment) Act 2024 will expand the scope of the Cybersecurity Act to regulate new classes of persons and widen the regulatory powers of the Commissioner of Cybersecurity. The amendments have yet to come into effect as of the date of writing.

Under the Cybersecurity Act, the Commissioner is empowered to issue codes of practice and standards of performance to ensure the cybersecurity of CII. In this regard, the Commissioner has issued the 'Cybersecurity Code of Practice for Critical Information Infrastructure (Sec
ond Edition)', last updated on 12 December 2022.

In addition, the Cybersecurity Agency of Singapore (CSA) has also introduced supplementary references to assist CII owners in compliance, including the 'Security-by-Design Framework' (a framework developed to guide CII owners in addressing cyberprotection considerations throughout their system's lifecycle) and the 'Security-by-Design Framework Checklist' (a quick reference guide assisting cybersecurity practitioners in adopting the Security-by-Design Framework).

The Cybersecurity Act operates alongside existing legislation and various self-regulatory or co-regulatory codes that promote cybersecurity, including but not limited to the following:

- the Computer Misuse Act 1993, which criminalises activities such as hacking, denial-of-service attacks, infection of computer systems with malware, possession or use of hardware, software or other tools to commit offences under the Act, and

other acts preparatory to or in furtherance of the commission of any offence under the Act;

- the Personal Data Protection Act 2012, which governs the processing of individuals' personal data by private sector organisations, and is administered and enforced by the Personal Data Protection Commission;
- the Strategic Goods (Control) Act 2002, which governs the transfer and brokering of strategic goods and strategic goods technology, including 'information security' systems, equipment and components (ie, designed or modified to use cryptography for data confidentiality having in excess of 56 bits of symmetric key length or equivalent);
- sector-specific codes of practice, such as the Telecommunication Cybersecurity Code of Practice formulated by the Infocomm Media Development Authority, the converged telecommunications and media regulator in Singapore, which is imposed on major internet service providers in Singapore and includes security incident management requirements;
- other sector-specific regulatory frameworks, such as the Notice on Technology Risk Management (and the related Technology Risk Management Guidelines) (TRM Notices and Guidelines) formulated by the Monetary Authority of Singapore, Singapore's central bank and the regulator responsible for overseeing the financial sector in Singapore, which imposes certain requirements relating to technology risk management for Monetary Authority of Singapore-regulated financial institutions; and
- in respect of public sector agencies, the 'Business Continuity Readiness Assessment Framework', which was put in place to assess the level of security readiness and preparedness of Singapore's public sector agencies.

Law stated - 19 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The Cybersecurity Act provides for the regulation of CII in 11 critical sectors. 'CIIs' are computers or computer systems i) designated by the Commissioner that are necessary for the continuous delivery of an essential service, the loss or compromise of which will lead to a debilitating effect on the availability of the essential service in Singapore, and ii) located wholly or partly in Singapore. Arising from the Cybersecurity (Amendment) Act, the scope of 'computer' and 'computer system' under the Cybersecurity Act will expand to include 'virtual computer' and 'virtual computer system' respectively. The amendments will empower the Commissioner to designate computers or computer systems that are wholly located outside Singapore as CIIs, so long as its owner is in Singapore and the computer or computer system would have been designated as a CII had it been located wholly or partly in Singapore.

The 11 critical sectors containing an essential service from which CII may be designated are:

- energy;
- info-communications;
- water;
- healthcare;
- banking and finance;
- security and emergency services;
- aviation;
- land transport;
- maritime;
- government; and
- media.

Law stated - 19 December 2024

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

The CSA has launched a certification scheme known as the Singapore Common Criteria Scheme (SCCS). The SCCS is based on the international standard ISO/IEC 15408 for computer security certification, otherwise known as the Common Criteria for Information Technology Security Evaluation. The SCCS aims to provide a cost-effective regime for the info-communications industry to evaluate and certify that their IT products conform to an accepted protection profile under the SCCS.

In addition, the CSA operates the Cybersecurity Labelling Scheme (CLS), which is a basic cybersecurity hygiene scheme for the labelling of network-connected consumer smart devices. Presently, the CLS is a voluntary scheme to allow time for market and developers to understand how the scheme would benefit them. The CSA has established arrangements with overseas partners for CLS-labelled products (of specific levels) to be recognised in Finland and Germany. Further, CLS Level 3 and Level 4 applications for consumer connected products may be granted both Singapore's CLS label and the Finnish Cybersecurity Label at once, with a single application process.

The CSA Cybersecurity Certification Centre also operates a National IT Evaluation Scheme (NITES) for the valuation and certification of IT products that meet the 'high assurance' requirement for Singapore government procurement. Products that are intended to be used for handling sensitive government data must be evaluated in accordance with NITES. NITES largely adopts the Common Criteria methodology for evaluating the products at 'high assurance' level.

More generally, the government has publicly stated that, in the implementation of the Cybersecurity Act, it will take reference from internationally recognised standards when developing codes of practice and standards of performance for different sectors.

Law stated - 19 December 2024

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Personal liability may in certain circumstances be imposed on certain individuals for offences committed by their organisations under the Cybersecurity Act. Such offences include, among others, the failure of a CII owner to notify the Commissioner of prescribed cybersecurity incidents within the prescribed period of becoming aware of such occurrence under section 14, and the failure of a CII owner to conduct regular cybersecurity audits and risk assessments with the stipulated frequency under section 15.

Where offences committed by corporations are concerned, section 36 of the Cybersecurity Act imposes personal liability on officers, members (where the affairs of a corporation are managed by its members) and individuals involved in the management of the corporation and who are in a position to influence its conduct for offences committed by the corporation under the Cybersecurity Act, where such person:

- consented or connived, or conspired with others to effect the commission of the offence;
- is in any other way knowingly concerned or party to the commission of the offence; or
- knew or ought reasonably to have known that the offence by the corporation would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence.

Where offences committed by an unincorporated association or a partnership are concerned, section 37 of the Cybersecurity Act imposes personal liability on officers of unincorporated associations and members of their governing bodies, partners in a partnership, or individuals involved in the management of the unincorporated association or partnership who are in a position to influence its conduct.

Further, the Cybersecurity Code of Practice for Critical Information Infrastructure (Second Edition) imposes requirements to ensure effective leadership from the board of directors and senior management in building the right organisational culture, mindset and structure in relation to cybersecurity, and to provide effective and timely business decisions on important cybersecurity matters. For instance, it is a requirement for CII owners to ensure that their board of directors (or equivalent body) includes at least one member who has knowledge and awareness of cybersecurity matters to have oversight of the cybersecurity risks to the CII, and to provide guidance to senior management on how to manage systemic cybersecurity risks.

Under general company law, a director's failure to adequately manage an organisation's cybersecurity arrangements may amount to a breach of his or her directors' duties – for example, under section 157 of the Companies Act 1967, which requires a director to use reasonable diligence in the discharge of the duties of his or her office.

The Code of Corporate Governance, which applies to listed companies in Singapore on a comply-or-explain basis, establishes the principle that the board of directors is responsible for the governance of risk and should ensure that management maintains a sound system of risk management and internal controls to safeguard the interests of the company and its shareholders.

Law stated - 19 December 2024

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

'Cybersecurity' is defined under section 2 of the Cybersecurity Act to mean the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state:

- the computer or computer system continues to be available and operational;
- the integrity of the computer or computer system is maintained; and
- the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

The Cybersecurity Act, which provides for the protection of CII and establishes powers for the investigation and prevention of cybersecurity threats and incidents, falls under the purview of the Commissioner.

There is no statutory definition of the term 'cybercrime'. In general, cybercrime issues are dealt with under the Computer Misuse Act, which criminalises activities such as the unauthorised access to computer material and the unauthorised modification of computer material. The investigation of offences under the Computer Misuse Act falls under the purview of the Singapore Police Force.

The protection of personal data falls under the purview of the Personal Data Protection Act, which is administered and enforced by the Personal Data Protection Commission.

Law stated - 19 December 2024

Mandatory minimum protective measures

6 | What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The Cybersecurity Act does not prescribe detailed protective measures to be taken. Instead, it imposes a set of general duties on owners of CII, including:

- a duty to comply with notices issued by the Commissioner for the CII owners to provide information (section 10);
- a duty to comply with codes of practice, standards of performance or written directions as may be issued by the Commissioner (sections 11 and 12);
- a duty to notify the Commissioner of any change in ownership of the CII (section 13);
- a duty to report prescribed cybersecurity incidents (ie, to notify the Commissioner of any prescribed cybersecurity incident relating to the CII) (section 14);
- a duty to conduct cybersecurity audits at the stipulated frequency (ie, to cause audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance, which are to be carried out by an auditor approved or appointed by the Commissioner) (section 15);
- a duty to conduct cybersecurity risk assessments at the stipulated frequency (section 15); and
- a duty to participate in cybersecurity exercises as directed by the Commissioner (section 16).

More detailed measures for the protection of CII may be prescribed in codes of practice, standards of performance or directions issued directly to CII owners.

The Cybersecurity Code of Practice for Critical Information Infrastructure (Second Edition) sets out minimum protective measures that CII owners need to comply with to ensure the cybersecurity of their CII. A non-exhaustive list of key requirements is provided below:

- Audit requirements for remediating findings from audits performed by CII owners to ensure compliance with the Cybersecurity Act and applicable codes of practice and standards of performance.
- Governance requirements that involve establishing and maintaining frameworks to ensure that the cybersecurity strategies of CII owners are aligned with their business objectives.
- Requirements to establish a risk management framework and to adopt a security-by-design approach to the extent that it applies to the CII's system development lifecycle.
- Identification requirements to assist CII owners to understand and identify resources and assets supporting critical business functions in delivering essential services, and the associated cybersecurity risks.
- Protection requirements such as access control measures, privileged access management, system hardening, network segmentation that help CII owners understand and implement the required people, process and technology controls to protect the CII and to limit and contain the impact of cybersecurity incidents.
- Detection requirements that aim to assist the CII owners in understanding and implementing the required people, process and technology controls to detect and identify any malicious activity or vulnerability that could compromise the CII, including any stepping-stone attacks and attacks against the crown jewels of the system. CII owners must investigate and identify potential threats and determine the

impact, root cause and controls for containing threats and incidents and fortifying CII. These include measures such as logging, monitoring of traffic and logs, establishing cyberthreat intelligence.

- Response and recovery requirements that involve CII owners establishing, managing and exercising cybersecurity incident response plans and crisis communication plans to prepare the CII for cybersecurity incidents.
- Cybersecurity resiliency requirements for CII owners and CII to withstand cybersecurity incidents, continue the delivery of essential services and recover from cybersecurity incidents.
- Cybersecurity training and awareness requirements to help employees understand proper cyber hygiene and the security risks associated with their actions, and identify cybersecurity incidents that they may encounter in their work.

Within the financial sector, the TRM Notices and Guidelines issued by the Monetary Authority of Singapore stipulate that financial institutions shall establish frameworks and processes for the identification of critical systems (as defined in the Notices), and shall implement IT controls to protect customer information from unauthorised access or disclosure. Such critical systems include, among others, automated teller machine systems, systems that support payment, clearing or settlement functions, and online banking systems. The TRM Guidelines were most recently updated on 18 January 2021.

The Monetary Authority of Singapore has issued the Cyber Hygiene Notices, which is a set of requirements legally binding upon financial institutions relating to the mitigation of cyberthreat risks (Cyber Hygiene Notices). The Cyber Hygiene Notices consist of separate notices that apply respectively to financial institutions such as banks, licensed financial advisers and credit card or charge card licensees.

The Cyber Hygiene Notices build upon the requirements contained in the TRM Notices and Guidelines and make it mandatory for financial institutions to:

- establish and implement robust security for IT systems;
- ensure that updates are applied to address system security flaws in a timely manner;
- deploy security devices to restrict unauthorised network traffic;
- implement measures to mitigate the risk of malware infection;
- secure the use of system accounts with special privileges to prevent unauthorised access; and
- strengthen user authentication for critical systems, as well as systems used to access customer information.

Broadly summarised, the Cyber Hygiene Notices require financial institutions to implement a set of cybersecurity measures to protect and secure systems from cyberattacks. A non-exhaustive list of key measures is provided below:

- Administrative accounts must be secured so as to prevent unauthorised access or use – this includes the granting of access rights on a 'need-to-use' basis, the establishment of procedures to assess and approve such grants, periodic reviews to verify their appropriateness, and other preventive controls such as password complexity, expiration, dual control and system administration duty segregation.

- Security patches must be applied to address system vulnerabilities within a time frame that is commensurate with the risk posed by such vulnerability (including the system's criticality, the security severity of the patches and any existing controls in the IT environment). If no security patch is available, controls could be instituted to reduce risk (eg, the use of network security devices to detect and intercept malicious payloads, where a zero-day vulnerability has been identified and no patch is available).
- A written set of security standards must be available for every system. The system must conform to such standards, and where this is not possible controls should be put in place to reduce any resulting risk (including processes to seek dispensation from senior management).
- Network perimeter defence controls must be implemented to restrict all unauthorised network traffic.
- One or more malware protection measures (eg, antivirus solutions) must be implemented on every system to mitigate the risk of malware infection (where such protection measures are available and can be implemented).
- Multi-factor authentication must be implemented in respect of all administrative accounts of operating systems, databases, applications, security appliances or network devices that are critical systems, as well as all accounts used to access customer information over the internet.

Where an entity is unable to comply with any requirement by reason of being unable to exercise direct control over the system, or unable to exercise indirect control over the system by requiring the service provider to ensure compliance and it is not reasonable to procure an alternative system provider over whom indirect control can be exercised, then compliance is not necessary to the extent that control cannot be exercised.

