Legal 500
Country Comparative Guides 2025

Cyprus
Data Protection & Cybersecurity

Contributor

Raphael Legal

Maria Raphael

Managing Director | maria@raphael.legal

Anastasia Georgiou

Lawyer | anastasia@raphael.legal

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Cyprus.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Cyprus: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Data Protection and Privacy:

- The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, commonly referred to as the General Data Protection Regulation ('GDPR'), is automatically binding to Cyprus. It was implemented by the Cyprus Law 125(I)/2018, on the Protection of Natural Persons with regard to the processing of personal data and on the free movement of such data, which entered into force on 31 July 2018 ('the National Law').
- The Law 44(I)/2019 implemented the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
- The Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the e-Privacy Directive') has been transposed into Cyprus Law with Part 14 of the Electronic Communications and Postal Services Law 112 (I) of 2004 ('the Electronic Communications Law').
  The Commissioner for the Protection of Personal Data ('the Commissioner') serves as the national independent supervisory authority in Cyprus, tasked with monitoring the implementation of Regulation (EU) 679/2016 (GDPR), as well as other regulations relating to the protection of individuals from the processing of personal data.
- The Law Regulating Electronic Communications and Postal Services 112(I)/2004, as amended (the "Telecoms Law"), regulates direct marketing activities with the use of electronic means, and forms part of the legal framework on data protection.
  The Office of the Commissioner for Regulation of Electronic Communications and Postal Regulation (the "Electronic Communications Commissioner") is responsible for the enforcement of this law as well as the Data Protection Commissioner (on matters relating to privacy).

Cybersecurity:

The Attacks on Information Systems Law of 2015 (Law 147(I)/2015)

- implements Directive 2013/40/EU and supplements the Cybersecurity framework, together with subsidiary legislation which ratifies the Convention on Cybercrime Signed in Budapest on 23/11/2001 (Law 22(III)/2020) and its additional protocols which criminalise acts of racist and xenophobic nature committed through computer systems (Law 26(III)/2004) (the "Cybercrime Laws").
- Supervisory and Enforcement Authority: The Cyprus police, which is designated as the national point of contact for the exchange of operational information with other EU Member States and relevant EU Bodies, handles urgent assistance requests and collects/transmits statistical data on offences, prosecutions, and convictions to the European Commission.

The NIS Directive (Directive (EU) 2016/1148), which had been transposed into Cyprus law via the **Security of Networks and Information Systems Law of 2020 (Law 89(I)/2020)**, has been repealed by the NIS2 Directive (Directive (EU) 2022/2555), also referred to as "NIS2 Directive."

NIS2 Directive:

- **Legal Reference:** (EU) 2022/2555 (NIS2 Directive)
- **Entry into force:** 16 January 2023
- **Applies from:** 18 October 2024
- **Deadline for transposition:** 17 October 2024
- **Supervisory Authority:** Digital Security Authority (DSA)

The NIS2 Directive replaces the original NIS Directive and significantly enhances cybersecurity requirements across the EU. On 10 April 2025, the National NIS2 Voted Law (hereinafter ''the NIS2 Voted Law'') was approved by the Plenary of the House of Representatives. Its official publication in the Official Gazette is expected within the coming weeks.

The NIS2 Directive applies to entities under any of the following four categories:

- Public and private entities of a certain size
- Certain public administration entities that provide electronic communications networks (PECNs), publicly available electronic communications services (PECSs), trust services, top level domain (TLD) name registries or domain name systems (DNS) services meet a national risk assessment
- Entities providing domain name registration services.
- Entities identified as critical entities under Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive), to the extent they also fall under the scope of NIS2.

The DSA, which will retain the role of the supervisory authority under NIS2, shall adopt the national cybersecurity strategy, which needs to be ratified by the Council of Ministers.

It shall also compile a list of essential and critical entities mandated to comply with the requirements (as well as entities providing domain name registration services) which shall be reviewed and be updated on a regular basis.

However, this shall be without prejudice to the obligation of entities to determine whether they fall within the scope of NIS2 and proceed with self-registration process based on the mechanism that will be prescribed by the DSA.

The NIS2 Directive introduces a broader scope by categorising entities as “essential” or “important,” with corresponding obligations such as:

- Cybersecurity risk management and governance measures;
- Mandatory incident notification to the DSA;
- Participation in cross-border cyber crisis response;
- Obligations to adopt certified ICT products and conduct risk assessments;
- Obligatory or voluntary cybersecurity information sharing mechanisms.

The EU Cybersecurity Act (CSA)

- **Legal Reference:** (EU) 2019/881
- **Appliers from:** 27 June 2019.
- **Overview:** aims to enhance the cybersecurity resilience and trustworthiness of the European Union. It includes two major elements:
- **Supervisory Authority in Cyprus:** DSA acting as the National Cybersecurity Certification Authority (NCCA).

a) Strengthening ENISA (European Union Agency for Cybersecurity):

2. ENISA is given a permanent mandate and is tasked with achieving a high common level of cybersecurity across the EU.
3. The agency helps develop and implement EU policies and laws, provides guidance and support for national authorities and EU institutions, and fosters cybersecurity cooperation among various stakeholders.
4. ENISA supports the development and implementation of EU-wide cybersecurity certification schemes for ICT products, services, and processes.

b) Cybersecurity Certification Framework:

This framework establishes voluntary cybersecurity certification schemes for ICT products, services, and processes. The goal is to create a digital single market by harmonizing cybersecurity standards across the EU and ensuring that ICT products comply with security requirements.

Certifications are categorized as basic, substantial, or high assurance levels, and they aim to protect the availability, authenticity, integrity, and confidentiality of data and services offered through these products.

The NCCA is responsible for supervising and enforcing EU cybersecurity certification schemes for ICT products, services, and processes. This includes oversight of conformity assessment bodies (CABs), handling complaints, authorising CABs, ensuring compliance, and imposing penalties where necessary. It collaborates with ENISA and the European Cybersecurity Certification Group (ECCG) and actively participates in EU-level coordination and peer review mechanisms. The NCCA also supports the development of Cyprus as a regional cybersecurity certification hub.

Cyber Solidarity Act

- **Legal Reference:** Regulation (EU) 2025/38
- **Entered into force:** 4 February 2025
- **Applicability:** 4 February 2025
- **Supervisory authority:** Digital Security Authority (DSA) as National Cybersecurity Certification Authority (NCCA)

It establishes a new EU framework for coordinated response and preparedness to large-scale cybersecurity threats. It supports mutual assistance between Member States and aims to enhance the Union's detection, situational awareness, and coordinated response capacity through the European Cyber Shield and a Cybersecurity Emergency Mechanism.

Directive on the Resilience of Critical Entities (CER Directive)

- **Legal Reference:** Directive (EU) 2022/2557
- **Entered into force**: 16 January 2023
- **Applicability:** 18 October 2024
- **Deadline for transposition**: 17 October 2024
- **Supervisory authority in Cyprus** : Civil Defence Authority

The CER Directive replaces Directive 2008/114/EC and introduces a legal framework to strengthen the resilience of critical entities that provide essential services in key sectors such as energy, transport, health, water, digital infrastructure, and public administration.

The directive requires Member States to adopt national strategies on the resilience of critical entities, designate competent authorities, and establish frameworks for risk assessments, reporting obligations, and cross-border cooperation. Entities covered by the directive must conduct their own risk assessments, adopt appropriate technical and organisational measures, and report disruptive incidents.

Digital Operational Resilience Act (DORA): Regulation (EU) 2022/2554 and Directive (EU) 2022/2556 (Amending Directive)

- **Entry into force:** 16 January 2023
- **Applies from:** 17 January 2025
- **Deadline for national transposition (Directive 2022/2556):** 17 January 2025
- **Competent Authorities:**

Cyprus has designated four competent authorities, each responsible for supervising specific segments of the financial sector:

a) Central Bank of Cyprus (CBC):

The CBC supervises credit institutions, payment institutions, electronic money institutions, and other entities under its purview.

b) Cyprus Securities and Exchange Commission (CySEC):

CySEC oversees Cyprus Investment Firms (CIFs), Central Securities Depositories, Trading Venues, Crypto Asset Providers (CASPs), Alternative Investment Fund Managers (AIFMs) and UCITs Management Companies (UCITS).

It has published guidance on DORA implementation and proposed annual ICT oversight fees for entities within its scope.

c) Insurance Companies Control Service (ICCS):

The ICCS supervises insurance and reinsurance undertakings, as well as insurance intermediaries.

d) Registrar of Occupational Retirement Benefit Funds:

This authority oversees institutions for occupational retirement provision (IORPs).

DORA is designed to consolidate and upgrade Information Communication Technologies (ICT) risk requirements throughout the EU financial sector to ensure that a wide range of participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations. DORA establishes requirements for dedicated ICT risk management capabilities, reporting of major ICT-related incidents, digital operational resilience testing, management by financial entities of ICT third-party risks, as well as information sharing among financial entities. It also introduces an EU oversight framework for critical ICT providers.

CySEC has issued detailed guidance outlining key aspects of DORA, including the scope of entities covered, the proportionality principle, and specific requirements on ICT risk management, incident reporting, resilience testing, and third-party risk. It has also clarified reporting expectations, especially for significant ICT-related incidents, and highlighted the relevance of upcoming Regulatory and Implementing Technical Standards (RTS/ITS) issued at EU level. CySEC's supervisory role will involve monitoring compliance, particularly among investment firms, trading venues, and other financial entities under its remit.

CySEC will also liaise with the European Supervisory Authorities (ESAs), namely EBA, EIOPA, and ESMA—on oversight activities, including the designation and supervision of critical ICT providers at EU level.

RED Delegated Act – Commission Delegated Regulation (EU) 2022/30

- **Legal Reference**: Commission Delegated Regulation (EU) 2022/30 of 29 October 2021
- **Entry into Force:** 1 February 2022 (20 days after publication in the Official Journal)
- **Applicability**: Initially set for 1 August 2024; postponed to 1 August 2025 to allow for the development of harmonised standards.
- **Overview**: This Delegated Regulation supplements Directive 2014/53/EU (Radio Equipment Directive) by activating essential requirements under Article 3(3), specifically points (d), (e), and (f), which relate to the

protection of the network, personal data, user privacy, and fraud prevention for certain categories of radio equipment.
- **Harmonised Standards and Conformity Assessment**: Depending on the nature and the intended purpose of the radio equipment, as well as the applicability of the essential requirements of the RED DA, presumption of conformity may be conferred through the use of harmonized standards. Otherwise, third party conformity assessment applies.
- **To be amended or repealed**: in order to avoid overlap with the CRA, the EC intends to repeal the Red Delegated Act.
- **Supervisory Authority:** Ministry of Communication & Works (MCW)-Department of Electronic Communications/Office of the Commissioner of Electronic Communications and Postal Regulation.

Data Governance and Emerging Data Regulations

Data Governance Act (DGA)

- **Legal Reference**: Regulation (EU) 2022/868
- **Entry into Force**: 23 June 2022
- **Applies from**: 24 September 2023
- **Overview**: Establishes mechanisms to facilitate data sharing across the EU, including the creation of data intermediaries and the reuse of certain public sector data.

European Health Data Space (EHDS)

- **Legal Reference**: Regulation (EU) 2025/327
- **Entry into Force**: 26 March 2025
- **Applies from**:
  - **26 March 2027**: Primary use provisions become applicable.
  - **26 March 2029**: Secondary use provisions become applicable.
  - **26 March 2031**: Extended applicability for certain data categories, such as medical imaging and genetic data.
- **Overview**: provides a common framework for the use of electronic health data by the industry across the EU, enhancing healthcare delivery and research.

Digital Platform and Consumer Regulation

Digital Markets Act (DMA)

- **Legal Reference**: Regulation (EU) 2022/1925
- **Entry into Force**: 1 November 2022
- **Applies from**: 2 May 2023
- **Overview**: Targets large online platforms acting as “gatekeepers," imposing obligations to ensure fair competition and prevent market abuse.
- **Supervisory Authority**: Commissioner for the Protection of Competition

Digital Services Act (DSA)

- **Legal Reference**: Regulation (EU) 2022/2065
- **Entry into Force**: 16 November 2022
- **Applies from**:
  - **25 August 2023**: Obligations for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).
  - **17 February 2024**: Obligations for other entities.
- **Overview**: Establishes a comprehensive framework for the regulation of intermediary services, focusing on content moderation, transparency for users and accountability of service providers.
- **Supervisory Authority**: Cyprus competent authorities, in addition to the Cyprus Television Authority (Digital Service Coordinator) include the Office of the Commissioner for Electronic Communications and Postal Regulation, the Ministry of Energy, Commerce and Industry and the Office of the Commissioner for Personal Data Protection.
- For further information on the DSA Services we provide, please refer to our website's Services section. https://www.privacyminders.com/services/dsa-legal-representative/

Product Safety & Liability

General Product Safety Regulation

- **Entered into force:** 12 June 2023
- **Applies from**: 13 December 2024

The General Product Safety Regulation replaces the former General Product Safety Directive (Directive 2001/95/EC) and introduces a modernised legal framework to ensure that all consumer products placed on the EU market are safe. It responds to the increased presence of online sales, connected devices, and complex supply chains, reinforcing the safety obligations of economic operators.

Key provisions include enhanced product traceability, clearer obligations for online marketplaces, mandatory accident reporting mechanisms, and improved recall procedures. The regulation also aligns product safety supervision across the EU and introduces stronger coordination between Member States and the European Commission, particularly through the Safety Gate rapid alert system.

Sector-Specific Regulations

Chips Act

- **Legal Reference**: Regulation (EU) 2023/1781
- **Entered into force**: 20 September 2023
- **Applies from:** 21 September 2023
- **Overview**: Establishes a framework to strengthen the EU semiconductor ecosystem, support innovation and reduce strategic dependencies.

Toys Safety Directive

- **Legal Reference**: Directive 2009/48/EC
- **Applies from:** 20 July 2011
- **Upcoming revision**: A proposal for a new Toys Safety Regulation was adopted by the European Commission in 2023.
- **Overview**: This Directive sets out safety requirements and conformity obligations for toys placed on the EU market to ensure a high level of protection for children's health and safety. It covers both physical and chemical risks and imposes responsibilities on manufacturers, importers, and distributors.
- **Supervisory authority:** Minister of Energy, Commerce, Industry & Tourism (MECIT), Competition & Consumer Protection Service

Regulation on Civil Aviation and Establishing EASA

- **Legal Reference**: Regulation (EU) 2018/1139
- **Entered into force:** 11 September 2018
- **Overview**: Sets common rules for aviation safety and establishes the European Union Aviation Safety Agency (EASA).
- **Supervisory authority**: Department of Civil Aviation

Vehicle Type-Approval Regulation

- **Legal Reference**: Regulation (EU) 2019/2144
- **Entered into force:** 5 July 2022
- **Applies from**: 7 July 2024
- **Overview:** Mandates advanced vehicle safety features like intelligent speed assistance, driver monitoring, and data event recorders.
- **Supervisory authority:** Department of Road Transport, Ministry of Transport, Communications and Works.

Medical Devices Regulation (MDR)

- **Legal Reference**: Regulation (EU) 2017/745
- **Entered into force**: 25 May 2017
- **Applies from**: 26 May 2021
- **Overview**: Establishes a regulatory framework for ensuring the safety and performance of medical devices placed on the EU market. It includes provisions related to software used as a medical device, cybersecurity requirements, and obligations to mitigate risks associated with connected technologies.
- **Supervisory authority**: Ministry of Health, Cyprus Medical Devices Competent Authority.

In Vitro Diagnostic Medical Devices Regulation (IVDR)

- **Legal Reference:** Regulation (EU) 2017/746
- **Entered into force:** 25 May 2017
- **Applies from:** 26 May 2022
- **Overview:** Establishes a strengthened regulatory framework for in vitro diagnostic medical devices to ensure safety, performance, and reliability. The IVDR introduces stricter requirements for conformity assessment, classification rules, post-market surveillance, and oversight of notified bodies. It also addresses the growing use of software and cybersecurity concerns in diagnostic tools.
- **Supervisory authority**: Ministry of Health, Cyprus Medical Devices Competent Authority

Note: Some of the listed laws and regulations, while not exclusively focused on cybersecurity, are included due to their cybersecurity-relevant provisions or their impact on digital infrastructure, product safety, or data governance. This note also applies to the instruments discussed under Question 2.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

CSA Revision

Current status: Public consultation open (11 April – 20 June 2025)

Planned adoption: Q4 2025

Supervisory Authority in Cyprus: Digital Security Authority (DSA) as National Cybersecurity Certification Authority (NCCA)

Currently, the European Commission is preparing a revision of this act to further clarify ENISA's mandate and improve the certification framework to enhance resilience. This revision is aimed at streamlining, simplifying, and supplementing EU legislation to make the cybersecurity framework more accessible to users and businesses. Additionally, the revised framework will prioritize measures to support the development of a secure and resilient supply chain, including the EU's cybersecurity industrial base.