Law stated - 19 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Under Part 7, Division 4 of the Copyright Act 2021, there are prohibitions on the circumvention of technological access control measures applied to copyrighted work (or a copy thereof) or a recording of a protected performance, as well as prohibitions on dealing in a circumventing device or service. A contravention of these provisions may constitute an offence under section 439 of the Copyright Act.

In addition, the provisions of the Computer Misuse Act, while not specifically targeted at addressing threats to intellectual property, may apply to cybercrime activities that involve threats to intellectual property.

Law stated - 19 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Yes. The Cybersecurity Act regulates designated CII in 11 critical sectors containing essential services such as energy, banking and finance. It imposes general duties on owners of CII to report prescribed cybersecurity incidents and to comply with prescribed codes of practice, standards of performance or written directions in relation to the CII, among others.

When the Cybersecurity (Amendment) Act comes into effect, the Cybersecurity Act will also impose duties on (1) providers of essential services who do not own the CII they use, but use CII owned by a computing vendor/third-party; (2) owner of a computer or computer system designated as a 'system of temporary cybersecurity concern'; (3) entity designated as an 'entity of special cybersecurity interest'; and (4) major foundational digital infrastructure service providers (in particular cloud computing service providers and data centre facility service providers).

Law stated - 19 December 2024

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There is no general restriction against the sharing of cyberthreat information. However, section 43 of the Cybersecurity Act provides that specified persons must not, except in limited circumstances, disclose certain information that has come into such persons' knowledge in the performance of their functions or discharge of their duties under the Cybersecurity Act. Such information includes matters relating to a computer or computer system.

Other general legislation aimed at preserving the confidentiality or secrecy of certain matters may also apply to prevent the sharing of cyberthreat information in certain circumstances. For example, information that relates to official secrets may also be protected from communication under the Official Secrets Act 1935.

Law stated - 19 December 2024

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The following is a non-exhaustive list of cyberactivities that are criminalised in Singapore:

- It is an offence for any person (which includes organisations) to knowingly cause a computer to perform any function for the purposes of securing unauthorised access to any program or data held in any computer (eg, by hacking or using another person's login details without authority) (section 3 of the Computer Misuse Act).
- It is an offence for any person to cause a computer to perform any function for the purpose of securing access to a computer (whether authorised or unauthorised) with the intent to commit or facilitate the commission of an offence involving property, fraud or dishonesty or which causes bodily harm (eg, identity theft or identity fraud) (section 4 of the Computer Misuse Act).
- It is an offence for any person to do any act that the person knows will cause an unauthorised modification of the contents of any computer (eg, deliberately infecting computer systems with malware and viruses) (section 5 of the Computer Misuse Act).
- It is an offence for any person to knowingly secure unauthorised access to any computer for the purpose of obtaining any computer service, or to perform unauthorised use or interception of any computer function (section 6 of the Computer Misuse Act).
- It is an offence for any person to knowingly cause unauthorised interference or obstruction of the lawful use of a computer or of the usefulness or effectiveness of any program or data stored within a computer (eg, denial-of-service attacks) (section 7 of the Computer Misuse Act).
- It is an offence for any person to disclose without authority access codes for wrongful gain, unlawful purposes or with the knowledge that it is likely to cause wrongful loss (section 8 of the Computer Misuse Act);
- it is an offence for any person to illegally obtain, retain or supply personal information about another individual from a computer in contravention of certain provisions under the Computer Misuse Act (eg, selling identity card numbers or credit card information without legitimate purpose) (section 9 of the Computer Misuse Act).
- It is an offence for any person to obtain or retain any item with the intent to using it to commit or facilitate the commission of an offence (eg, buying or dealing in hacking tools) (section 10 of the Computer Misuse Act).
- It is an offence for an organisation or individual to evade requests made by individuals to access or correct their personal data by disposing of, altering, falsifying, concealing or destroying records containing personal data or information about the collection, use or disclosure of personal data (section 51 of the Personal Data Protection Act). This may constitute a cyberactivity if the records were kept on a computer.

Law stated - 19 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Locally, the Singapore authorities have introduced a number of initiatives to enhance the security standards of cloud service providers. Legislative initiatives include the Cybersecurity Act, which aims to enhance cybersecurity among essential services in 11 critical sectors.

When the Cybersecurity (Amendment) Act comes into effect, the Cybersecurity Act will also impose duties on (1) providers of essential services who do not own the CII they use, but use CII owned by a computing vendor/third-party; (2) the owner of a computer or computer system designated as a 'system of temporary cybersecurity concern'; (3) an entity designated as an 'entity of special cybersecurity interest'; and (4) major foundational digital infrastructure service providers (in particular cloud computing service providers and data centre facility service providers).

Further, the Commissioner's regulatory powers will also be widened (eg, the types of incidents to be reported to the Commissioner will be expanded, the Commissioner will have the power to authorise the conduct of on-site inspections under certain circumstances).

On 17 October 2023, the CSA and the Cloud Security Alliance published two 'Cloud Security Companion Guides for Cyber Essentials and Cyber Trust', which are national cybersecurity standards developed by the CSA. The Cloud Security Companion Guides provide guidance to cloud customers, including small and medium enterprises (SMEs), so they can better understand their cloud-specific risks and responsibilities, and the necessary steps to take.

Other initiatives include the Multi-Tier Cloud Security Standard for Singapore (SS 584) issued by the Information Technology Standards Committee for voluntary adoption by cloud service providers (CSPs). The SS 584 standard provides for three tiers of security certification (Tier 1 being the base level and Tier 3 being the most stringent). Although adoption of the SS 584 standard is voluntary, certification under the SS 584 standard may be a requirement to participate in government tenders for public cloud services.

The Infocomm Media Development Authority has also issued a set of Cloud Outage Incident Response Guidelines (COIR Guidelines) for voluntary adoption by CSPs. The COIR Guidelines guide CSPs in planning for and responding to cloud outages, with a focus on operational mistakes, infrastructure or system failure and environmental issues (eg, flooding, fire).

Law stated - 19 December 2024

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The Cybersecurity Act and the Personal Data Protection Act may be applicable to foreign organisations doing business in Singapore. The frameworks generally do not impose differing standards of regulatory obligations on the foreign organisations to which they apply, as compared with local organisations.

The framework for the protection of CII under the Cybersecurity Act applies to any CII located wholly or partly in Singapore (section 3 of the Cybersecurity Act). Section 7 of the Cybersecurity Act allows computers or computer systems that are located wholly or partly in Singapore to be designated as CII. Hence, owners of CII that are partly located in Singapore would need to comply with the requirements of the Cybersecurity Act. For completeness, under the Cybersecurity (Amendment) Act, a new section 7(1A) will be introduced in the Cybersecurity Act to allow the Commissioner to also designate computers or computer systems that are wholly located outside Singapore as CIIs, so long as the computer or computer system is necessary for the continuous delivery of an essential service and its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore, and the computer or computer system would have been designated as a CII under section 7(1) had it been located wholly or partly in Singapore.

Further, overseas companies that are not registered in Singapore but provide licensable cybersecurity services to the Singapore market must apply for a Cybersecurity Service Provider licence pursuant to Part 5 of the Cybersecurity Act.

Moreover, the term ‘organisation’ is defined under the Personal Data Protection Act to include any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the law of Singapore, or resident or having an office or a place of business in Singapore. Therefore, the Personal Data Protection Act may be applicable to foreign entities that fall under this definition of ‘organisation’.

Law stated - 19 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes. The Singapore authorities have introduced various non-legislative initiatives aimed at enhancing cybersecurity standards. For instance, the authorities have introduced standards and guidelines to promote security among cloud service providers. More recently, the Cybersecurity Agency of Singapore (CSA) has published the Safe App Standard 2.0 on 15 October 2024, which aims to strengthen the overall security posture of mobile apps in Singapore and ensure better safeguards for app transactions and user data. On the same day, the 'Guidelines on Securing AI Systems and Companion Guide on Securing AI Systems' were released. These documents aim to help system owners secure artificial intelligence (AI) throughout its life cycle, and provide practical measures and best practices to address cybersecurity risks to AI systems respectively.

The CSA has also published supplementary references to help owners of critical information infrastructure (CII) proactively secure and build resilience into their systems, such as its Security-by-Design Framework, which was developed to guide CII owners

through the process of incorporating security into their systems development life cycle process.

The Singapore Computer Emergency Response Team (SingCERT), which is part of the CSA, facilitates the detection, resolution and prevention of cybersecurity-related incidents on the internet. It publishes alerts, advisories and recommendations from time to time, detailing procedures or mitigating measures for organisations to respond to new cyberthreats.

On 14 September 2021, the Personal Data Protection Commission issued its 'Guide to Data Protection Practices for ICT Systems', which compiles best practices for organisations to incorporate into their information and communications technology (ICT) policies, systems and processes.

A non-exhaustive list of measures recommended in the 'Design for ICT Systems Guide' includes the following:

- prior to development, a data protection impact assessment should be conducted;
- the collection of personal data by information and communication technology (ICT) systems that is not used or necessary should generally be avoided;
- user acceptance testing, load testing and stress testing should be performed at the near-end stage of the system development cycle, and business requirements are properly captured and documented during requirements gathering;
- with respect to web applications and websites, ensuring that the system validates all data input by users so that no unexpected inputs can be keyed in through the user interface;
- updates and security patches should be applied to ICT system components as soon as possible;
- https instead of http should be utilised;
- a web application firewall should be deployed; and
- code reviews, vulnerability assessments, penetration testing and user acceptance testing should be conducted.

Law stated - 19 December 2024

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

The government has publicly stated that it does not intend to provide funding to offset the costs of CII obligations that are regulatory requirements under the Cybersecurity Act. However, the government has established several schemes to enhance the cybersecurity capabilities of organisations, particularly for small and medium enterprises (SMEs).

For instance, the Infocomm Media Development Authority has established an SME Digital Tech Hub, a dedicated hub that provides specialist digital technology advice to SMEs on areas including, but not limited to, data analytics and cybersecurity. It also works with

SME Centres and Trade Association and Chambers to provide assistance in connecting SMEs with digital technology vendors and consultants, as well as conducting workshops and seminars to improve the digital capabilities of SMEs. The CSA has also tailored SG Cyber Safe cybersecurity toolkits for SME owners and employees for awareness and cybersecurity training. In February 2023, the CSA launched a cybersecurity health plan scheme with funding support for SMEs. The scheme encourages SMEs facing manpower constraints in hiring cybersecurity personnel to engage cybersecurity consultants for chief information security officer-as-a-service. The CSA will provide funding support to SMEs by co-funding up to 70 per cent of their costs for consultancy services for the first year.

The CSA and the Infocomm Media Development Authority have also established partnerships with private organisations through the Critical Infocomm Technology Resource Programme Plus, Cybersecurity Professional Scheme, Cyber Security Associates and Technologists programme and the Tech Skills Accelerator initiative. These partnerships help to train and up-skill professionals with ICT or engineering disciplines, enabling them to take on cybersecurity job roles through company-led, on-job training.

Furthermore, the CSA launched the SG Cyber Talent Development Fund in 2022 to encourage communities, associations and industry partners to develop initiatives that engage, up-skill or advance the cybersecurity workforce. In particular, training or job placement programmes for cybersecurity talent, will receive the highest tier of support with up to S$90,000 for projects lasting up to a year. In late 2023, it was announced that a new cyber talent programme, SG Cyber Associates, would be rolled out to provide foundational and targeted cybersecurity training for non-cybersecurity professionals to develop cybersecurity skills relevant to their work. This is part of the CSA's existing efforts to increase the capacity of the cybersecurity workforce. The SG Cyber Leadership and Alumni Programme was also launched in 2023 – a structured training programme targeted at participants at different stages of their cybersecurity journey and open to all countries.

In the area of certifications and accreditations, the government has also announced that it will allow small service providers to apply for government funding to cover a proportion of the costs to become member companies of CREST (an international not-for-profit, membership body representing the global cybersecurity industry). The CREST Singapore chapter has been established in collaboration and partnership with the CSA, the Association of Information Security Professionals, the Monetary Authority of Singapore, the Association of Banks in Singapore and the Infocomm Media Development Authority, and offers various certifications for cybersecurity services in Singapore.

Law stated - 19 December 2024

Industry standards and codes of practice

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The following publicly available industry standards and codes of practice may be accessed at the links provided:

-

the Cybersecurity Code of Practice for Critical Information Infrastructure may be accessed on the CSA website at https://www.csa.gov.sg/legislation/codes-of-practice;

- the TRM Notices and Guidelines (Notice on Technology Risk Management, and the related Technology Risk Management Guidelines) may be accessed on the Monetary Authority of Singapore website at http://www.mas.gov.sg;
- the Cyber Hygiene Notices may be accessed on the Monetary Authority of Singapore website at https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&page=1&q=cyber%20hygiene;
- the Personal Data Protection Commission's various advisory guidelines and guides may be accessed on the Commission's website at http://www.pdpc.gov.sg; and
- the Association of Banks in Singapore's industry guidelines on cybersecurity can be accessed on its website at http://www.abs.org.sg.

Law stated - 19 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

In the case of certain breaches involving personal data, there may be a need to notify the authorities.

The mandatory data breach notification obligation (Part 6A of the Personal Data Protection Act 2012 (PDPA)) came into effect on 1 February 2021. In the event of a data incident, an organisation has a duty to conduct, in a reasonable and expeditious manner, an assessment of the incident to determine if it is a 'notifiable data breach'. If the data incident is a 'notifiable data breach', the organisation has an obligation to notify the Personal Data Protection Commission of such a data breach as soon as practicable, but in any case no later than three calendar days from when the organisation makes the assessment.

A data breach is classified as a 'notifiable data breach' if the data breach results in, or is likely to result in, significant harm to the individual; or is, or is likely to be, of a significant scale (read with the Personal Data Protection (Notification of Data Breaches) Regulations 2021).