The Cyber Resilience Act (EU) 2024/2847 (CRA)

- **Entry into force:** 23 October 2024
- **Applies from**: 11 December 2027
- **Earlier applicability date for manufacturers' reporting obligations**: 11 September 2026

It establishes rules for making products available on the market with digital elements to ensure their cybersecurity, essential cybersecurity requirements for the design, development and production of such products, and obligations for economic operators in relation those products with respect to cybersecurity. It also introduces essential cybersecurity requirements for the vulnerability handling processes put in place by the manufacturers to ensure the cybersecurity of such products during the time the products are expected to be in use, and obligations for economic operators in relation to those processes. Additionally, it sets our rules on market surveillance, including monitoring, and enforcement of the rules and requirements.

The essential cybersecurity requirements set out in the CRA include all the elements of the essential requirements referred to in Article 3 (3), points (d), (e) and (f) of the Radio Equipment Directive and activated by the RED Delegated Directive.

“Products with digital elements” include hardware or software products and their remote data processing solutions, including components placed on the market separately. “Software” refers to the computer code part of an electronic information system, while “hardware” refers to the physical system or components capable of processing, storing, or transmitting digital data.

The products with digital elements that completed the appropriate conformity assessment process, depending on their product category, will bear the CE marking.

Data Governance & AI Regulation

Data Act

- **Legal Reference**: Regulation (EU) 2023/2854
- **Entry into Force**: 11 January 2024
- **Applies from**: 12 September 2025
- **Overview**: Establishes harmonised rules on fair access to and use of data, aiming to unlock industrial data and foster a competitive data market. It complements the Data Governance Act by clarifying rights and obligations regarding data access and use.

EU Artificial Intelligence Act (AI Act)

- **Legal Reference**: Regulation (EU) 2024/1689
- **Entry into Force**: 1 August 2024
- **Applies from**:
  - **2 February 2025**: Provisions banning AI systems posing unacceptable risks.
  - **2 August 2025**: Requirements for general-purpose AI systems and related governance provisions.
  - **2 August 2026**: Obligations for high-risk AI systems become applicable.
- **Overview**: Introduces a risk-based framework for AI systems, categorising them into unacceptable, high, limited, and minimal risk levels, with corresponding obligations to ensure safety and fundamental rights.

Supervisory Authorities in Cyprus:

1. **Communications Commissioner**, designated as the Notifying and Market Surveillance Authority, serving as the Single Point of Contact for AI-related matters.
2. **Commissioner for Personal Data Protection**, responsible for overseeing AI applications within her remit, particularly those involving personal data processing.
3. **Commissioner for Administration and the Protection of Human Rights (Ombudsman)** tasked with ensuring that AI systems uphold fundamental rights.

Product Safety and Liability

Revised Product Liability Directive

- **Legal Reference:** EU Product Liability Directive 2024/2853
- **Entered into force**: 23 October 2024
- **Applies from:** 9 January 2027
- **Deadline for transposition:** 9 December 2026
- **Overview:** It introduces updated liability rules for defective products, including those involving emerging technologies such as software, AI systems, and digital services. It expands the scope of liability to better reflect the modern digital economy and the increasing reliance on interconnected and autonomous products.

Sectoral and Emerging Technology Regulation

Machinery Regulation (Regulation (EU) 2023/1230)

- **Entered into force**: 19 July 2023
- **Applies from**: 20 January 2027
- **Overview**: Replaces Machinery Directive 2006/42/EC. Updates safety rules for AI-integrated and autonomous machines.
- **Supervisory authority in Cyprus**: Currently Department of Labour Inspection, Ministry of Labour and Social Insurance

eIDAS2 Regulation (Regulation (EU) 2024/1183)

- **Entered into force**: January 2024
- **Applies gradually from**: 2025 onwards
- **Overview**: Updates the eIDAS framework to enable a European Digital Identity Wallet and improve cross-border trust services.
- **Supervisory authority in Cyprus**: Department of Electronic Communications, Ministry of Transport, Communications and Works

Digital Product Passport Regulation (upcoming – part of EU Ecodesign Regulation)

- **Expected adoption:** Late 2025
- **Overview:** Introduces a mandatory digital passport to provide product information for sustainability and circularity.

Digital Networks Act (DNA) – Forthcoming EU Regulation

Status: Legislative proposal expected in Q4 2025

Entry into force / applicability: To be determined

Overview: The DNA is a forthcoming EU regulation aimed at modernising the framework for electronic communications across the Union. It is expected to revise or replace aspects of the European Electronic Communications Code (EECC), simplifying rules on gigabit network deployment, spectrum management, and cross-border connectivity.

The Act will seek to harmonise infrastructure access conditions, accelerate permit procedures, and support strategic connectivity initiatives—such as 5G corridors and secure cross-border services.

CSIRT-CY: The national Computer Security Incident Response Team

In Cyprus, CSIRT-CY operates under the Digital Security Authority (DSA), serving as the central body for managing cybersecurity incidents and coordinating with EU frameworks.

It was originally established in the context of implementing the NIS Directive and the respective national law 89 (I)/2010.

Since then, the national CSIRT's role is expanded under the NIS2 Directive. The CSIRT is tasked with incident handling, providing early warnings, disseminating information to stakeholders, and participating in the EU CSIRTs Network to facilitate cooperation across Member States. The CSIRT's role is further enhanced by the following EU legislative frameworks:

- Cybersecurity Act: While primarily focused on ENISA and certification schemes, the CSIRT supports the implementation of EU cybersecurity certification frameworks and collaborates with relevant authorities to enhance national cybersecurity capabilities.
- Cyber Resilience Act: The CSIRT acts as a coordinator for vulnerability disclosures, facilitating communication between reporters and manufacturers to address identified vulnerabilities in products with digital elements.
- Digital Operational Resilience Act (DORA): The CSIRT contributes to the financial sector's resilience by assisting in the management of ICT-related incidents and supporting information sharing among financial entities.
- Cyber Solidarity Act: The CSIRT participates in the European Cybersecurity Alert System, collaborates in the Cybersecurity Emergency Mechanism, and contributes to the Cybersecurity Incident Review Mechanism to strengthen the EU's collective response to significant cyber threats.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Data Protection Laws

There are no registration or licensing requirements for entities under the data protection laws.

Cybersecurity Laws

DORA:

Under the DORA there are no new licensing or registration requirements introduced beyond the entities' existing financial regulatory authorisations. However, DORA imposes specific ongoing compliance obligations for digital operational resilience, which effectively function as a regulatory layer over the already licensed financial entities.

CySEC issued the circular C700 to inform the Regulated Entities of their reporting obligations:

a) Incident Reporting (Article 19 of DORA)

Entities must report major ICT-related incidents using a structured three-stage reporting process (Initial, Intermediate, and Final reports), following strict timelines.

There is also an option for voluntary reporting of significant cyber threats. The submission process includes using the templates ''Major ICT-related Incident Form'' and the ''Significant Cyberthreats Template (Voluntary)'' through the TRS system.

Failure to report such incidents in the required manner or within the required timeframe constitutes non-compliance, which may lead to regulatory sanctions or supervisory measures by CySEC.

b) Register of Information (Article 28 of DORA)

Regulated entities must maintain and annually submit a Register of Information detailing all contractual arrangements with ICT third-party service providers. This submission must follow CySEC's format and be completed through its XBRL Portal.

Entities that fail to maintain or submit this register risk regulatory breaches and may face enforcement action, especially if the omission undermines CySEC's oversight or the identification of systemic ICT risks.

For CySEC-supervised entities, the first submission deadline is 30 April 2025, with a reference date of 31 March 2025.

NIS2 Directive:

- DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking service platforms shall submit specific information set out in article 27 (2) of the NIS2 Directive to DSA.
- The DSA has yet to provide a specific platform or form for registration purposes. Until this happens, the above-mentioned entities are encouraged to provide such information by email, so that the DSA assesses whether they classify as critical or important entities.

Failure to submit the required information under Article 27(2) may subject entities to supervisory measures under Article 32 of the NIS2 Directive, including audits, inspections, mandatory remediation actions, and potentially administrative fines

AI Act:

It establishes mandatory registration obligations for specific actors involved in the development, deployment, and testing of high-risk AI systems. These registrations must be completed in the EU AI Database, established under Article 71 and maintained by the European Commission, unless otherwise specified.

a) Providers of High-Risk AI Systems: Article 49(1)

Before placing on the market or putting into service a high-risk AI system listed in Annex III (excluding point 2), the provider or, if applicable, the authorised representative shall register themselves in the EU AI Database and register the high-risk AI system, including required documentation.

b) Providers Concluding a System Is Not High-Risk: Article 49 (2)

If a provider determines that a system listed in Annex III is not high-risk under Article 6(3), they shall register themselves and the system in the EU AI database and provide a justification for the classification.

c) Deployers that Are Public Authorities or EU Bodies: Article 49(3) and Article 8

Before putting into service or using a high-risk AI system listed in Annex III (excluding point 2), public authorities, Union institutions, and their agents shall register themselves in the EU AI database, select the AI system from the database and register the intended use of the system in the database.

d) Critical Infrastructure (article 49 (5) and Annex III (point 2)

High-risk AI systems used for critical infrastructure must be registered at a national level, not in the EU AI database.

e) Real-Word Testing of High -Risk AI systems:

Prospective providers testing high-risk AI systems in real-world conditions must register the testing activity in the relevant section of the EU AI database (unless exempt) and submit a testing plan outlining safeguards, oversight, and risk mitigation measures.

f) Restricted Database Access for Certain Use Cases

For high-risk AI systems in areas such as law enforcement, migration, asylum, and border control (Annex III, points 1, 6, and 7), registration must occur in a non-public section of the EU AI database. Access is limited to the European Commission and national market surveillance authorities.

Organisations that fail to comply with the registration

obligations under Article 49 of the AI Act may be subject to penalties, including warnings and administrative fines, in accordance with Articles 99(1) and 99(2) of the Regulation. These penalties are to be established and enforced by Member States under their national legal frameworks, within the parameters set by the Regulation.

Digital Services Act (DSA):

Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate a legal representative in one of the Member States where offers its services.

Providers of intermediary services shall notify the name, postal address, email address and telephone number of their legal representative to the Digital Services Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is publicly available, easily accessible, accurate and kept up to date.

Failure to comply with an obligation under the Digital Services Act may lead to the imposition of fines at a maximum amount of 6 % of the annual worldwide turnover of the provider of intermediary services concerned in the preceding financial year.

The maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be 1 % of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year.

In view of the particular responsibilities and obligations of providers of online platforms, they should be made subject to transparency reporting obligations, which apply in addition to the transparency reporting obligations applicable to all providers of intermediary services under the DSA. Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period.

Providers of very large online platforms or of very large online search engines shall publish the comprehensible reports at the latest by two months from the date of application of the designation of the very large online platforms and very large online search engines, and thereafter at least every six months.

The Commission Implementing Regulation (EU) 2024/2835 of the Digital Services Act lays down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms. It also stipulates the reporting and retention period of the transparency reports.

4. How do the data protection laws in your jurisdiction define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”)? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., “controller”, “processor”, “data subject”, etc.)?

Personal Data means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Data subject means the individual that the personal data relates to.

There is no special definition for personal data of special category.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

- **Lawfulness, fairness and transparency**: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Lawful basis for processing**: Processing of personal data shall be lawful only if and to the extent that at least one of the following legal bases apply:
  - the data subject has given consent to the processing for one or more specific purposes;
  - processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract;
  - processing is necessary for compliance with a legal obligation of the controller;
  - processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (It must be noted that, according to derogations allowed under the GDPR, the National Law states that the processing of personal data is lawful when carried out by the courts acting in their judicial capacity for the purpose of serving justice. This includes processing necessary for the purpose of publishing or issuing a court judgment. Additionally, the processing of personal data is lawful when carried out by the Parliament in the context of its powers.); or
  - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
- **Storage limitation**: Personal data shall be retained in a format that allows for the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for extended periods if the processing is solely for archiving purposes in the public interest, scientific, historical research purposes or statistical purposes. However, such extended storage shall be subject to the implementation of appropriate technical and organisational measures mandated by GDPR to safeguard the rights and freedoms of the data subject.
- **Integrity and confidentiality**: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage.
- **Accountability**: The controller shall be responsible for and be able to demonstrate compliance with the data protection principles set out above.
- **Proportionality**: This is a key concept in the GDPR, ensuring that the regulation does not go beyond what is necessary to achieve its objectives. It requires that only personal data, which is proportionate, relevant, compatible and necessary for the purposes of the processing is collected and processed. In the context of fundamental rights, proportionality requires that the advantages of limiting a right are not outweighed by the disadvantages to the exercise of that right.
- **Data protection by design and by default**: A controller shall implement appropriate technical and organisational measures designed to implement the data protection principles into the personal data processing.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Consent is required when processing involves special categories of personal data, like health or biometric data

under the GDPR, or when data is used for marketing purposes, profiling, or transferred to third parties for their own use—particularly for marketing or analytics. Specific laws, also require consent for cookies and similar tracking technologies.

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations.

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

If the processing can't meet the requirements for valid consent and no other basis applies, then the processing should not occur at all.

Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given.

Informed consent must clearly explain who is collecting the data, what data is being collected, why and how it will be used, who it will be shared with, how long it will be retained, and the data subject's rights, including the right to withdraw consent. It must be as easy to withdraw consent as it is to give it.

Consent cannot be bundled with terms of service or other agreements if the data processing is not necessary for performing the service. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. It must be separate, allowing users to opt in to individual purposes such as marketing, analytics, and profiling. Data controllers must always select the lawful basis that most accurately reflects their relationship with the individual and the purpose of processing. If another lawful basis is more appropriate, consent cannot be implied.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Under **GDPR Article 9**, special categories of personal data include:

- **Health data**
- **Biometric data** (for identification)
- **Genetic data**
- **Racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Trade union membership**
- **Sex life or sexual orientation**

Additionally:

- **Children's data** gets **special protection** under GDPR Article 8 and equivalent laws, especially in relation to consent.

Processing special category data is **prohibited by default**, **unless** one of the **Article 9(2) exceptions** applies, such as:

1. **Explicit consent** of the data subject.
2. Processing is necessary for **employment, social security, or social protection law**.
3. Necessary to protect the **vital interests** of the data subject or another person.
4. Carried out by a **not-for-profit** with a legitimate aim (e.g., religious organization).
5. Data made **manifestly public** by the individual.
6. Necessary for **legal claims**.
7. Necessary for **public interest** reasons in the area of public health.
8. For **archiving, research, or statistics** under appropriate safeguards.

Children's Data

- Processing personal data of children **under 16** (can be lowered to 13 by member states) for **information society services** requires **parental consent**.
- Controllers must take steps to verify the age and parental consent.
- Language must be clear and understandable to a child.

When the provision of information society services directly to a child is based on the child's consent, the

processing of personal data is lawful if the child is at least 14 years old according with the National Law.

For a child younger than 14 years old, the processing of personal data shall be lawful when consent is given or authorised by the holder of parental responsibility.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The national law does not introduce any derogations from the GDPR in relation to the following GDPR articles:

- Article 4(7) and (9) (Definitions – Controller and Main Establishment)
- Article 6(4) (Further processing)
- Article 17(1)(e) and (3)(b) (Right to erasure)
- Article 22(2)(b) (Automated decision-making)
- Article 26(1) (Joint controllers)
- Article 28(3), first sentence, (a), (g) and (4) (Processor obligations)
- Articles 29 and 32(4) (Processing on instructions and security)
- Article 40(1) (Codes of conduct)
- Article 42 (Certification)
- Article 51(3) in conjunction with Article 68(4) (Supervisory authorities)
- Articles 52(4)-(6), 57(1)(c), and 80(1)-(2) (DPO independence and representation of data subjects)
- Articles 87, 88, 90(1), and 91(2) (National ID number, employment, secrecy, and religious associations).

The National Law introduces the following derogations to the GDPR Articles:

Article 6(1)(c) and (e): Processing is lawful when carried out by courts acting in a judicial capacity, or by Parliament in the exercise of its powers, for the purpose of serving justice or publishing court decisions.

Article 8(1): The age of digital consent for information society services is set at 14 years in Cyprus. For children under 14, parental authorization is required.

Article 9: Cypriot law prohibits the processing of genetic and biometric data for health and life insurance purposes. When such processing is based on consent, separate consent is required for further processing.

Article 10: The processing of personal data related to criminal convictions for journalistic, academic, artistic, or literary purposes is permitted, provided it is proportionate and respects fundamental rights.

Article 14(5)(c)-(d): The transparency obligations under Article 14 do not apply where they would infringe on freedom of expression or journalistic confidentiality.