In addition, organisations are also required to notify the affected individuals of the 'notifiable data breach' in a reasonable manner, unless an exception applies. The two exceptions are: if, on or after assessing that the data breach is a 'notifiable data breach', the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data breach will result in significant harm to the affected individual.

Apart from the mandatory data breach notification obligation, the Personal Data Protection Commission's 'Guide on Managing and Notifying Data Breaches under the PDPA' contains a number of recommendations that organisations may consider in responding to a data breach, including that an organisation should act as soon as it is aware of a data breach and consider the following measures, where applicable:

- isolating the compromised system that led to the data breach;
- establishing whether steps can be taken to recover lost data and limit any damage caused by the data breach;
- isolating causes of the data breach in the system and, where applicable, changing the access rights to the compromised system and removing external connections to the system;
- rerouting or filtering network traffic, firewall filtering, closing particular ports or mail servers;
- preventing further unauthorised access to the system, and resetting passwords if accounts and passwords have been compromised;
- notifying the police if criminal activity is suspected and preserving evidence for investigation;
- putting a stop to practices that led to the data breach; and
- addressing lapses in processes that led to the data breach.

Further, to the extent that a breach constitutes a prescribed cybersecurity incident under the Cybersecurity Act, section 14 imposes an obligation on CII owners to notify the Commissioner of such occurrence in the form and manner prescribed within the prescribed period under the Cybersecurity (Critical Information Infrastructure) Regulations 2018. Under the Cybersecurity (Amendment) Act, owners of a system of temporary cybersecurity concern, entities of special cybersecurity interest and major foundational digital infrastructure service providers must also notify the Commissioner of the occurrence of any of the prescribed cybersecurity incidents in accordance with sections 17F, 18F and 18M.

Law stated - 19 December 2024

Voluntary information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Section 45 of the Cybersecurity Act protects the identities of informers of certain offences relating to CII. Generally, no witness in any proceedings for an offence under Part 3 of the Cybersecurity Act is obliged or permitted to:

- disclose the name, address or other particulars of an informer who has given information with respect to that offence, or the substance of the information received; or
-

answer any question if the answer would lead, or tend to lead, to the discovery of the name, address or other particulars of the informer.

Under the Cybersecurity (Amendment) Act, section 45 of the Cybersecurity Act will expand to also cover offences under Parts 3A to 3D, and civil penalties under sections 37A or 37C.

In addition, the court must also order any entries containing the informer's name or descriptions found in any document that is in evidence or liable to inspection in any proceedings as mentioned in section 45(1) of the Cybersecurity Act, which may lead to the discovery of the informer's identity, to be concealed from documents in evidence, or to be obliterated to the extent as may be necessary to protect the informer from discovery.

In the telecommunications sector, the Infocomm Media Development Authority has published a Cyber Security Vulnerability Reporting Guide to facilitate and encourage the reporting of cybersecurity vulnerabilities that the cybersecurity researcher community has detected in the public-facing applications and networks of telecommunication service providers, such as internet access, mobile and fixed-line voice and data service providers, broadcast, print (newspaper) and postal service providers.

In the financial sector, the Monetary Authority of Singapore has partnered with the Financial Services Information Sharing and Analysis Centre to set up a regional centre in Singapore to share information on cybersecurity threats among financial institutions.

Law stated - 19 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In practice, it is not uncommon for the government to consult industry players and relevant private sector parties in developing legislative and regulatory standards. For instance, prior to the introduction of the Cybersecurity Act, the government had conducted several rounds of consultations with potential CII owners, industry associations and cybersecurity professionals. Similarly, prior to the passing of the Cybersecurity (Amendment) Act, the government held a public consultation on the draft Cybersecurity (Amendment) Bill and has continued closed-door industry consultations with relevant stakeholders since the close of the public consultation. The government has also announced its intent to continue working with the industry and professional association partners to establish accreditation regimes for cybersecurity professionals.

The Singapore government has actively promoted cybersecurity through research and development (R&D) collaborations between government, academia and industry. In 2013, the Singapore government launched the National Cybersecurity R&D Programme (NCRP) to promote such research collaboration, with a total of S$190 million in funding having been made available to support the programme until 2020. As part of the NCRP, the CSA established in 2023 a CyberSG R&D Programme Office at theNanyang Technological University, which will receive funding of S$62 million. The government has also kick-started other initiatives, such as the Cybersecurity Consortium with S$1.5 million in funding over three years from 2016, and the National Cybersecurity R&D Laboratory. In July

2024, the CSA and the National University of Singapore's joint initiative – the CyberSG Talent, Innovation and Growth Collaboration Centre – was opened. It aims to provide cybersecurity companies and talents with resources and growth opportunities. This includes the Cybersecurity Industry Call for innovation and CyberBoost programmes, which aim to encourage the development of innovative cybersecurity solutions through funding of up to S$1 million for each selected solution, and provide tailored support to cybersecurity companies respectively.

Grant schemes such as the Co-Innovation and Development Proof-of-Concept Funding Scheme are also available to Singapore-registered companies or overseas firms that partner with Singapore-registered companies. The scheme aims to support the co-development of innovative cybersecurity solutions that help to meet national cybersecurity needs, with potential for commercial application.

The CERTs overseeing specific sectors also issue advisories to the operators in their respective sectors. For example, the Info-communications Singapore CERT, or ISGCERT, issues alerts to operators in the telecommunications and media sector to enhance their cyber readiness, and advisories on cybersecurity vulnerabilities pertaining to this sector.

SingCERT also works with the sectoral CERTs, where necessary, to inform local companies and affected customers on cybersecurity threats and incidents.

Further, to encourage businesses to place cybersecurity in the centre of their operations, the CSA, in partnership with the Association of Trade & Commerce (Singapore) launched the SME Cybersecurity Excellence Award to recognise SMEs in Singapore that are committed to cybersecurity.

Law stated - 19 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Yes, various insurance solutions covering cyberrisks are offered by several insurers in the Singapore market. Common coverage would include business interruption loss, data loss and restoration, and incident response and investigation costs.

Law stated - 19 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Commissioner of Cybersecurity is responsible for the enforcement of the Cybersecurity Act 2018. At present, the Chief Executive of the Cybersecurity Agency of

Singapore (CSA) has been appointed as the Commissioner. The Cybersecurity Act also provides for the appointment of a Deputy Commissioner and Assistant Commissioners to assist the Commissioner. The Assistant Commissioners will be appointed from officers of sector regulators.

The Singapore Police Force, which is overseen by the Ministry of Home Affairs, working together with the Public Prosecutor, is generally responsible for investigating and prosecuting criminal offences, such as those under the Computer Misuse Act 1993.

In relation to data protection, the Personal Data Protection Commission is the authority responsible for administering and enforcing the Personal Data Protection Act 2012.

Sector regulators, such as the Monetary Authority of Singapore, which regulates the finance sector, and the Infocomm Media Development Authority, which regulates the info-communications sector, are responsible for enforcing their individual sector-specific frameworks.

Law stated - 19 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Commissioner has broad powers under the Cybersecurity Act to require critical information infrastructure (CII) owners to furnish information relating to CII, including information to ascertain the level of cybersecurity of CII. The Commissioner also has broad powers to investigate cybersecurity threats or incidents generally, including those that involve non-CII, by requiring the production of documents and examining relevant persons.

Section 15 of the Cybersecurity Act requires CII owners to conduct cybersecurity risk assessments of CII and cybersecurity audits of the compliance of the CII with the statute and the applicable codes of practices and standards of performance, and to furnish reports to the Commissioner. Under the Cybersecurity (Amendment) Act 2024, the Commissioner may also require an audit in respect of the provider-owned CII (and the cost of such audit shall be borne by the owner) or authorise the inspection of the provider-owned CII by the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer.

Concerning investigations of cybersecurity threats or incidents, section 19 of the Cybersecurity Act sets out the powers of the Commissioner and authorised officers, which include powers to investigate cybersecurity threats or incidents for the purposes of assessing the impact or potential impact of the cybersecurity threat or incident; preventing any or further harm arising from the cybersecurity incident; or preventing a further cybersecurity incident from arising from that cybersecurity threat or incident.

Under section 19(2) of the Cybersecurity Act, the powers that are to be exercised against persons affected by the cybersecurity threat or incident include the powers to:

- require the person to attend at a specified place and time to answer questions or to provide a signed statement concerning the cybersecurity threat or incident;

- require the person to produce any record or document, or provide any relevant information;
- inspect, copy or take extracts from such records or documents; and
- examine orally the person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident.

Section 20 of the Cybersecurity Act sets out the powers of the Commissioner with respect to 'serious' cybersecurity threats or incidents, namely, those that satisfy the severity threshold specified in section 20(3) of the Cybersecurity Act.

Under section 20 of the Cybersecurity Act, the powers that may be exercised against persons affected by 'serious' cybersecurity threats or incidents include the powers to:

- exercise any power mentioned above in section 19(2) of the Cybersecurity Act;
- direct the person to carry out such remedial measures, or to cease carrying on such activities, in relation to the affected computer or computer system, to minimise cybersecurity vulnerabilities;
- require the person to take any action to assist with the investigation, including but not limited to:
    - preserving the state of the affected computer or computer system by not using it;
    - monitoring the affected computer or computer system; performing a scan of the affected computer or computer system to detect cybersecurity vulnerabilities and to assess the impact of the cybersecurity incident; and
    - allowing the incident response officer to connect any equipment to, or install any computer program on, the affected computer or computer system as necessary;
- after giving reasonable notice, enter the premises where the affected computer or computer system is reasonably suspected to be located;
- access, inspect and check the operation of the affected computer or computer system, or use the computer or computer system to search any data contained in or available to that computer or computer system;
- perform a scan of the affected computer or computer system to detect cybersecurity vulnerabilities;
- take a copy of or extracts from any electronic record or computer program affected by the cybersecurity incident; and
- with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

Under section 40 of the Cybersecurity Act, notwithstanding any provision to the contrary in the Criminal Procedure Code 2010, a district court of Singapore has jurisdiction to try any offence under the statute and has the power to impose the full penalty or punishment in respect of the offence.

With respect to investigations of data breach incidents involving personal data, section 50 of the Personal Data Protection Act sets out that the Personal Data Protection Commission has the powers to conduct an investigation (upon complaint or on its own motion) determine whether or not an organisation or an individual is complying with the Personal Data Protection Act. The specific powers of investigation of the Personal Data Protection Commission are further set out in the Ninth Schedule of the Personal Data Protection Act.

Law stated - 19 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

In relation to data breaches involving personal data, the Personal Data Protection Commission has been active in its enforcement of the Personal Data Protection Act. As of 4 December 2024, the Personal Data Protection Commission has issued a total of 258 decisions, with a significant percentage of these decisions relating to breaches of the protection obligation, namely the requirement imposed on organisations to make 'reasonable security arrangements' to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks with respect to personal data held or processed by those organisations, and the loss of any storage medium or device on which personal data is stored (section 24 of the Personal Data Protection Act).

Notably, the largest penalty the Personal Data Protection Commission has imposed on an organisation to date (S$750,000) arose from the organisation's failure to take sufficient security steps or make the necessary arrangements to protect the personal data from unauthorised access (see *Re Singapore Health Services Pte Ltd and another* [2019] SGPDPC 3).

Law stated - 19 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Section 14 of the Cybersecurity Act provides that the owner of a CII must notify the Commissioner within the prescribed period in the prescribed form and manner upon becoming aware of the occurrence of any of the following events:

- a prescribed cybersecurity incident in respect of a CII;
- a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with a CII; and
- any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the owner.

For this purpose, the prescribed cybersecurity incidents are set out in the Cybersecurity (Critical Information Infrastructure) Regulations 2018 and include:

- the unauthorised hacking of a CII;
- the installation or execution of unauthorised software or code on a CII;
- man-in-the-middle attacks, session hijacks or other unauthorised interception of communication between a CII and an authorised user; and
- denial of service attacks.

Under the Cybersecurity (Amendment) Act, owners of CII must also notify the Commissioner in the prescribed form and manner upon becoming aware of the occurrence of any of the following events:

- a prescribed cybersecurity incident in respect of any other computer or computer system under the owner's control that does not fall within the scope of which is in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the CII; and
- a prescribed cybersecurity incident in respect of any computer or computer system under the control of a supplier to the owner that is interconnected with or that communicates with the provider owned CII.

Additionally, owners of a system of temporary cybersecurity concern, entities of special cybersecurity interest and major foundational digital infrastructure service providers will be required to notify the Commissioner of the occurrence of any of the prescribed incidents.

In relation to data breaches, under the Personal Data Protection Act, organisations are required to notify the Personal Data Protection Commission of a data breach that:

- results, or is likely to result, in significant harm to the affected individuals (ie, where the compromised personal data falls within certain prescribed categories set out in the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or
- is, or is likely to be, of a significant scale (ie, affects 500 or more individuals).

Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

Organisations will then have to notify the Personal Data Protection Commission as soon as practicable, but in any case no later than three calendar days after determining that the breach meets the notification criteria.

Where the data breach results, or is likely to result, in significant harm to the affected individuals (ie, data subjects), organisations will also be required to notify affected individuals on or after notifying the Personal Data Protection Commission, unless any of the stated exceptions apply, namely:

- the organisation, on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that

renders it unlikely that the notifiable data breach will result in significant harm to the affected individual;

- the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure that rendered it unlikely that the notifiable data breach would result in significant harm to the affected individual;
- the organisation is instructed by a prescribed law enforcement agency, or directed by the Personal Data Protection Commission, not to notify the affected individual; or
- the Personal Data Protection Commission, on the written application of the organisation, waives the requirement, subject to any conditions that the Commission thinks fit.