Article 23 – Restrictions of data subject rights: Restrictions may apply to Articles 12, 18, 19, and 20. A DPIA and prior consultation with the supervisory authority are required. Conditions may be imposed by the supervisory authority, and the data subject must be informed.

Articles 35(10) and 36(5): Where a law or regulation foresees a specific processing activity, a DPIA and prior consultation with the supervisory authority is required, unless the authority is satisfied with the DPIA carried out during the legislative process.

Article 37(4) and 38: The supervisory authority can define cases requiring a DPO and impose confidentiality obligations on DPOs, without affecting investigative powers.

Article 43(1): Accreditation of certification bodies is handled by the Cyprus Organisation for the Promotion of Quality (COPQ), in cooperation with the supervisory authority.

Article 49 – Transfers based on derogations: Transfers of special category data under Article 49 require a **DPIA and prior consultation**. The supervisory authority may impose restrictions for serious public interest.

Articles 54–58 – Supervisory Authority Powers: The Commissioner has additional investigative and enforcement powers, including warrantless access (excluding residences), seizure of data/equipment, and reporting to public authorities. The Commissioner may also participate in joint investigations and negotiate memoranda of understanding.

Article 59 (Annual Report): The Commissioner's annual report must be submitted to the President of the Republic and the President of Parliament, and published on the official website.

Article 83(7): Administrative fines on public authorities or bodies not engaged in profit-making activities are capped at €200,000.

Article 84 – Criminal Sanctions: A range of criminal offences are established for non-compliance with GDPR obligations. Sanctions vary depending on the type and severity of the offence, and may include imprisonment and/or fines, with increased penalties where national security or government operations are threatened.

Articles 85–86: Derogations are provided to protect freedom of expression, journalistic confidentiality, and access to official documents, in line with national laws on public access to information.

Article 89(2)-(3): When processing is for archiving in the public interest, scientific or historical research, or statistical purposes, it may not be used to make decisions that produce legal or similarly significant effects on data subjects.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

Data Protection Impact Assessment (DPIA)

Yes. In Cyprus, Data Protection Impact Assessments (DPIAs) are required under Article 35 of the GDPR and are further by the National Law, which designates specific processing activities as inherently high-risk and prescribes DPIAs as obligatory in those cases.

Under Article 35 GDPR, a DPIA must be carried out prior to any processing that is likely to result in a high risk to the rights and freedoms of natural persons, especially when using new technologies, conducting large-scale profiling or surveillance, or processing sensitive categories of data. If residual high risk remains after mitigation, Article 36 GDPR requires prior consultation with the supervisory authority.

The National Law requires a DPIA in the following cases, alongside prior consultation with the Office of the Commissioner.

- **Article 10**: Combination of large-scale filing systems by public bodies involving special category data, criminal data, or national ID numbers.
- **Article 11**: Implementation of measures restricting data subject rights (Articles 12, 18, 19, and 20 GDPR).
- **Article 12**: Waiver of the obligation to notify a data breach to the data subject under Article 34 GDPR.
- **Article 13**: Prior to adopting laws or regulations providing for specific data processing operations.
- **Article 18**: Transfers of special categories of data to third countries under Article 49 GDPR derogations.

Each of these provisions reflects a **legislative determination that the processing in question presents a high risk**, removing the controller's assessment on whether high risk is posed.

As part of this prior consultation process, the controller must submit the DPIA findings, including:

- The nature, scope, context, and purposes of processing;
- The necessity and proportionality of processing;
- The risks to the rights and freedoms of individuals;
- The technical and organisational measures envisioned to address those risks.

The Cyprus Commissioner has published an indicative (non-exhaustive) list of processing activities that are considered likely to present a high risk and therefore require a DPIA. These include:

- Combination of filing systems involving special category data, criminal records, or universal identifiers (e.g., national ID numbers) in accordance with article 10 of the National Law.
- Restriction of data subject rights under Articles 12, 18, 19, and 20 of the GDPR, as provided in article 11 of the National Law.
- Waiving the obligation to notify a data breach to data subjects under Article 23 GDPR, as provided in article 12 of the National Law.
- Adoption of laws or bylaws that provide for specific processing operations (article 13 of National Law).
- Transfers of special categories of data to third countries or international organisations based on GDPR Article 49 derogations, as provided in article 18 of the National Law.
- Establishment of a credit reference or fraud prevention database.
- Systematic monitoring of employees, including via GPS, internet usage, or workstation surveillance.
- Hospital systems processing genetic or health-related data.
- Systematic CCTV monitoring of public spaces.
- Profiling using public social media data.
- Use of new technologies, such as large-scale data collection via smart devices.
- Applications that store highly personal information (e.g., diaries, life-logging tools, note-taking e-readers).
- Biometric and genetic data processing operations.

This list is indicative and non-exhaustive, and the Commissioner may update it from time to time.

Transfer Impact Assessment (TIA)

Transfers of personal data to other jurisdictions under the GDPR do indeed require a Transfer Impact Assessment, especially in the absence of an adequacy decision by the European Commission. This assessment helps ensure that the level of protection for personal data in the legislation and practices of the third country is essentially equivalent to that within the EU and to identify any supplementary measures that may be needed to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The EDPB's Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data provide further insights.

According to National Law, a transfer carried out by a controller or processor, of special categories of personal data to a third country or an international organisation, which is based on derogations for specific situations provided for in Article 49 of the Regulation, requires carrying out an impact assessment and prior consultation with the Commissioner.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

As of now, there are no official Codes of Conduct under Article 40 of the GDPR approved in Cyprus.

However, the Office of the Commissioner participated in the EU-funded project 'TRAIN-GR-CY', which led to the development of a Standard Code of Practice aimed at facilitating compliance with the data protection legal framework in Cyprus and Greece. While not a formal GDPR Article 40 Code of Conduct, this document provides practical instructions for lawful data handling tailored to the specificities of different activities and sectors. It can be seen as a useful interpretative tool for fostering good practice.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Controllers and processors are required to keep an internal record of processing activities to ensure compliance with Article 30 of the GDPR. The record is made available to the Commissioner upon request. The record shall be kept electronically and in Greek, with English documentation required for cross-border processing activities and other specific cases.

The requirement to keep this record does not apply to a business or organisation employing fewer than 250 people, unless the processing is likely to cause a risk to the rights and freedoms of the data subject, the processing is not occasional or the processing involves special categories of data e.g. health data or biometric data.

If an organisation has fewer than 250 employees, but the processing it performs may pose a risk to the rights and freedoms of the data subject, or it processes personal data on a non-occasional basis, or the processing includes special categories of data, e.g. health data or biometric data or data relating to criminal convictions, then the organisation is obliged to keep the record of processing activities.

Although not all organisations are legally required to maintain an internal record of processing activities, the Office of the Commissioner encourages its use as a good practice to support accountability.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Storage limitation is one of the principles of GDPR. Personal data shall be retained in a format that allows for the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for extended periods if the processing is solely for archiving purposes in the public interest, scientific, historical research purposes or statistical purposes. However, such extended storage shall be subject to the implementation of appropriate technical and organisational measures mandated by GDPR to safeguard the rights and freedoms of the data subject.

Organizations must set and enforce time limits for how long personal data is retained the criteria they use to determine the retention period and should define retention periods based on the **purpose of processing** and if any legal requirements apply.

The data subject shall have the right to obtain from the

controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing, the data subject objects to the processing, the personal data have been unlawfully processed, the personal data have to be erased for compliance with a legal obligation, the personal data have been collected in relation to the offer of information society services.

The controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Under Article 36 of the GDPR, where a data protection impact assessment (DPIA) indicates that a planned processing activity is likely to result in a high risk to the rights and freedoms of individuals and the controller cannot sufficiently mitigate those risks, the controller is required to consult with the Commissioner for the Protection of Personal Data before proceeding.

In Cyprus, prior consultation is required in all such cases. The Commissioner must respond to a consultation request **within eight weeks**, which may be extended by an additional six weeks in complex cases.

Moreover, specific provisions of national law explicitly require both a DPIA and prior consultation in certain circumstances, including:

- **The combination of filing systems** involving special category data or identifiers of general application (e.g., ID numbers) by public authorities (Article 10 of the National Law).
- **Restrictions on data subject rights** (Articles 11 and 12 of the National Law).
- **Transfers of special categories of personal data** to third countries or international organisations based on derogations under Article 49 GDPR (Article 18 of the National Law).
- **Before adopting laws or bylaws** providing for specific processing operations (Article 13 of the National Law).

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

In accordance with the GDPR, controllers and processors shall designate a data protection officer ('DPO') in any case where:

- the processing is carried out by a public authority/body irrespective of what data is being processed, except for courts acting in their judicial capacity;
- the core activities of controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

When the GDPR does not explicitly necessitate the appointment of a DPO, organisations may opt to designate one voluntarily.

The European Data Protection Board ('EDPB') and the Commissioner encourage such voluntary endeavours.

DPOs shall have at least the following tasks:

- Inform and advise controllers, processors and employees who carry out processing of their obligations pursuant to the GDPR and other EU or Cypriot data protection provisions.
- Monitor compliance with GDPR and other EU or Cypriot data protection provisions, as well as the policies of controllers/processors in relation to the protection of personal data. This includes the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and conducting related audits. As part of these duties, the DPO may collect information to identify processing activities, analyse and check the compliance of processing activities, and inform, advise and issue recommendations.
- Provide advice where requested regarding DPIAs and monitor their performance.
- Cooperate with the Commissioner.
- Act as the contact point for the Commissioner on issues relating to processing, including prior

consultation as mandated by the GDPR, and to consult, where appropriate, on any other matter.

DPOs shall be bound by an obligation to comply with secrecy or confidentiality, subject to the provision of any law regulating issues of professional secrecy or confidentiality.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

While the GDPR does not impose a standalone, explicit obligation for employee training, it is implicitly required and strongly recommended as part of an organisation's general compliance duties.

Article 39(1)(b) of the GDPR states that one of the core tasks of the Data Protection Officer (DPO) is to "monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

Under the accountability principle (Article 5(2)), the controller is required not only to comply with the GDPR but also to demonstrate such compliance. Training programs for employees handling personal data are widely accepted as a necessary organisational measure to meet this obligation.

Article 24(1) requires controllers to implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR. This includes ensuring that staff are aware of their data protection responsibilities.

Article 32(1) on the security of processing obliges controllers and processors to implement *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk."* While the provision lists examples like encryption, system availability, and restoration capabilities, it explicitly states that these are non-exhaustive (*"including inter alia, as appropriate"*). In practice, data protection authorities and EDPB guidance recognise staff training as a key organisational measure to reduce the likelihood of breaches due to human error or lack of awareness.

Although National Law does not explicitly mention employee training, the Commissioner has repeatedly highlighted the importance of internal awareness programs.

As such, organisations operating in Cyprus are expected to regularly train employees involved in personal data processing on topics such as data protection principles, data breach reporting procedures, data minimisation, confidentiality obligations, and secure handling of data.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Under Article 13 of GDPR, data controllers are required to provide individuals with specific information at the time their personal data is collected. This information could be provided in the Privacy Notice of the controller. The information provided must include the identity and contact details of the data controller (and, where applicable, the data protection officer), the purposes and legal basis for the processing, any legitimate interests pursued by the controller or a third party, the recipients or categories of recipients of the data, and whether the data will be transferred to a third country or international organization, including details about safeguards in place. Additionally, individuals must be informed about the data retention period or the criteria used to determine it, their rights (such as access, rectification, erasure, restriction, objection, and data portability), the right to withdraw consent at any time, the right to lodge a complaint with a supervisory authority, and whether the provision of personal data is a statutory or contractual requirement and the possible consequences of not providing it. If automated decision-making, including profiling, is involved, information about the logic, significance, and consequences must also be communicated. All information must be provided in a concise, transparent, intelligible, and easily accessible form using clear and plain language.

Under Article 14 of the GDPR, when personal data is not obtained directly from the data subject, data controllers are required to provide specific information to ensure transparency. This includes the identity and contact details of the data controller (and, where applicable, the data protection officer), the purposes and legal basis for processing, the categories of personal data involved, the source of the data and, if applicable, whether it came from publicly accessible sources. Controllers must also inform individuals about the recipients or categories of recipients of the data, any intention to transfer the data to a third country or international organization (including

applicable safeguards), the data retention period or the criteria used to determine it, and the individual's rights under the GDPR—such as the right to access, rectify, erase, or restrict processing of their data, object to processing, and the right to data portability. Additionally, individuals must be informed of their right to withdraw consent, their right to lodge a complaint with a supervisory authority, and whether the provision of data is a legal or contractual requirement. If automated decision-making, including profiling, is involved, meaningful information about the logic involved and the potential consequences must also be provided. This information must be given within a reasonable period, no later than one month after obtaining the data, at the first communication with the data subject, or before disclosure to another recipient.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

Controllers must implement and regularly review appropriate technical and organisational measures to ensure, and demonstrate, GDPR-compliant processing, taking into account the nature, scope, and risks of the processing. These measures should incorporate data protection principles such as data minimisation and may include policies like pseudonymisation.

At the time of determining the means of processing and during processing itself, controllers must build in data protection by design and by default. They are also required to maintain a record of their processing activities (Article 30 GDPR).

In the event of a personal data breach, controllers must notify the supervisory authority within 72 hours, unless the breach is unlikely to pose a risk to individuals' rights and freedoms. Processors must notify controllers without undue delay.

Controllers must inform data subjects of processing activities under Articles 13 and 14 and may rely on approved codes of conduct or certification mechanisms as compliance tools.

When engaging processors, controllers must ensure they provide sufficient guarantees of GDPR compliance and that their processing activities are governed by binding contracts detailing roles, responsibilities, and scope. Processors must not subcontract without prior authorisation and must also maintain records of processing (Article 30(2)).

Both parties are required to cooperate with supervisory authorities upon request.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

The Data Protection Commissioner released Guidance on the use of cookies, aligning with the legislative measures that implement Directive 2009/136/EC. This Guidance states that information can only be stored on, or accessed from, a user's or subscriber's device if they have given informed consent based on clear and detailed information. However, consent is not required when the data access or storage is solely for enabling the transmission of a communication over an electronic communications network, or when it is strictly necessary for the service provider to deliver a specific service that the user or subscriber has explicitly requested.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

The GDPR applies to the extent the online targeted advertising involves the processing of personal data, which is broadly defined as any information relating to an identified or identifiable individual.

The Digital Services Act (DSA) prohibits presenting advertising based on profiling using: (i) personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor; or (ii) special categories of personal data (as defined under the GDPR).

The DSA requires identifying online targeted advertising as such. It also requires providing the following information: (i) the identity of the natural or legal person on whose behalf the advertisement is presented; (ii) the identity of the natural or legal person that paid for the advertising (if different from the person under (i)); and meaningful information about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, information on how to change these parameters.

The Digital Markets Act (DMA) restricts the processing of personal data for providing online advertising. For

example, gatekeepers are not allowed to use for online advertising purposes the personal data of end users that use a gatekeeper's platform to access and use third party services.

The ePrivacy Directive (transposed into national law Electronic Communications Law) requires that any storage of or access to information on a user's device—commonly used for such advertising—can only occur with the user's prior consent, after being provided with clear and comprehensive information about the purposes of the tracking. This means that organizations must implement opt-in mechanisms (such as cookie banners) before engaging in behavioral or targeted advertising. The only exceptions to this rule are when the tracking is strictly necessary to carry out the transmission of a communication or to provide a service explicitly requested by the user.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

Cyprus data protection law does not explicitly define or restrict the "sale" of personal data. However, any disclosure or transfer of personal data, whether for monetary gain or otherwise, must comply with the GDPR principles, be based on a lawful basis, conducted transparently, and respect individuals' rights. Organizations must exercise caution and ensure compliance with all relevant provisions to avoid legal implications.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

According to the Regulation of Electronic Communications and Postal Services Laws of 2004, the use of automated calling and communications systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, for the purposes of direct marketing, may only be permitted with respect to subscribers who have given their prior consent.

Where a natural or legal person obtains contact details for electronic mail directly from customers, in the context of sale of a product/service, such person may use the said details for direct marketing provided that customers are given the opportunity to object clearly and distinctly, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

The practice of sending electronic mail for the purposes of direct marketing disguising or concealing the identity of the sender or the person on whose behalf and/or for whose benefit the communication is made, or without a valid address to which the recipient may send a request that such communications cease, or encouraging recipients to visit websites that violate the Law, shall be prohibited.

Although the law does not define terms such as "telephone calls," "text messaging," or "email communication," it regulates their use within the framework of direct marketing. The term "direct marketing" is also not expressly defined but is understood in line with EU practice as communication aimed at promoting goods or services directly to individuals.