Law stated - 19 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The Cybersecurity Act provides for a number of offences, including the following:

- an owner of a CII who fails, without reasonable excuse, to comply with the duty to furnish information relating to the CII pursuant to a notice by the Commissioner, shall be liable upon conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years or to both, and in the case of a continuing offence, to a further fine not exceeding S$5,000 for every day or part of a day during which the offence continues after conviction (section 10(2));
- an owner of a CII who fails, without reasonable excuse, to comply with the duty to notify the Commissioner within 30 days of making a material change to the design, configuration, security or operation of the CII after any information has been furnished to the Commissioner pursuant to a notice given, shall be liable on conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding 12 months or to both (section 10(7));
- any person who, without reasonable excuse, fails to comply with a direction issued by the Commissioner, shall be liable upon conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years or to both, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction (section 12(6));
- any owner of a CII who fails, without reasonable excuse, to comply with the duty to conduct cybersecurity risk assessments and cause an audit of the compliance of the CII by an auditor approved or appointed by the Commissioner, and other requirements under the same provision (such as to comply with the Commissioner's directions under subsections (3), (5)(a) or (6), or obstructs or prevents an audit mentioned in subsection (4) or a cybersecurity risk assessment under subsection (5)(b) from being carried out), shall be liable upon conviction to a fine not exceeding

S$100,000 or to imprisonment for a term not exceeding two years or to both, and in the case of a continuing offence, to a further fine not exceeding S$5,000 for every day or part of a day during which the offence continues after conviction (section 15(7));

- any owner of a CII that, without reasonable excuse, fails to furnish a copy of the report of the audit or cybersecurity risk assessment within 30 days of completion of such audit or assessment, shall be liable upon conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding 12 months or to both, and in the case of a continuing offence, to a further fine not exceeding S$2,500 for every day or part of a day during which the offence continues after conviction (section 15(8));
- any person who, without reasonable excuse, fails to comply with the duty to participate in a cybersecurity exercise if directed to do so by the Commissioner, shall be liable on conviction to a fine not exceeding S$100,000 (section 16(3));
- any person who, without reasonable excuse, fails to comply with a Magistrate's order under section 19(5), or who wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required by an incident response officer under section 19(2) in the investigation of a cybersecurity incident, shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding six months or to both (section 19(8)); and
- in the case of an investigation into serious cybersecurity incidents, any person who, without reasonable excuse, fails to comply with sections 19(2) or 19(5) as mentioned above, or who fails to comply with a direction, requirement or lawful demand of an incident response officer made in the discharge of the officer's duties under section 20, shall be liable on conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding two years or to both (section 20(7)).

When the Cybersecurity (Amendment) Act takes effect, the penalties are higher for offences relating to entities of special cybersecurity interest and major foundational digital infrastructure service providers, with a fine not exceeding the greater of S$200,000 or 10 per cent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine note exceeding S$5,000 for every day or part of a day during which the offence continues after conviction.

The amendments to the Cybersecurity Act will also introduce a new civil penalty regime. The CSA may issue civil penalties *in lieu* of prosecution for contravening any provision under Parts 3, 3A, 3B, 3C or 3D of the amended Cybersecurity Act. The civil penalty can be up to 10% of the annual turnover of the person's business in Singapore, or S$500,000, whichever is higher.

In the case of a breach of the data protection provision of the Personal Data Protection Act, the Personal Data Protection Commission is empowered to issue directions to organisations to stop collecting, using or disclosing personal data in contravention of the Personal Data Protection Act; destroy personal data collected in contravention of the Personal Data Protection Act; provide access to or correct personal data, or reduce or make a refund of any fee charged for any access or correction request; and/or pay a financial penalty.

Law stated - 19 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Section 14 of the Cybersecurity Act provides that an owner of a CII who, without reasonable excuse, fails to comply with the duty to report any prescribed cybersecurity incident within the prescribed period shall be liable on conviction to a fine not exceeding S$100,000, or to imprisonment for a term not exceeding two years, or to both.

When the Cybersecurity (Amendment) Act takes effect, designated providers responsible for third party-owned CII, owners of systems of temporary cybersecurity concern who, without reasonable excuse, fails to comply with the duty to report the prescribed cybersecurity incidents within the prescribed period shall be liable on conviction to a fine not exceeding S$100,000, or to imprisonment for a term not exceeding two years, or to both. Entities of special cybersecurity interest and major foundational digital service providers who fail to do so are subject to different penalties, being a fine not exceeding S$200,000 or 10 per cent of the annual turnover of their business in Singapore.

Section 48J of the Personal Data Protection Act provides if an organisation fails to comply with the obligations under the Personal Data Protection Act (including the mandatory data breach notification obligation), the Personal Data Protection Commission is empowered to impose the following financial penalties:

- in the case of a contravention by an organisation whose annual turnover in Singapore exceeds S$10 million, the Personal Data Protection Commission may impose financial penalties up to 10 per cent of the annual turnover in Singapore of the organisation; and
- in any other case, the Personal Data Protection Commission may impose financial penalties up to S$1 million.

Law stated - 19 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The Cybersecurity Act does not confer any private rights on parties to seek redress for unauthorised cyberactivity or failure to adequately protect systems and data.

Under the Computer Misuse Act, a court may order an offender to pay compensation to a victim of the offence. The victim may separately pursue a civil remedy against the offender, and the compensation ordered under the Computer Misuse Act will not prejudice the

victim's right to recover more than the amount compensated under the Computer Misuse Act.

By contrast, the Personal Data Protection Act provides for a right of private action for individuals. Under section 48O of the Act, any person who suffers loss or damage directly as a result of a contravention of any provision in Parts 4, 5, 6, 6A or 6B by an organisation shall have a right of action for relief in civil proceedings in a court, and the court may grant to the applicant relief by way of injunction or declaration, damages and/or such other relief as the court thinks fit.

Law stated - 19 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Sections 11 and 12 of the Cybersecurity Act impose duties on critical information infrastructure (CII) owners to comply with the codes of practice or standards of performance, or directions either of a general or specific nature issued by the Commissioner, which may contain provisions with respect to the measures to be taken by them to ensure the cybersecurity of the CII. Under the Cybersecurity (Amendment) Act, the Commissioner may also issue direct compliance with prescribed technical or other standards relating to cybersecurity in respect of provider-owned CII.

On 4 July 2022, the Commissioner of Cybersecurity issued the Cybersecurity Code of Practice for CII (Second Edition), which specifies the minimum requirements that CII owners have to comply with to ensure the cybersecurity of their CII. The Cybersecurity Agency of Singapore (CSA) has also introduced various supplementary references as additional resources to help CII owners comply with this.

In relation to the obligation to put in place reasonable security measures to protect personal data, the Personal Data Protection Commission does not prescribe any 'one-size-fits-all' solution to compliance as it recognises that each organisation will need to address its own unique circumstances. For instance, the Commission's 'Advisory Guidelines on Key Concepts in the PDPA (revised 16 May 2022)' sets out security arrangements (including administrative, physical and technical measures) that organisations may use to protect personal data.

The Commission has also published the 'Guide to Data Protection Practices for ICT Systems', which compiles best practices for organisations to incorporate into their information and communication technology (ICT) policies, systems and processes.

In particular, the 'Guide to Data Protection Practices for ICT Systems' sets out a series of good practices that organisations should undertake, including but not limited to:

- providing clear direction on ICT security goals and policies for personal data protection within the organisation;
-

establishing, enforcing and periodically reviewing ICT security policies, standards and procedures;

- instituting a risk management framework to identify security threats, assessing the risks involved and determining the controls to remove or reduce them; and
- logging database activities, such as any changes to the database and data access activities to track unauthorised activities or anomalies.

The Guide to Data Protection Practices for ICT Systems also sets out a series of enhanced practices that organisations may consider, including but not limited to:

- designing and implementing an internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type, etc;
- monitoring LAN and Wi-Fi regularly and removing unauthorised clients and Wi-Fi access points;
- using network proxies to restrict employee access to known malicious websites;
- using two-factor authentication and strong encryption for remote access; and
- disallowing non-administrative employees from installing software or changing security settings, except on a need-to basis.

Law stated - 19 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There are currently no provisions in the Personal Data Protection Act 2012 (PDPA) expressly requiring organisations to keep records of cyberthreats or attacks. It may, however, be prudent for organisations to consider the need to keep records to ensure compliance with other regulatory requirements – for example, in the case of CII owners, to fulfil audit requirements, or in the case of a breach of personal data, to keep records so that they may be provided to the Personal Data Protection Commission if it conducts an investigation into a data breach.

Law stated - 19 December 2024

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Under the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (CII Regulations), where the owner of a CII is required to notify the Commissioner of a cybersecurity incident in respect of the CII, the report must be submitted within two hours of the owner becoming aware of its occurrence and must include the following details:

- the CII affected;
- the name and contact number of the owner of the CII;
- the nature of the cybersecurity incident, whether it was in respect of the CII or an interconnected computer or computer system, and when and how it occurred;
- the resulting effect that has been observed, including how the CII or any interconnected computer or computer system has been affected; and
- the name, designation, organisation and contact number of the individual submitting the notification.

Within 14 days of the initial submission, the owner of the CII must submit in writing, via the CSA's website and to the fullest extent practicable, the following supplementary details:

- the cause of the cybersecurity incident;
- its impact on the CII, or any interconnected computer or computer system; and
- what remedial measures have been taken.

In relation to the reporting of data breaches to the authorities, the amendments to the PDPA has a mandatory data breach notification regime. If the organisation forms the view, following its assessment of a potential data breach, that the breach is 'likely to result in significant harm or impact to the individual to whom the information relates' or 'the data breach is of a significant scale' (ie, involving personal data of 500 or more individuals), the organisation must notify the Personal Data Protection Commission and, subject to certain exceptions, would also be required to notify affected individuals.

Under the Personal Data Protection (Notification of Data Breaches) Regulations 2021- , the notification to the Personal Data Protection Commission must contain the following information:

- the date on which and the circumstances in which the organisation first became aware that the data breach had occurred;
- a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment that the data breach is a notifiable data breach;
- information on how the notifiable data breach occurred;
- the number of individuals affected by the notifiable data breach;
- the personal data or classes of personal data affected by the notifiable data breach;
- the potential harm to the affected individuals as a result of the notifiable data breach;
- information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Personal Data Protection Commission of the occurrence of the notifiable data breach:
    - to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and
    -

to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

- information on the organisation's plan (if any) to inform, on or after notifying the Personal Data Protection Commission of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach; and
- the business contact information of at least one authorised representative of the organisation.

The notification to the Personal Data Protection Commission must also be in the form and manner specified on the Personal Data Protection Commission's website at www.pdpc.gov.sg.

As for notification to individuals, the notification must contain the following information:

- the circumstances in which the organisation first became aware that the notifiable data breach had occurred;
- the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach;
- the potential harm to the affected individual as a result of the notifiable data breach;
- information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual:
    - to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and
    - to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
- the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the individual's personal data affected by the notifiable data breach; and
- the business contact information of at least one authorised representative of the organisation.

Apart from the Personal Data Protection Commission, where criminal activity (eg, hacking, theft or unauthorised system access by an employee) is suspected, organisations should consider alerting the police and preserving evidence for police investigation. Where a case of cyberattack is suspected, organisations should also consider alerting the CSA through the Singapore Computer Emergency Response Team.

Within the financial sector, the Notice on Technology Risk Management issued by the Monetary Authority of Singapore (MAS) requires financial institutions to notify MAS as soon as possible, but not later than one hour, upon the discovery of a relevant IT incident. The Notice also requires the financial institution to submit a root-cause and impact analysis

report in respect of the IT incident to MAS within 14 days or such longer period as MAS may allow, from the discovery of the relevant IT incident.

Law stated - 19 December 2024

Time frames

30 | What is the timeline for reporting to the authorities?

Section 14 of the Cybersecurity Act sets out that the owner of a CII must notify the Commissioner within the prescribed period upon becoming aware of the occurrence of the cybersecurity breaches described above.

The prescribed period is set out in regulation 5 of the CII Regulations, which sets out that a CII owner must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in the required form within two hours after becoming aware of the occurrence, and provide, within 14 days of the initial submission, the following supplementary details:

- the cause of the cybersecurity incident;
- its impact on the CII, or any interconnected computer or computer system; and
- what remedial measures have been taken.

In relation to the reporting of personal data breaches to the authorities, where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. If the organisation determines that the data breach is notifiable, it must then notify the Personal Data Protection Commission as soon as practicable, but in any case no later than three calendar days after determining that the breach meets the notification criteria.

Law stated - 19 December 2024

Other reporting requirements

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no provisions within the Cybersecurity Act that expressly require organisations to report threats or breaches to others in the industry, to customers or to the general public.

In relation to notification of data breaches involving personal data to the public, organisations must notify affected individuals of the data breach, unless an exception applies. Specifically, organisations must, on or after notifying the Personal Data Protection Commission, notify the individuals affected by a notifiable data breach, if the data breach results in, or is likely to result in, significant harm to an affected individual. The notification

should be in the form and manner as prescribed and contain information to the best of the knowledge and belief of the organisation at the time.

However, there are exceptions to this requirement. Organisations do not need to notify the affected individuals if one of the stated exceptions applies, namely, if the organisation:

- takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- has implemented, prior to the occurrence of the notifiable data breach, any technological measure that rendered it unlikely that the notifiable data breach would result in significant harm to the affected individual.

Law stated - 19 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

With the rapid development of cyberthreats, regulators will need to keep abreast of rapid changes in the cybersecurity landscape in order to ensure that regulations are up-to-date and effective. The Cybersecurity (Amendment) Act was brought about to combat the increased risk of cyberattacks and to keep pace with the developments in the cyberthreat landscape and business environment, and the need to ensure that there are necessary safeguards beyond that for CII.

Companies and other relevant private sector parties also play a role in helping shape legislative and regulatory standards through participation in consultation sessions conducted by the government.