The Commissioner of Electronic Communications and Postal Regulation, upon consultation with the Commissioner, shall take all appropriate measures to ensure that unsolicited calls for the purpose of direct marketing, are not permitted without the consent of interested subscribers or users.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

The National law incorporates the definition of biometric data as set out in Article 4(14) of the GDPR. Biometric data refers to "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data."

Under article 9 of the National Law, the processing of genetic and biometric data for the purposes of health and life insurance is explicitly prohibited.

Moreover, where the processing of such data is based on the data subject's consent, and in addition to the requirement that any further processing must be compatible with the original purpose in accordance with Article 5(1)(b) of the GDPR, the data controller must also obtain separate consent for the further processing

activity.

5 (1) b of the GDPR, a separate consent is needed for further processing.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

At present, Cyprus has not enacted legislation specifically regulating artificial intelligence or machine learning (AI/ML). However, AI systems that process personal data are subject to the General Data Protection Regulation (GDPR) and the National Law.

The relevance of data protection law arises when AI systems process personal data or a combination of personal and non-personal data. In such cases, the core GDPR principles shall apply and data subject rights shall be safeguarded.

Among the most significant provisions:

- Article 22 GDPR provides individuals with the right not to be subject to solely automated decisions, including profiling, that produce legal or similarly significant effects.
- Article 25 GDPR (Data Protection by Design and by Default) plays a central role in ensuring that data protection principles are embedded at the design stage of AI systems, and throughout their lifecycle. This includes implementing technical and organisational measures to support principles such as data minimisation, purpose limitation, and access control.
- Article 5(1)(f) GDPR (integrity and confidentiality) reinforces the importance of information security, which is essential for the safe and lawful deployment of AI systems. This aligns closely with cybersecurity objectives, particularly the need to uphold confidentiality, integrity, and availability.
- The need for Data Protection Impact Assessments (Article 35 GDPR) becomes particularly relevant where AI systems pose a high risk to the rights and freedoms of individuals.

In practice, data protection by design must be translated into concrete technical goals for developers of AI systems. These may include embedding privacy into model training, algorithmic transparency, risk mitigation, and lifecycle data governance. AI systems must not only respect data protection rules in theory but operationalise them through auditable, measurable safeguards.

While Cyprus has not adopted a standalone AI legal framework, it is expected that national practice will align with the AI Act.

In Cyprus, the enforcement of the EU Artificial Intelligence Act is assigned to three national authorities:

a. Communications Commissioner – designated as the Notifying and Market Surveillance Authority, serving as the Single Point of Contact for AI-related matters.
b. Commissioner for Personal Data Protection – responsible for overseeing AI applications within her remit, particularly those involving personal data processing.
c. Commissioner for Administration and the Protection of Human Rights (Ombudsman) – tasked with ensuring that AI systems uphold fundamental rights.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Any transfer of personal data that is undergoing processing or intended for processing after transfer to a third country or an international organisation shall take place only if the conditions laid down in the GDPR are complied with by controllers and processors, including for onward transfers of personal data from the third country or international organisation to another third country or international organisation.

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Where the transfer to a third country or international organisation cannot be based on an adequacy decision or the provision of appropriate safeguards and any of the derogations of Article 49 do not apply, this can only be

done if the transfer is not repeated, concerns only a limited number of data subjects and is necessary for the purposes of overriding legitimate interests pursued by the controller; which, however, cannot override the interests and freedoms of the data subject and provided that he or she has provided appropriate safeguards for the personal data to be transferred. In such a case, the controller shall inform the Commissioner of the transfer.

Additionally, the provisions of article 18 of the National Law should be taken into account, based on which, when it comes to the transmission of special categories and/or sensitive personal data on the basis of the aforementioned derogations, an impact assessment should be carried out and there should be prior consultation with the Commissioner.

Data exporters relying on the transfer tools of Article 46.2 and 46.3 GDPR for their transfers, have an obligation to assess the level of protection in third countries of destination and the need for additional safeguards. This assessment is the Transfer Impact Assessment (TIA) and shall be conducted to ensure that the transfer of personal data guarantees an adequate level of protection.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Both data controllers and data processors have responsibilities for ensuring data security. Data controllers are primarily tasked with implementing appropriate technical and organisational measures to safeguard personal data against various risks, including unauthorised or unlawful processing, as well as accidental loss, destruction or damage. Similarly, data processors also bear obligations under the GDPR to implement adequate security measures and ensure the security of the data they handle. To address these responsibilities effectively, both controllers and processors must implement suitable technical and organisational measures. This entails considering factors such as measures adhering to privacy as the default principle, and the nature of processing, all while assessing the risks to the rights and freedoms of individuals.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Controllers are obligated to report a personal data breach to the Commissioner without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

The report to the Commissioner must include details such as the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the name and contact details of the DPO or other contact point to further information, the likely consequences of the personal data breach, and the measures taken or proposed to be taken to address the breach, including any measures to mitigate its possible adverse effects.

Controllers are required to document all personal data breaches, including relevant facts, effects and remedial actions taken, demonstrating the organisation's commitment to data protection and transparency. This documentation should enable the Commissioner to verify compliance.

If a personal data breach is likely to pose a high risk to the rights and freedoms of individuals, the controller must notify the affected data subjects without undue delay. This notification should outline the nature of the breach, provide contact details for obtaining further information and offer recommendations for mitigating potential harm. These communications to data subjects should be conducted as soon as reasonably possible and in close coordination with the Commissioner, following established guidance. The communication to the data subject should use clear and straightforward language.

In addition to the exemption conditions in Article 34 (3) of the GDPR and in accordance with the National Law, a controller may be exempt from the obligation to inform data subjects about a personal data breach, either entirely or partially, for one or more of the purposes outlined in Article 23(1) of the GDPR. However, this exemption from notifying the data subject requires conducting an impact assessment and consulting with the Commissioner beforehand.

According to Article 33(2) of the GDPR, a data processor shall notify the data controller without undue delay after becoming aware of a personal data breach and shall provide the controller with all relevant information needed to support their own notification obligations.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

- Right to transparent communication and information: Data subjects have the right to receive specific information about their relationship with the controller, including the controller's identity and contact details, the purposes and legal basis for processing their data, and any recipients, particularly in third countries. The controller must also disclose the data source if obtained from a third party to enable the data subject to exercise their rights effectively.
- Right of access: The data subjects have the right to request a copy of the personal data being processed and obtain from the controller confirmation and, if so, access the following information:
  - the purposes of processing;
  - the categories of personal data;
  - the recipients or categories of recipients, especially in third countries or international organisations and transfer safeguards for data sent to them;
  - the storage period or criteria to determine it;
  - the existence of rights to request rectification, erasure, restriction, to object to processing or to lodge a complaint with the Commissioner;
  - the source of data if not collected from the data subject;
  - the existence of automated decision-making, including profiling, and its logic, significance and consequences; and
  - the appropriate safeguards, if personal data are transferred in third countries.
- Right to rectification: Data subjects have the right to obtain from the controller without delay the rectification of inaccurate personal data concerning them and have the right to have incomplete personal data completed.
- Right to erasure ('to be forgotten'): Data subjects have the right to request the erasure of their personal data without delay if:
  - the data is no longer necessary for its original purposes;
  - consent is withdrawn and no other legal basis for processing exists;
  - the data subject objects to processing and no overriding legitimate grounds exist, or objects to processing for direct marketing;
  - the data has been unlawfully processed;
  - erasure is required to comply with a legal obligation; or
  - the data was collected in relation to offering information society services. This right does not apply if processing is necessary for:
  - exercising freedom of expression and information;
  - complying with a legal obligation or performing a task in the public interest or official authority;
  - reasons of public interest in public health;
  - archiving in the public interest, scientific or historical research, or statistical purposes if erasure impairs these objectives; or
  - establishing, exercising or defending legal claims.
- Right to restriction: Data subjects have the right to request the restriction of processing if:
  - the accuracy of the personal data is contested, allowing time for verification;
  - the processing is unlawful, and the data subject opposes erasure and requests restriction instead;
  - the controller no longer needs the data, but it is required for legal claims by the data subject; or
  - the data subject has objected to processing, pending verification of overriding legitimate grounds.
- Right to data portability: Data subjects have the right to receive their personal data, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - the processing is based on consent or on a contract; or
  - the processing is carried out by automated means.
- Right to objection: Data subjects have the right to object at any time to the processing of their personal data based on public interest or the legitimate interest of the controller, including profiling. The controller must stop processing the data unless there are compelling legitimate grounds that override the data subject's interests, rights and freedoms, or for the establishment, exercise or defence of legal claims. For direct marketing purposes, data subjects can object at any time to the processing of their data, including related profiling. Upon objection, the personal data must no longer be processed for such purposes.
- Right to not be subject to automated decision-

making: Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting them.
- Right to withdraw consent: Data subjects have the right to withdraw consent at any time. This shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, data subjects shall be informed thereof. It shall be as easy to withdraw as to give consent.
- Right to lodge a complaint: Data subjects residing in Cyprus or whose rights are allegedly infringed concerning the processing of their personal data within Cyprus have the right to lodge a complaint with the Commissioner. The Commissioner shall inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy.
- Right to an effective judicial remedy: Data subjects have the right to effective judicial remedy in the following cases:
  - If the Commissioner does not handle a complaint or fails to inform the data subject within three months about the progress or outcome of the complaint.
  - Against a legally binding decision of the Commissioner concerning them.
  - When data subjects believe their rights under the Law have been infringed due to the non-compliant processing of their personal data.
- Right to compensation and liability: Any data subject who has suffered material or non-material damage as a result of an infringement of GDPR, shall have the right to receive compensation from the controller or processor for the damage suffered.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Under Article 79 of GDPR, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with GDPR. Such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.