During the Committee of Supply Debate 2024, the Ministry of Digital Development and Information announced that the Taskforce on the Resilience and Security of Digital Infrastructure and Services was studying the introduction of a Digital Infrastructure Act to address the security and resilience of digital infrastructure and services in Singapore. While the Cybersecurity Act is focused on mitigating cyber-related risks, the Digital Infrastructure Act will go further to address a broader set of resilience risks faced by providers of digital infrastructure and services. This may include misconfigurations in technical architecture and physical hazards such as fires and cooling system failures.

Law stated - 19 December 2024

DREW & NAPIER

Lim Chong Kin chongkin.lim@drewnapier.com
Anastasia Su-Anne Chen anastasia.chen@drewnapier.com

Drew & Napier LLC

Switzerland

Markus Naef, **Oliver Scharp**, **Carol Tissot**, **Nadine Zollinger**
Eversheds Sutherland

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

To date, Switzerland has not adopted legislation specifically dedicated to cybersecurity, and the Swiss regulatory framework for cybersecurity consists of a mosaic of legislative texts and ordinances.

Effective from 1 January 2023, the Information Security Act (ISA) and its four Ordinances, as amended on 1 January 2024, govern the organisation of the federal administration with respect to protection against cyberrisks, regulating the duties of federal cybersecurity bodies, establishing the National Cyber Security Centre (NCSC), and regulating various compliance aspects regarding external service providers contracting with the federal administration. The ISA and its Ordinances notably introduce an obligation to report cyberattacks targeting critical infrastructure, which must be reported to the NCSC.

Below is a list of the most relevant legislative acts that explicitly or implicitly deal with cybersecurity in the private sector, and that are applicable in Switzerland:

- The Budapest Convention on Cybercrime came into effect in Switzerland on 1 January 2012. It requires member states to harmonise their criminal laws, adopt effective investigation and prosecution measures, and establish a rapid and efficient regime of international cooperation in cybersecurity.
- The revised Federal Data Protection Act (FADP), which came into force on 1 September 2023, and its Ordinance introduced significant changes in the Swiss data protection regime, aiming for better alignment with the EU General Data Protection Regulation. It ceases the protection of data pertaining to legal entities and limits it to natural persons, enhances transparency, mandates the notification of data breaches in certain cases and strengthens criminal liability for violations of the FADP. Regarding data security, the legislator has introduced new requirements in the revised FADP.
- Under the Federal Telecommunications Act and its Ordinance, the Federal Office of Communication is responsible for implementing the administrative and technical requirements related to the security and availability of telecommunications services.
- The Federal Act on Surveillance of Post and Telecommunications and the Federal Intelligence Act govern information requests and the surveillance, in real-time or retrospectively, of postal and telecommunications traffic, as well as the monitoring of data flows for national security objectives. This law notably obliges telecommunications service providers and network operators to cooperate, mandates the retention of certain traffic and metadata by the providers, and allows for specific or general surveillance of communications (with judicial authority approval) and the gathering of intelligence on broader communication patterns, necessitating the implementation of technologies and security protocols for secure data management and analysis. Lastly, it also permits access to location information in the context of law enforcement investigations.

- The Federal Act on Financial Market Infrastructures (FinMIA) contains several cybersecurity measures, particularly focused on the protection and security of critical financial market infrastructures. It requires financial market infrastructures to have robust IT systems capable of effectively responding to emergencies and ensuring business continuity. It also mandates the implementation of reliable access controls to prevent unauthorised access to systems and data. Lastly, it requires measures to detect and remedy security incidents.
- According to the Ordinance on Internet Domains , the registries for the '.ch' and '.swiss' domain extensions are required, under certain conditions, to block domain names suspected of being used for phishing, distributing harmful software (malware), or supporting such activities.

Law stated - 4 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In Switzerland, cybersecurity laws and regulations impact on various sectors, particularly those that are of critical importance to national security, economic stability and the protection of sensitive personal data. These sectors have made significant progress towards promoting cybersecurity; others may need further improvement.

Sectors most affected by cybersecurity laws and regulations

- Financial services: this sector is highly regulated due to its critical importance to the economy and the potential catastrophic impact of cyber incidents. The FinMIA emphasises the need for robust IT systems and effective emergency responses. Financial institutions are under the strict oversight of the Swiss Financial Market Supervisory Authority, which imposes rigorous cybersecurity requirements.
- Healthcare: with the increasing digitalisation of health records and the sensitivity of personal health information, the healthcare sector is significantly affected by cybersecurity regulations. The FADP has implications for how personal data is protected, requiring healthcare providers to implement stringent measures to safeguard patient data.
- Telecommunications: as a backbone of digital infrastructure, the telecommunications sector is subject to specific cybersecurity regulations, including the Federal Telecommunications Act and the Ordinance on Telecommunications Services. These laws mandate measures to ensure the security and availability of telecommunications services.
- Public administration: following the implementation of the ISA, federal and cantonal governments have enhanced their cybersecurity frameworks. The establishment of the NCSC underscores the sector's progress in promoting cybersecurity.
-

Critical infrastructure: beyond specific industries, sectors considered to be critical infrastructure, such as energy, water supply and transport, are also highly regulated. Although Switzerland does not have a dedicated cybersecurity law for all critical infrastructure sectors, various legislative instruments address cybersecurity risks relevant to these areas, including the above-mentioned ISA. The regulation and protection of critical infrastructure sectors may involve additional sector-specific regulations and measures that complement the overarching principles set forth by the ISA. These supplementary regulations are designed to address the unique vulnerabilities and security requirements of each critical infrastructure sector, ensuring a comprehensive protective stance against cybersecurity threats.

Sectors that need to improve

- Small and medium-sized enterprises (SMEs): while not a sector per se, SMEs across various industries often lack the resources or knowledge to implement comprehensive cybersecurity measures. Enhanced support and awareness initiatives could improve cybersecurity resilience within this group.
- Education and research: as digital technologies become increasingly integral to educational and research activities, this sector must continue to improve its cybersecurity posture to protect intellectual property and personal data.

Law stated - 4 December 2024

International standards

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

In Switzerland, adherence to international cybersecurity standards is not mandatory. However, these standards are widely recognised and often voluntarily adopted by organisations seeking to enhance their information security practices. The ISO 27001:2013, which provides specifications for information security management systems, is particularly noteworthy. This standard helps organisations manage the security of assets such as financial information, intellectual property, employee details and information entrusted by third parties.

Swiss organisations, across various sectors, actively pursue ISO 27001 certification as part of their commitment to cybersecurity. This is because adherence to ISO 27001 is widely recognised as a strong indicator of an organisation's dedication to managing information security risks.

Law stated - 4 December 2024

Personnel and director obligations

4 |

What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Swiss law does not specify detailed cybersecurity obligations for directors and responsible personnel. In Switzerland, the obligation to safeguard cybersecurity predominantly resides with the organisations processing data, not the individuals charged with its management. Since September 2023, the FADP has imposed sanctions for failing to adhere to essential data protection protocols. According to article 61 of the FADP, purposeful neglect of these security measures could incur fines up to 250,000 Swiss francs. Therefore, individuals who intentionally bypass these protocols are at risk of facing hefty penalties, enforced by the prosecuting authorities.

The duty to devise a comprehensive cybersecurity strategy, ensuring the establishment of an adequate organisational structure and the implementation of necessary policies, processes and safeguards, is allocated to the company's board of directors. This is especially pertinent for addressing cyberthreats that might affect the veracity of the company's financial statements. These issues should be managed by an internal control system, which might extend its remit beyond that typically required for statutory audits. As cybersecurity becomes increasingly critical, the responsibility for it cannot be solely attributed to the IT department. Board members and senior executives might face personal accountability to the company, its shareholders and creditors for any damages caused by a significant data breach – a consequence of failing to institute robust internal cybersecurity frameworks and procedures.

Law stated - 4 December 2024

Key definitions

5 How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

There is no definition in current Swiss law for the terms 'cybersecurity' and 'cybercrime'. However, article 3a of the former Ordinance on Protection against Cyber Risks in the Federal Administration defines 'cybersecurity' as 'the desired state in which data processing via information and communication infrastructures, in particular the exchange of data between persons and organisations, works as intended'.

Digital crime (commonly known as cybercrime) encompasses all digital offences, which primarily refer to criminal activities carried out on telecommunication networks, especially the internet. Digital crime covers five major areas: economic cybercrime, cyber sexual crimes, cyber damage to reputation and unfair practices, the dark net and a category called 'other'.

Law stated - 4 December 2024

Mandatory minimum protective measures

6

What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

According to article 8 of the FADP, data controllers and processors must ensure the security of personal data against risks through appropriate organisational and technical measures. These measures should prevent any data security breaches.

The FADP outlines broad protective measures, leaving significant leeway in defining specific minimum requirements, even in tightly regulated sectors such as critical infrastructures, where measures are seldom explicit. Organisations managing these infrastructures are considered most capable of determining and applying the necessary cybersecurity levels based on their unique operational risks. Government intervention is reserved for instances of self-regulation failure.

Law stated - 4 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Switzerland does not have specific laws addressing cyberthreats against intellectual property, but the Swiss Federal Copyright Act's article 39a forbids bypassing digital rights management (DRM) technologies that protect copyright material. DRM encompasses tools designed to prevent unauthorised access to and use of intellectual property, such as encryption and access control. It is illegal to create, distribute or promote methods for circumventing DRM. A federal surveillance office oversees DRM's impact, focusing on its misuse by industry rather than cyberthreats to intellectual property.

Law stated - 4 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Switzerland has implemented strategies and legislative measures to mitigate cyberthreats against critical infrastructure and specific sectors. This includes actions to protect vital information infrastructures from cyberrisks, part of a wider cybersecurity strategy encompassing the National Strategy for Protection against Cyber Risks. This strategy details actions for preventing cyberincidents, reducing vulnerabilities and mitigating the impact of cyberattacks. Furthermore, there is an act dedicated to safeguarding federal information and infrastructures from cyberthreats, setting standards that could influence the cybersecurity practices of private entities within critical sectors like finance, healthcare and transportation.

Additionally, the ISA aims to ensure the protection of federal information and information processing infrastructures against cyberthreats. While the ISA primarily applies to federal bodies, it also sets a benchmark for cybersecurity practices that can influence private sector entities, especially those operating within or in partnership with critical infrastructures.

Switzerland's approach to cybersecurity in critical infrastructure is comprehensive, involving regulatory measures, public-private partnerships and initiatives aimed at enhancing the cybersecurity posture of essential services across various sectors, including finance, healthcare, energy and transportation.

Law stated - 4 December 2024

Restrictions on cyberthreat information sharing

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In Switzerland, there are no specific regulations that expressly limit the exchange of information regarding cyberthreats. The nation's strategy for cybersecurity and data protection primarily revolves around the FADP and its associated Ordinance. These laws enforce the secure handling of personal data by requiring proper technical and organisational safeguards against unauthorised access, which broadly covers the management of cyberthreat information as well.

The NCSC, under the Federal Office for Cybersecurity, is instrumental in orchestrating responses to cyber incidents and aiding critical infrastructure operators in dealing with such challenges. This includes efforts to enhance public awareness and streamline the reporting and addressing of cybersecurity incidents.

The recent amendments to the FADP have provided the Swiss Federal Data Protection and Information Commissioner with greater powers for enforcing data protection standards. This includes the authority to investigate and mandate modifications in data processing practices, thereby indirectly affecting how cyberthreat information is handled and shared.

Furthermore, collaboration with entities like the government's computer emergency response team, GovCERT, is encouraged to facilitate the exchange of cyberthreat intelligence, especially for the safeguarding of vital IT infrastructures. This collaborative approach is intended to bolster collective defensive measures against cyberthreats.

To sum up, while explicit laws restricting the sharing of cyberthreat intelligence do not exist in Switzerland, the country's data protection and cybersecurity framework ensures that such information is managed securely, emphasising the protection of personal data and enhancing national cybersecurity resilience.

Law stated - 4 December 2024

Criminal activities

10

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The following cybercrimes are sanctioned pursuant to the Swiss Criminal Code:

- unauthorised obtaining of data (article 143);
- unauthorised access to a data processing system (article 143-bis);
- damage to data (article 144-bis);
- computer fraud (article 147);
- breach of secrecy or privacy through the use of an image-carrying device (article 179-quater);
- obtaining personal data without authorisation (article 179-novies); and
- breach of postal or telecommunications secrecy (article 321-ter).

The Telecommunications Act specifies criminal consequences for unauthorised use or sharing of private data received via telecommunications in article 50, setting up telecommunications systems to disrupt services as per article 51, and unauthorised data processing on external devices without user consent according to article 45c, all considered misdemeanours. Article 50 also criminalises spam as unfair competition.

Law stated - 4 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

While cloud services have significantly gained traction in Switzerland, the legal framework specifically targeting cloud computing security is not thoroughly developed. Instead, cloud security is broadly governed under the umbrella of general data protection regulations. This scenario places cloud service processing under the purview of third-party data processing rules, implying that personal data handled by cloud providers is subject to standard data protection obligations. Entities engaging cloud services (principals) are mandated to ensure their cloud providers adhere to stringent data security measures. This often includes, but is not limited to, verifying that the provider's security practices are up to par, a task that might necessitate security audits – a challenging feat given the nature of cloud environments.

The global nature of cloud computing introduces additional complexity, particularly when it involves transferring personal data across borders. In such cases, Swiss law mandates that personal data can only be shared internationally if it does not compromise subjects' privacy due to insufficient data protection laws in the recipient country. Nevertheless, the law also acknowledges that in the absence of equivalent privacy laws, cross-border data sharing via cloud services can still proceed, provided that alternative measures, such as contractual agreements, are in place to ensure an adequate level of data protection.

Law stated - 4 December 2024

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Switzerland does not have specific cybersecurity laws aimed at foreign organisations operating within its borders. However, under the country's legal framework, any foreign entity processing personal data in Switzerland or affecting Swiss residents must comply with the FADP. Additionally, foreign companies with Swiss branches must adhere to any sector-specific data security regulations. This approach ensures that all entities, regardless of their location, uphold the privacy and protection standards required within Switzerland when dealing with Swiss data.

Law stated - 4 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The National Cyber Security Centre (NCSC) has issued guidelines aimed at assisting small and medium-sized businesses. These recommendations cover a range of cybersecurity practices, including the elimination of malware, website clean-up procedures, secure practices for e-banking, and strategies to mitigate the impact of distributed denial-of-service attacks.

Law stated - 4 December 2024

Government incentives

14 How does the government incentivise organisations to improve their cybersecurity?

In addition to initiatives by the Cyber Security Delegate, the Swiss government engages in several key collaborations and programmes to bolster national cybersecurity. Among these efforts is the Swiss Cyber Experts group, a public-private partnership that brings together cybersecurity professionals from the information and communication technology and science sectors, spanning both public and private entities. Aimed at fortifying Switzerland's digital defences, this alliance works on various fronts to enhance security across the board.

Parallel to this, the Swiss Internet Security Alliance focuses on minimising the risk of malware infections within the country, striving to lower the overall rate of compromised

devices. This project represents a concerted effort to safeguard the digital ecosystem within Switzerland's borders.

For innovative cybersecurity solutions, Innosuisse plays a pivotal role. As the federal agency tasked with promoting science-based innovation, Innosuisse offers financial support, expertise and networking opportunities to projects at the forefront of cybersecurity research and development. This support underscores the government's commitment to fostering technological advancements and securing the nation's digital infrastructure.

Moreover, the establishment of a 'cyber defence campus' within Switzerland's federal technology institutes (ETH Zurich and EPFL Lausanne) signifies a substantial investment in the future of cybersecurity education and research. These campuses serve as hubs for cutting-edge studies and collaborations in the field, cementing Switzerland's status as a leader in cybersecurity excellence.

Law stated - 4 December 2024

Industry standards and codes of practice

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

Relevant industry standards, such as ISO 27001:2022, are available through the Swiss Association for Standardisation. Additionally, the NCSC offers supplementary advice on cybersecurity practices.

Law stated - 4 December 2024

Responding to breaches

16 Are there generally recommended best practices and procedures for responding to breaches?

In Switzerland, the legal framework for responding to breaches and implementing security measures includes provisions from the Federal Data Protection Act (FADP). While the FADP itself outlines general obligations for data security and breach notifications, specific procedures such as engaging third-party forensic firms, notifying affected parties and strategising post-breach responses align with the broader principles of data protection and privacy under Swiss law. Detailed regulations and best practices for breach response can be derived from guidelines issued by the Swiss Federal Data Protection and Information Commissioner (FDPIC) and the NCSC, which complement the legal requirements.

Law stated - 4 December 2024

Voluntary information sharing

17

Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Individuals and entities affected by cyberattacks are urged to communicate these incidents to, and collaborate with, the NCSC, which plays a crucial role in orchestrating efforts to mitigate the effects of cyberincidents.

Law stated - 4 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The national strategy for protecting Switzerland against cyberrisks, initially endorsed by the government in 2012 and updated in 2018, recognises a growing need within the industry for enhanced collaboration among public authorities, the private sector and critical infrastructure operators to mitigate cyberrisks. Stakeholders advocate for greater coherence in developing standards and procedures through collaborative efforts. The government emphasises that the primary responsibility for combating cyberattacks rests with individual organisational units, with authorities intervening only when public interests are jeopardised or when risks exceed the capacity of subordinate levels to address. Consistent with this strategy, the government participates in private initiatives aimed at promoting cybersecurity awareness and bolstering defence mechanisms.

Law stated - 4 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

In Switzerland, businesses have the option to take out cybersecurity insurance, for financial protection against the repercussions of cyberattacks and data breaches. The coverage offered by cyber insurance policies can differ, yet typically includes several key aspects:

- Protection against data breaches: costs for notifying impacted parties, credit monitoring services, restoring data and legal expenses tied to breaches are covered.
- Liability insurance: if a company faces lawsuits due to privacy violations or data breaches, this includes coverage for legal costs and settlements.
- Costs for recovery from cyberattacks: expenses for reinstating computer operations, fixing damage from malware or ransomware and compensating for revenue losses during downtime are covered.
- Protection against digital extortion: certain policies may reimburse ransom payments in ransomware incidents and cover negotiation costs with attackers.

- Crisis management costs: expenses for engaging cybersecurity experts, stakeholder communication and public relations efforts to preserve the company's image post-attack are included.

It is crucial for companies to understand that cyber insurance policies differ regarding coverage scope, liability limits and deductibles.

Law stated - 4 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In Switzerland, the regulatory authorities primarily responsible for enforcing cybersecurity rules include:

- the Swiss Federal Data Protection and Information Commissioner (FDPIC), which is responsible for enforcing data protection laws, including those related to cybersecurity, and ensuring compliance with the Federal Data Protection Act (FADP) and other relevant regulations. It oversees the processing of personal data and investigates data breaches and privacy violations; and
- the Swiss Cybercrime Coordination Unit, which is part of the Federal Office of Police and is responsible for coordinating efforts to combat cybercrime in Switzerland. It collaborates with national and international partners to investigate and prosecute cybercrimes, including those relevant to businesses and organisations.

Law stated - 4 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Regarding investigative powers, differentiation needs to be made between the general economy and regulated sectors. At a general level, the FDPIC possesses the authority to initiate investigations autonomously or upon request from a third party. The FDPIC holds investigative powers and various enforcement measures, including issuing injunctions (eg, halting specific data processing activities, providing information, prohibiting cross-border data transfers and mandating data security enhancements). In regulated sectors, regulatory authorities have expanded investigative powers within their respective domains. For instance, the Swiss Financial Market Supervisory Authority (FINMA) can designate independent experts to conduct audits of supervised individuals and entities. These entities are obligated to furnish the experts with all necessary information and documents to facilitate their duties.

Law stated - 4 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Phishing attempts are among the most frequently reported cyber incidents at the National Cyber Security Centre (NCSC). Cybercriminals use social engineering methods tailored to their target groups.

Most of the phishing-related complaints received by the NCSC relate to emails or text messages designed to look like they originate from Swiss Post, the SBB/SwissPass, banks or, more recently, booking.com.

For the moment, there is no legal provision in Switzerland that directly addresses these offences. They are treated in the same way as all other cybercrimes, and the NCSC also issues recommendations in their regard.

Law stated - 4 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

As of 1 September 2023, the FADP imposes an obligation to report breaches of data security that pose a significant risk to the privacy or fundamental rights of data subjects. This reporting obligation does not automatically require informing data subjects but is mandated only if ordered by the FDPIC or if it is deemed necessary to protect the data subject. However, sector-specific regulations may still require notification, as seen in the banking sector where the FINMA Circular 2023/01 mandates that banks establish a clear communication strategy in the event of serious incidents affecting the confidentiality of client-identifying data.

Law stated - 4 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The FADP includes clauses stipulating that disregarding fundamental data security prerequisites could result in criminal fines. Disregarding directives from regulatory bodies might amount to a criminal offence or result in administrative penalties, contingent upon the relevant legislation in force.

Law stated - 4 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In regulated sectors, the omission of mandatory report submission to regulatory bodies may result in criminal prosecution or administrative penalties, depending on the relevant legislation. Non-compliance with the reporting obligation outlined in the FADP could incur criminal penalties. Additionally, the failure to implement basic data security requirements is subject to criminal sanctions in the form of fines.

Law stated - 4 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Individuals who have fallen victim to cyberattacks have the option to pursue legal recourse through civil action against the perpetrator. This could involve legal action against the cybercriminal themselves or the entity responsible for failing to uphold adequate data security standards and protocols. Under the FADP, if it is determined that basic data security measures were neglected, the affected party has the right to file a criminal complaint, which could result in the imposition of a criminal fine.

Law stated - 4 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Personal data must be safeguarded against unauthorised processing through suitable technical and organisational measures, as outlined in the Federal Data Protection Act (FADP). Any system involved in processing personal data must adhere to state-of-the-art technical standards to mitigate the risk of unauthorised or accidental destruction, loss, technical vulnerabilities, tampering, theft, unlawful access, copying, use, alteration or other form of unauthorised processing. Systems employing automated processing of personal data are subject to additional requirements, including appropriate controls over access, disclosure, storage and usage. While the revised FADP enhances data security

requirements, it does not specify technical criteria. However, sector-specific regulations and guidance may offer more detailed technical requirements or recommendations.

Law stated - 4 December 2024

Record-keeping requirements

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The FADP does not expressly require companies to keep a record of cyberattacks. That said, it is in the interest of companies to document such events, so they can justify to the authorities that they have taken appropriate action in response.

Law stated - 4 December 2024

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

As of 1 September 2023, the FADP introduced a mandatory obligation to report data breaches to the Swiss Federal Data Protection and Information Commissioner (FDPIC). Data controllers are required to promptly notify the FDPIC when a data breach occurs and is expected to pose a significant risk to the privacy or fundamental rights of the data subject. Conversely, data processors must promptly report all breaches of data security to the data controller. However, this breach notification mechanism does not automatically mandate informing data subjects, as such action is only necessary for the protection of the data subject or if requested by the FDPIC.

Specific notification duties apply to certain sectors and critical infrastructures, for example:

- in the financial services sector, mandatory notification to the Swiss Financial Market Supervisory Authority is required without delay for events that are materially relevant for the supervision of the relevant supervised entity;
- in the telecommunications sector, notification to the National Emergency Operations Centre is required (no longer to the Federal Office of Communications) for faults in the operation of telecommunications networks that could affect at least 10,000 customers;
- in the aviation sector, notification to the Federal Office of Civil Aviation is necessary in the event of safety-related data breaches;
- in the railway industry, notification to the Federal Department of the Environment, Transport, Energy and Communications is required in the event of severe incidents; and
- in the nuclear sector, notification to the Swiss Federal Nuclear Safety Inspectorate is mandatory in the event of safety-related data breaches.

Law stated - 4 December 2024

Time frames

30 What is the timeline for reporting to the authorities?

Provisions tailored to specific sectors may obligate the involved entity to promptly notify authorities of any pertinent cybersecurity incidents. Under the FADP, it is mandated that breaches in data security, which could pose a significant risk to the privacy or fundamental rights of individuals affected, should be reported 'without undue delay'.

Law stated - 4 December 2024

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

As of 1 September 2023, the FADP includes regulations regarding the notification of data breaches. According to these regulations, the data controller might need to notify affected individuals about the breach if such notification is deemed necessary for protecting the data subjects or is demanded by the FDPIC.

Law stated - 4 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Developing cybersecurity regulations in Switzerland faces several principal challenges, reflecting both broader issues seen worldwide and those unique to the Swiss context:

- Balancing privacy with security: Switzerland has strong traditions of privacy and data protection. Crafting regulations that enhance cybersecurity without infringing on personal privacy rights is a delicate balance. This is particularly challenging given the global nature of cyberthreats, which may necessitate cross-border data flows and cooperation.
- Rapid technological advancement: the pace of technological change outstrips the speed at which regulations can be developed and implemented. Ensuring that laws remain relevant and effective in the face of evolving cyberthreats requires a flexible and forward-thinking approach.
-

Coordination across sectors and borders: cybersecurity threats do not respect sectoral or national boundaries, making coordination essential. Developing a regulatory framework that allows for effective cross-sector and international collaboration while respecting Switzerland's federal structure and neutrality is complex.

- Resource allocation: effective cybersecurity measures and the enforcement of regulations require significant resources. Allocating these resources efficiently, especially in a way that supports smaller businesses and organisations, poses a challenge.

Companies can help shape a favourable regulatory environment by:

- engaging in dialogue and actively participating in discussions with regulators and policymakers to share expertise and insights;
- promoting best practices by demonstrating effective cybersecurity measures and sharing knowledge across industries;
- supporting education and awareness through investment in cybersecurity education and awareness programmes to raise the overall security posture of the Swiss digital landscape; and
- collaborating on standards by working with standard-setting bodies and industry groups to develop and adopt cybersecurity standards that can inform regulations.

Throughout 2025, it is expected that cybersecurity laws and policies in Switzerland may evolve in several directions:

- Increased emphasis on critical infrastructure: given the global increase in attacks on critical infrastructure, Swiss regulations may focus more on protecting these vital sectors.
- Greater international cooperation: Switzerland may enhance its participation in international cybersecurity initiatives and agreements to tackle the cross-border nature of cyberthreats.
- Adoption of emerging technologies: regulations may begin to address the security implications of emerging technologies such as artificial intelligence, internet of things and blockchain more explicitly.
- Strengthening of reporting and compliance: the trend towards stricter reporting requirements and compliance checks for data breaches and cybersecurity incidents is likely to continue, possibly with more explicit guidelines and penalties for non-compliance.

These anticipated changes reflect the global trend towards strengthening cybersecurity defences and regulatory frameworks, with a recognition that cybersecurity is not just a technical issue but a critical component of national security, economic stability and personal privacy.

Law stated - 4 December 2024

EVERSHEDS SUTHERLAND

Markus Naef markus.naef@eversheds-sutherland.ch
Oliver Scharp oliver.scharp@ eversheds-sutherland.ch
Carol Tissot carol.tissot@eversheds-sutherland.ch
Nadine Zollinger nadine.zollinger@eversheds-sutherland.ch

Eversheds Sutherland

United Kingdom

Lawrence Brown, **Robert Allen**
Simmons & Simmons

Summary

LEGAL FRAMEWORK

Key legislation
Most affected economic sectors
International standards
Personnel and director obligations
Key definitions
Mandatory minimum protective measures
Cyberthreats to intellectual property
Cyberthreats to critical infrastructure
Restrictions on cyberthreat information sharing
Criminal activities
Cloud computing
Foreign organisations

BEST PRACTICE

Recommended additional protections
Government incentives
Industry standards and codes of practice
Responding to breaches
Voluntary information sharing
Public-private cooperation
Insurance

ENFORCEMENT

Regulatory authorities
Extent of authorities' powers
Most common enforcement issues
Regulatory and data subject notification
Penalties for non-compliance with cybersecurity regulations
Penalties for failure to report threats and breaches
Private enforcement

THREAT DETECTION AND REPORTING

Internal policies and procedures
Record-keeping requirements
Regulatory reporting requirements
Time frames
Other reporting requirements

UPDATE AND TRENDS

Recent developments and future changes

LEGAL FRAMEWORK

Key legislation

1 Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The United Kingdom does not have a comprehensive cybersecurity law – instead, cybersecurity requirements and obligations are set out in various legislation:

- The Network and Information Systems Regulations 2018 (NISR) impose security and incident reporting requirements on organisations that are operators of essential services (OESs) and relevant digital service providers (RDSPs). An RDSP is an online marketplace, online search engine or cloud computing service provider established in, or with a representative established in, the United Kingdom and which is not a micro or small enterprise. These organisations must have proportionate and effective security measures and procedures to ensure continuity of business services and effective incident reporting. Following a 2022 consultation of the NISR, the Financial Stability Board published an overview of responses ('-Achieving Greater Convergence in Cyber Incident Reporting'). No changes have, however, been implemented.
- The Communications Act 2003 requires public electronic communications services (ECS) and electronic communications network (ECN) providers to ensure the security of their networks and services, including incident mitigation. A Code of Practice has now been issued pursuant to section 105 of the Act.
- The Telecommunications (Security) Act 2021 amends the Communications Act 2003 and imposes new legally binding security requirements on ECN and ECS providers.
- The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 impose data security requirements on controllers and processors of personal data, and prescribe a risk-based approach to data security.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003, which implemented the European Union's ePrivacy Directive (2002/58/EC), place further obligations on ECS providers.
- The National Security and Investment Act 2021 sets out a new regime for permitting the UK government to scrutinise, block and add conditions to acquisitions and investments within sensitive sectors or locations potentially impacting on national security.

In respect of the financial services sector, the FCA Handbook also imposes a number of cybersecurity requirements on firms through its governance obligations.

Law stated - 11 December 2024

Most affected economic sectors

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Publicly listed companies and those within the financial services sector are subject to governance and security requirements which, either directly or indirectly, impose cybersecurity obligations upon them. The enforcement action that may be taken against such organisations can include significant fines and other sanctions, and there is significant reputational risk associated with such measures.

Operators of essential services (including in the energy, transport and health sectors) and digital service providers are subject to the additional cybersecurity and reporting obligations under the NISR. These organisations must implement appropriate technical and organisational measures to manage the cybersecurity risks to their networks and systems, and adopt measures that will enable them to mitigate the impact of incidents.

The UK government's National Cyber Strategy 2022 highlights the interaction between established sectors of the economy and new and unregulated businesses (eg, electric vehicle charging or those that provide microgeneration) as an area of potential concern, with the diversification of the business landscape likely to result in fundamental changes to the regulatory approach to cybersecurity.

There are not currently any cybersecurity obligations that apply explicitly to professionals in the legal sector; however, firms will be subject to broader data protection legislation such as the GDPR when conducting their business.

Law stated - 11 December 2024

International standards

3 Has your jurisdiction adopted any international standards related to cybersecurity?

There are no mandatory ISO standards in the United Kingdom. However, organisations may adopt standards such as ISO 27001:2013 to evaluate which security measures are required to meet their obligations under the NISR. Similarly, adherence to the standards is a means by which data controllers can demonstrate compliance with their obligations under the GDPR and the Data Protection Act 2018.

Organisations also frequently elect to adopt ISO standards through contractual provisions, to demonstrate that their cybersecurity policies and procedures are sufficiently robust.

Law stated - 11 December 2024

Personnel and director obligations

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

There is no legislation that imposes direct responsibility for cybersecurity compliance on personnel and directors. However, directors of organisations that fail to adequately ensure cybersecurity may be held responsible under the Companies Act 2006, which requires directors to exercise reasonable skill, care and diligence in the performance of their functions.

Law stated - 11 December 2024

Key definitions

5 | How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Cybercrime encompasses two main types of criminal activities as defined by the government's National Cyber Strategy. First, cyber-dependent crimes, which are offences that can only be carried out with information and communications technology (ICT) devices, with these devices serving both as the means and the target of the crime. Examples include creating and spreading malware for profit, or hacking to steal, damage or destroy data and networks. Second, cyber-enabled crimes, which are traditional crimes that have their scale or reach amplified by the use of computers, networks or other ICT forms, such as fraud and data theft that are facilitated by technology. The National Cyber Strategy defines 'cybersecurity' as the protection of internet-connected systems (including hardware, software and associated infrastructure), the data on them and the services they provide, from unauthorised access, harm or misuse.

The NISR relate to the security of network and information systems and therefore amount to cybersecurity obligations. However, information security requirements under the NISR also include other system and environmental considerations (eg, management of system failure, human error and natural events).

Law stated - 11 December 2024

Mandatory minimum protective measures

6 | What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The UK GDPR does not prescribe specific security measures that organisations must have in place; firms must implement appropriate technical and organisational measures to ensure the security of personal data, which may include measures such as encryption or pseudonymisation of data.

Organisations that fall within the NISR must also take appropriate and proportionate technical and organisational measures to ensure that risks to their systems are managed. In addition, the NISR provide for obligations relating to:

- the security of network and information systems and facilities;
- incident handling (including detection procedures and incident reporting);

- business continuity management (including disaster recovery capabilities);
- monitoring, auditing and testing (including processes to reveal flaws in the security mechanisms used to protect the network and information systems); and
- compliance with international standards relating to the security of network and information systems.

Law stated - 11 December 2024

Cyberthreats to intellectual property

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no legislation that specifically addresses cyberthreats to intellectual property. However, the National Cyber Strategy specifically identifies the protection of intellectual property in critical cyber technologies as an objective, with a particular focus on the sectors mentioned in the National Security and Investment Act, including artificial intelligence, communications and cryptographic authentication.

Law stated - 11 December 2024

Cyberthreats to critical infrastructure

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The NISR apply to OESs in a number of sectors (including energy, transport and health) and RDSPs and provides that organisations must take appropriate and proportionate technical and organisational measures to manage risks posed to their network and information systems, including measures to mitigate the impact of incidents. The NISR also impose reporting standards on these organisations, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring. Compliance with the NISR is actively monitored by the designated authorities (including the Information Commissioner's Office (ICO)) and the United Kingdom has adopted an audit framework in respect of OESs and RDSPs to ensure compliance with the relevant requirements.

In respect of the financial services sector, the 'Senior Management Arrangement Systems and Controls' section of the FCA Handbook applies to providers of financial services infrastructure, and requires firms to have effective and proportionate risk-based systems to combat financial crime.

Law stated - 11 December 2024

Restrictions on cyberthreat information sharing

9

Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Investigatory Powers Act 2016 criminalises the unlawful interception of communications within the United Kingdom. The Act also limits the sharing of information lawfully obtained by UK law enforcement bodies and intelligence agencies via interception. It is a criminal offence under the Act for communication service providers or public officials to disclose the existence and content of a warrant or authorisation where a government agency has, under a bulk or targeted warrant, intercepted communications in the interests of national security or for the prevention of serious crime.

The Counter-terrorism Act 2008 covers disclosure of information to the intelligence services for the purposes of national security or the prevention of serious crime.

The UK GDPR and the Data Protection Act 2018 only permit personal data sharing to law enforcement authorities where it is necessary and proportionate. Except where the ICO determines that publication is in the public interest, the ICO is prohibited from publicising information disclosed to it via a personal data breach notification that relates to any identifiable individual or business that is not already in the public domain.

Article 8 of the Human Rights Act, which deals with an individual's right to privacy, can be interfered with by a public authority only where it can be shown that such interference is lawful, necessary and proportionate to protect national security.

Law stated - 11 December 2024

Criminal activities

10 What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The Computer Misuse Act 1990 is the primary cybercrime legislation in the United Kingdom. The Act criminalises unauthorised access to computer networks, such as hacking; intention to commit a cybercrime; modifying, removing or ransoming data; and aiding computer misuses. A consultation on the Act took place between 7 February and 6 April 2023. It was concluded that the law is generally sufficient, but some proposals for change were made and are due to be considered further when parliamentary time allows. These include, for example, the prevention of symmetrical domain creation, and the possibility of introducing a statutory power to allow law agencies to take down or seize domains associated with criminal activity. It therefore appears as though there are some changes on the horizon, but these are yet to be documented in greater detail.

Section 3 of the Investigatory Powers Act criminalises the unlawful interception of communications within the United Kingdom.

In relation to personal data processing, the Data Protection Act 2018 creates a number of offences, such as unlawfully obtaining personal data, knowingly or recklessly disclosing personal data without the consent of the data controller, and selling personal data obtained illegally. Fraud by false representation, which could cover certain phishing incidents, is punishable under the Fraud Act 2006.

Law stated - 11 December 2024

Cloud computing

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The NISR specifically govern certain categories of digital services, including cloud computing services, and aim to establish a common level of security for network and information services.

The National Security and Investment Act 2021 allows the government to scrutinise and intervene in acquisitions of control of companies involved in 17 'sensitive areas of the economy', where there is a potential impact on the United Kingdom's national security. One such area is cloud computing. The rules came into force on 4 January 2022, although they can be enforced retrospectively for deals that were completed on or after 12 November 2020. Completion of a notifiable acquisition without approval could lead to criminal or civil penalties.

The United Kingdom's National Cyber Security Centre offers a framework to organisations in the UK public sector built around 14 cloud security principles that cover how organisations should configure, deploy and use cloud services securely.

Law stated - 11 December 2024

Foreign organisations

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The NISR apply to OESs and RDSPs outside of the United Kingdom that offer services in the United Kingdom, and require these organisations to nominate a representative to the relevant competent authority for enforcement purposes.

The CMA has extraterritorial effect in relation to offences with a significant link to the United Kingdom (ie, where the accused was in the United Kingdom when the offence was committed, or the unauthorised action was committed or the target computer was located in the United Kingdom). The Serious Crime Act 2015 amended the CMA to provide for additional extraterritorial powers where there is a significant link. A significant link is established if the conduct in question caused serious damage of a material nature in the United Kingdom. Additionally, if the accused is a UK national and commits an offence while outside of the United Kingdom under the law of another country, then a significant link is established.

The Investigatory Powers Act also provides for extraterritorial application in respect of communications carried out in the United Kingdom (ie, where an individual in the United Kingdom is communicating with persons in other jurisdictions). UK law enforcement

agencies may issue warrants under the Act to overseas service providers for data, the interception of communications or the monitoring of computer equipment.

Foreign organisations will be subject to the UK GDPR, including its security requirements, if they offer goods or services to individuals in the United Kingdom. Personal data transferred from the United Kingdom to organisations in third countries must be subject to appropriate safeguards, which typically involves the execution of standard data protection clauses, including provisions covering security measures, between the exporting and importing organisation. The ICO published a new form of International Data Transfer Agreement to be used for this purpose (which received parliamentary approval on 21 March 2022).

Companies should also be mindful of the Cyber (Sanctions) (EU Exit) Regulations 2020, which, among other things, prohibit cybervity with sanctioned companies where the object or effect is to directly or indirectly undermine the integrity, prosperity or security of the United Kingdom.

Law stated - 11 December 2024

BEST PRACTICE

Recommended additional protections

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Enhanced cybersecurity protections, beyond those mandated by law, are recommended by numerous authorities, with guidance notes and advice widely available.

The National Cyber Security Centre is an organisation within the UK government that provides advice and support for the public and private sector to promote cybersecurity. The central pillar of its advice is 'Cyber Aware', which provides a set of guidelines built around six key actions. In addition, it also maintains '10 Steps to Cyber Security', guidance aimed at medium-sized to large organisations that employ cybersecurity professionals, and a 'Small Business Guide: Cyber Security'. On top of this, the Centre publishes various focused guides on passwords, ransomware, phishing, devices, personal data malware, operational security and the cloud.

Other authorities also recommend enhanced protections. The Global Cyber Alliance, Action Fraud, the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) are among other authorities that also recommend protections beyond those strictly mandated by law.

It should be noted that while industry and regulatory codes or guidance do not constitute protections mandated by law, failure to follow such codes may still give rise to adverse consequences. For example, the ICO states, in its Regulatory Action Policy, that failure to follow an approved or statutory code of conduct is an aggravating factor when it considers sanctions. It is also worth noting that on 9 December 2022, the UK government published a Code of Practice for app developers and app store operators, which sets out practical steps designed to protect users. Parts of the Code were developed in conjunction with the ICO, and certain principles contained therein are mandated through existing legislation.

Law stated - 11 December 2024

Government incentives

14 | How does the government incentivise organisations to improve their cybersecurity?

On 19 January 2022, the government published a policy paper titled '2022 Cyber Security Incentives and Regulation Review'. In that it noted that it was for the market to incentivise better security practices for organisations, but recognised that those incentives (eg, consumer pressure and competitive advantage) have not yet formed effectively. To mitigate this, the government plans to take a more interventionalist approach through guidance, further market participations and strengthening of UK cyber legislation. In June 2023, the government published a research paper titled 'Cybersecurity in the UK', which in part supplements the 2022 policy paper.

At the CyberUK 2024 conference, the UK government unveiled initiatives as part of its £2.6 billion National Cyber Strategy to enhance artificial intelligence (AI) model security, aiming to set a global benchmark against hacking and sabotage. These efforts, emphasising the secure development and operation of AI, are bolstered by research and a public consultation on AI cybersecurity from May to July 2024, highlighting the government's commitment to leading in cyber technology and ensuring AI's safe utilisation.

Law stated - 11 December 2024

Industry standards and codes of practice

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The National Cyber Security Centre publishes a guide dealing with issues such as cyber defence, threat and ransomware. The Centre's '10 Steps to Cyber Security' sets out a number of key areas for medium-sized to large organisations to ensure that technology, systems and information are protected against cyberattacks. In doing so the guide emphasises the need to take a risk-based and proactive approach to cybersecurity.

Organisations operating within the regulated financial services sector are also guided by a range of materials produced by the FCA in order to achieve compliance with its Principles, and the standards set out in the 'Senior Management Arrangement Systems and Controls' section of the FCA Handbook. One such example is the FCA's publication on 'Good Cyber Security – The Foundations', which demonstrates the FCA's approach to working with other organisations (namely, the National Cyber Security Centre) in order to achieve effective levels of cybersecurity within the sector.

Law stated - 11 December 2024

Responding to breaches

16 | Are there generally recommended best practices and procedures for responding to breaches?

The best way to mitigate the impact of a data breach is to ensure you are properly prepared. A number of public organisations have published guidance for responding to data breaches (including the ICO and the National Cyber Security Centre). You should already have a detailed cybersecurity policy and within that should be a data breach response plan. Such a plan should be accessible to all employees and form part of standard onboarding training.

The first recommended step is to identify the extent of the breach and preserve relevant evidence. Although it may seem basic, it is important to document how the breach was identified and keep a careful note of steps taken. Such steps might include ensuring the correct internal stakeholders have been contacted (eg, HR, security), determining whether the breach contained personal data, and identifying which jurisdictions may have been affected. Answering these questions will inform the scope of external bodies that need to be involved in the crisis response team (eg, forensic experts to track the extent of the breach).

Where the target of the attack has in place cyber insurance cover (specifically, breach response), it should notify its provider promptly and ensure that no steps are taken without the relevant insurer's consent. Doing so may put the insured entity in breach of the terms of its policy, which in turn may jeopardise its entitlement to cover.

Next, your focus should shift to analysis – that is, understanding the ‘how’. For example, how did the breach occur and is it ongoing? If so, what steps need to be taken to fix (or ‘patch’) the breach? At this stage, you should consider whether stopping the breach might ‘tip off’ the attacker and lead to the destruction of evidence; this should be balanced against your data protection duties. You should also consider any external and internal communications. For example, you might want to consider a formal press release, or an internal notice reminding employees of the sensitivities of publicly discussing the breach with the media.

Again, consideration should be given here to any cyber insurance and relevant claims conditions that may apply.

You should then consider the remedies and next steps available to you. Depending on the circumstance of the breach, this can range from initiating legal action to instigating a PR strategy.

Lastly, you should consider your long-term response. If the breach identified any holes in your security system or staff training, these should be addressed as a matter of urgency. You should also reflect on whether you need to strengthen the relationships with necessary third parties; you may want, for example, to have forensic experts or legal counsel on retainer for data breaches.

Law stated - 11 December 2024

Voluntary information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

It is considered best practice to share information on cybersecurity threats, although this usually occurs after the threat has been properly resolved. You can share this information informally, for example through social media, or more formally on a voluntary basis to Action Fraud or the National Cyber Security Centre.

Law stated - 11 December 2024

Public-private cooperation

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The UK government's National Cyber Strategy 2022 sets out an aim for the United Kingdom to establish itself as a global cyberpower, which includes strengthening the UK cyber ecosystem between government, academia and industry. The Strategy intends to build on the existing relationships between the National Cyber Security Centre and industry stakeholders, most notably the regional cyber clusters formalised by the UK Cyber Cluster Collaboration.

Industry experts have also organised to help direct the UK technology sector. In particular, techUK (the United Kingdom's technology trade association) brings together organisations to enhance government collaboration and accelerate innovation. techUK has over 800 members across the United Kingdom, from sector leaders, such as Amazon and DeepMind, to law firms and emerging start-ups.

Law stated - 11 December 2024

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Insurance for cybersecurity breaches is available in the jurisdiction and has become more prevalent and available in the past six or so years. As at the date of writing, the cyber insurance market remains in a hard state. Previously, insureds that suffered cyberattacks or were involved in cyberincidents would try to claim under their existing commercial insurance policies (eg, those relating to property or commercial risks). While some of these 'silent' cyber risks could attach, many would not fall within cover. This state of affairs helped drive the 'affirmative' cyber insurance marketplace forward. However, given the ever-increasing frequency of ransomware attacks, the likelihood that insurers will eventually cease to provide cover for this particular type of risk is greater than ever. Overall, cyber insurance is becoming increasingly common, as threat actors and the attacks they deploy are more sophisticated now than ever before.

Law stated - 11 December 2024

ENFORCEMENT

Regulatory authorities

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

A number of authorities share this responsibility. The National Cyber Crime Unit (which operates within the National Crime Agency) is responsible for responding to the most critical cyberincidents and also pursues longer-term activity against cybercriminals. The Information Commissioner's Office (ICO) enforces cybersecurity rules where they involve personal data (through the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018), and enforces the Network and Information Systems Regulations 2018 (NISR). Industry-specific regulators (eg, the Financial Conduct Authority (FCA)) may enforce cybersecurity rules where a breach falls within their jurisdiction. Criminal prosecutions are (with some limited exceptions) carried out by the Crown Prosecution Service.

Law stated - 11 December 2024

Extent of authorities' powers

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Authorities have relatively wide-ranging powers to monitor compliance, conduct investigations and support prosecutions. The ICO has statutory powers as set out in the Data Protection Act 2018 (Parts 5 and 6). Among other things, it is empowered to conduct compliance assessments, issue information requests, enter premises, call for documents and interview staff. It is a criminal offence to obstruct a person executing an ICO warrant. Sector-specific regulators have certain similar powers, which vary between regulators and are provided for by statute (eg, the FCA).

Where criminal proceedings are on foot or in contemplation, the power of authorities to monitor and investigate are the same as those for criminal investigations generally.

Law stated - 11 December 2024

Most common enforcement issues

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The National Cyber Security Centre has identified ransomware as the most significant cyberthreat facing the United Kingdom since 2021. The government's 'Cyber Security Breaches Survey (2022)' notes that despite phishing being the most common type of breach, ransomware continues to be identified as the biggest threat by private

organisations. The UK government's National Cyber Strategy 2022 makes clear that ransomware attacks continue to become more sophisticated and damaging, making identification, and therefore enforcement, all the more difficult.

As expected, there has been a return to pre-covid 19 pandemic levels of regulatory action. Fines following a cyberattack generally concern the lack of preparedness for the incident through failure to have put in place adequate preventative measures or efficient incident response systems. The Information Commissioner fined Interserve £4.4 million in October 2022 for failure to put appropriate measures in place to prevent a cyberattack (which happened over three years earlier). Meanwhile, the FCA fined Equifax Limited over £11 million in October 2023 for 'failing to manage and monitor the security of UK consumer data it had outsourced to its parent company based in the US'. This fine was in relation to the huge 2017 data breach suffered by Equifax Inc, and cybersecurity incidents at providers of outsourced services (including data processors) are increasingly affecting companies (the recent Capita breach is a good example). Within the private sector, efforts are being made to address this through stricter cyber due diligence and audit of entities in supply chains.

Law stated - 11 December 2024

Regulatory and data subject notification

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data. A notification to the ICO is not required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business that is subject to the breach must also inform those affected individuals without 'undue delay' and, in practice, this should be done as soon as possible.

While the obligations under the UK GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services Regulation.

Law stated - 11 December 2024

Penalties for non-compliance with cybersecurity regulations

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Cybersecurity law in the jurisdiction has not been centrally codified and instead is based on a legal framework comprising numerous statutory enactments. It is therefore difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

By way of an example, however, the NISR impose obligations on operators of essential services and relevant digital service providers. The former operate services that are deemed critical to the economy such as energy, water and transport. The latter operate (among others) online marketplaces and provide cloud computing services. The NISR require these entities to have sufficient security systems in place, and allow a competent authority (the ICO) to impose penalties for breaches of its provisions.

Where, for example, there has been a material contravention of the regulations, which is deemed to have caused (or could cause) an incident resulting in the disruption of service for a significant period of time, penalties of up to £8.5 million may be imposed. If the disruption results in an immediate threat to life or a significant adverse impact on the economy, the penalty could be up to £17 million.

Law stated - 11 December 2024

Penalties for failure to report threats and breaches

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Again, the absence of a centrally codified cybersecurity law makes it difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

Most of the relevant regulations impose obligations to report either threats or breaches and in doing so, give competent authorities the power to issue penalties (usually in the form of enforcement notices). By way of an example, the NISR require incidents to be reported without undue delay. If, however, a failure to do so amounts to a 'material contravention', the penalty could, in theory, be up to £17 million in certain circumstances. Where personal data is involved, the Data Protection Act 2018 and the UK GDPR will also be relevant.

Law stated - 11 December 2024

Private enforcement

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The UK GDPR gives you a right to claim compensation if you have suffered damage as a result of breach of data protection laws. 'Damage' includes material and non-material damage, meaning financial loss or suffering distress (an arguably low bar). In the first instance, you should contact the individual or company who held your data at the time of the breach; they may agree to pay you without further action. If they don't, you might consider bringing formal proceedings (although you should take independent legal advice before doing so).

Law stated - 11 December 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

UK legislation does not mandate specific policies or procedures in this respect. The security principle set out in the UK General Data Protection Regulation (GDPR) requires organisations to process personal data securely by implementing appropriate technical and organisational measures. Similarly, the Network and Information Systems Regulations 2018 (NISR) requires operators of essential services (OESs) and relevant digital service providers (RDSPs) to undertake measures to manage the risks posed to the security of their networks. Under the UK GDPR and the NISR, organisations should assess the security risk associated with their own operations and implement appropriate controls, which could be in the form of organisational policies, physical and technical measures and/or conducting risk analysis.

Organisations regulated by the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) will need to comply with the data security obligations set out in the Financial Services and Markets Act 2000 and are required to have in place adequate systems and controls to monitor, detect and prevent financial crime.

Law stated - 11 December 2024

Record-keeping requirements

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the UK GDPR organisations are required to record all personal data breaches, regardless of whether they are reported to a regulator. There is no specific rule on format or timing for retaining the records, although the record must contain the facts relating to each data breach, its effect and the remedial action taken.

Under the Privacy and Electronic Communications Regulations), the Information Commissioner's Office (ICO) requires that communications network and service providers keep a log of any personal data breaches, and that they submit this to the ICO on a monthly basis. The log should contain the facts of the breach, the consequences and any remedial action taken.

Under the NISR, regulated entities must maintain records evidencing the appropriate and proportionate technical and organisational measures taken to manage risks to their systems. The NISR do not prescribe any format or retention period for these records. Records should be accurate and accessible to the competent authority.

Law stated - 11 December 2024

Regulatory reporting requirements

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

For breaches that compromise network security, the NISR require OESs and RDSPs to notify the ICO of security incidents without undue delay. The government has consulted on changes to the NISR which would require enhanced cyberdent reporting to other regulators, such as Ofcom and Ofgem. An overview of responses to the consultation was published by the Financial Stability Board in April 2023.

In relation to cybersecurity breaches that involve personal data, the UK GDPR and the Data Protection Act 2018 require data controllers to notify the ICO without undue delay, and no later than 72 hours after becoming aware of the incident, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The notification must provide details of (1) the nature of the breach; (2) the organisation's Data Protection Officer (if relevant); (3) the likely consequences of the breach; and (4) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

The Privacy and Electronic Communications Regulations require telecoms and internet service providers to notify the ICO if a personal data breach occurs within 24 hours of becoming aware of the facts of the breach. The notification must include the name of the service provider, circumstances of the breach, nature and content of the personal data and the technical and organisational measures applied to the affected personal data.

The ICO website provides links for the reporting of incidents under the UK GDPR, Privacy and Electronic Communications Regulations and NISR.

The FCA also requires regulated organisations to notify the FCA and PRA in the case of a data security breach.

Law stated - 11 December 2024

Time frames

30 | What is the timeline for reporting to the authorities?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data. A notification to the ICO will not be required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business that is subject to the breach must inform those affected individuals without 'undue delay'. In practice, the notification to the data subject will be required as soon as possible provided the breach is sufficiently severe to be considered high risk.

While the obligations under the GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services Regulation.

The NISR also impose reporting standards on these organisations in essential services, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring.

Law stated - 11 December 2024

Other reporting requirements

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no generally applicable requirements to reports threats or breaches to industry, customers or the general public.

In relation to cybersecurity breaches that involve personal data, the UK GDPR requires data controllers to inform affected individuals about breaches that are likely to result in a high risk to their rights, without undue delay, after becoming aware of the incident. The communication must provide details of (1) the organisation's data protection officer (if relevant); (2) the likely consequences of the breach; and (3) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

Law stated - 11 December 2024

UPDATE AND TRENDS

Recent developments and future changes

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Cybersecurity affects all internet-enabled businesses, but imposing the same regulations on all market participants is not practical. To date, UK regulations have focused on critical service providers, with the National Cyber Security Centre issuing guidance to sectors of the economy such as the self-employed and small and medium-sized enterprises.

Cybersecurity regulations must also allow for flexibility and be technology-agnostic to enable emerging threats to be countered. It is in this spirit that the UK government is consulting on changes to the Network and Information Systems Regulations 2018 (NISR) to create a process for the government to designate unregulated organisations as being 'critical' and therefore subject to the NISR's requirements.

In 2022, the NISR underwent a consultation process, and on 13 April 2023 the Financial Stability Board published an overview of that process titled 'Achieving Greater Convergence in Cyber Incident Reporting'.

Law stated - 11 December 2024

Lawrence Brown lawrence.brown@simmons-simmons.com
Robert Allen robert.allen@simmons-simmons.com

Simmons & Simmons