Any natural or legal person shall have the private right of action before the Cyprus Courts when their rights have been infringed under the GDPR and the National Law.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

The law does not require that actual and material damage to be sustained in order to claim compensation. Non-material harm alone is sufficient, provided the individual can demonstrate a causal link between the GDPR violation and the damage suffered.

30. How are data protection laws in your jurisdiction typically enforced?

Please refer to Question 1.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Under the GDPR, infringements of provisions regarding the basic principles of processing, including conditions for consent, are subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Non-compliance with an order by the supervisory authority shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Infringements of the provision regarding the obligations of the controller and processor, of the certification body, and of the monitoring body, shall be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Additionally, an offence is committed by a controller or processor who does not comply with the provisions of the

GDPR and the National Law when carrying out a processing activity and shall be subject to imprisonment for up to one year or a fine of up to €10,000, or both penalties.

Penalties can also be imposed in accordance with the National Law. The Commissioner may impose the following administrative sanctions for violations of the provisions of the National Law.

- A warning, with instructions and/or recommendations to correct the violation or prevent a potential violation.
- A reprimand.
- An order to cease the violation, if necessary, within a specified timeframe.
- A temporary or permanent ban on processing.
- An administrative fine of up to €200,000.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

The European Data Protection Board (EDPB) has published the Guidelines 04/2022 on the calculation of administrative fines under the GDPR, which outlines a five-step methodology for calculating fines, considering factors such as identifying the processing operations in the case and evaluating the application of Article 83(3)GDPR, finding the starting point for further calculation based on an evaluation of a) the classification b) the seriousness of the infringement c) the turnover of the undertaking, evaluating aggravating and mitigating circumstances, identifying the relevant legal maximums for the different processing operations and analysing whether the final amount of the calculated fine meets the requirements of effectiveness, dissuasiveness and proportionality.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

According to Article 28 of the National Law any natural or legal person shall have the right to appeal against a decision of the Commissioner before the Administrative Court.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

The Office of the Commissioner conducts regular audits across various organisations and companies within the private and public sector to identify gaps in compliance with the applicable data protection laws and drafts reports specifying the deficiencies. Furthermore, it organizes training seminars for individuals and data protection officers.

It is noted that the Office of the Commissioner will acquire additional powers under the AI Act in cases where the use of Artificial Intelligence (AI) poses high risks to these rights. These powers will apply from 2 August 2026.

The Commissioner is also engaged in preparatory work for her recent appointment as one of the national competent authorities responsible for implementing the Digital Services Act ('DSA'). The DSA aims to enhance consumer protection, ensure transparency of online platforms and impose stricter measures against illegal content.

The Commissioner is very active at the European level, holding the position of Vice President of the EDPB. In this capacity, she often represents the EDPB President at European and International fora. In certain cases she represented both Cyprus and the EDPB in her role as Vice-Chair of the Board.

At national level, the Commissioner is actively addressing matters related to surveillance systems monitoring (CCTVs). An announcement was recently issued concerning the installation of CCTV systems by Municipalities.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

According to the NIS2 Voted Law, the DSA may, by virtue of its powers and in particular upon request from an interested body/provider or organization, take provisional measures, including the issuance of a provisional Decision, in cases where there is a potential risk to the security of networks and information systems.

The DSA shall adopt a national cybersecurity strategy which provides for the strategic objectives, the resources needed to achieve those objectives, appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. Within the forthcoming weeks, the release of the updated

Cybersecurity Strategy of the Republic of Cyprus, aligned with NIS2 Directive is expected.

The NIS2 Voted Law imposes on essential and important entities specific measures to manage risks. These entities shall receive appropriate and proportionate technical, operational and organisational measures to manage network system security risks, and information they use for their activities or for the provision of their services, and to prevent or minimize the impact of incidents on the recipients of the services or other services.

According to Article 21 of NIS2 Directive, Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

Both the NIS2 Directive and the Cyber Resilience Act (CRA) place significant emphasis on securing the digital supply chain as a regulatory priority.

Under the NIS2 Directive, entities in critical and important sectors are required to manage cybersecurity risks not only within their own operations but also across their supply chains. This reflects the growing recognition that third-party vulnerabilities can undermine the resilience of essential services. The directive promotes a proactive approach, encouraging organisations to assess risks linked to their suppliers and adopt safeguards accordingly.

Similarly, the Cyber Resilience Act addresses supply chain cybersecurity by requiring that products with digital elements are designed and developed with security in mind throughout their lifecycle and supply chains, making final products with digital elements and their components more secure.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

Article 29 of NIS 2 Directive provides that Member States shall ensure that entities falling within the scope of the Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks.

Under the NIS2 Voted Law, the DSA may enter into cooperation with the National Response Teams Computer Security Incidents (CSIRTs), third country. In the context of the cooperation, the Authority shall facilitate the effective, efficient and secure exchange of information with these National Computer Security Incident Response Teams (CSIRTs), using relevant information exchange protocols, including the Traffic Light Protocol (TLP).

Article 19 of the NIS2 Voted Law, provides that in order to ensure the best exercise of its powers and powers, the DSA, complying with the principle of proportionality, with a reasoned request, has the power to require from important and/or essential entities, and mobile communications providers, and if the DSA deems it appropriate at the request of the Police, to provide the DSA and/or the Police with the necessary information for public policy and national security purposes and to request from the important and/or essential entities to provide the information required for the assessment the security of network and information systems.

Information that is confidential in accordance with EU or national rules, such as business rules confidentiality, are exchanged with the Commission and other competent authorities in accordance with the NIS2 Voted Law and only if such exchange is necessary for the application of the Law, relevant and proportionate to its purpose exchange.

The essential and important entities that fall within the scope of the NIS2 Voted Law and, where applicable, other entities that do not fall within the scope of the Law may exchange cybersecurity-related information with each other on a voluntary basis, including information related to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, hostile tactics, threat actor specific information, cybersecurity warnings and recommendations on tool customization to detect cyberattacks.

38. Do the cybersecurity laws in your jurisdiction

require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

DSA has published the Decision 389/2020 under "The Network And Information Systems Security Law Of 2020 (repealed)" which defines the framework of minimum security measures for network and information systems.

The context of the technical and organisational measures are described in Annex III of the Decision.

Under this Decision, the entities are required to appoint a Network and System Security Officer information, who serves as a regulatory point of contact and has the following responsibilities:

- To inform and advise the institution and the employees who have access to their network and information systems on their obligations, in accordance with decision's framework,
- To monitor compliance with the framework, with other national or European information security provisions, and the Agency's policies in relation to the security of network and information systems,
- To provide advice on information security management and monitor its performance in accordance with Part III for risk management,
- To cooperate and act as a point of contact with the DSA on matters relating to the activities of the DSA within the framework of its competences,
- To prepare reports on information security threats, vulnerabilities and risks to top-level management through formal and regular reports.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

For a detailed breakdown of regulations applied on specific industries, please refer to the responses under Question 1 and Question 2.

40. What impact do international cybersecurity standards have on local laws and regulations?

International cybersecurity standards have a direct and growing impact on local laws and regulatory frameworks in Cyprus, especially through their integration into EU legislation.

CYS, the Cyprus Standardization body, plays an active role in shaping European cybersecurity and emerging technology standards by participating in the technical committees of the European Standardization Organizations, CEN, CENELEC, and ETSI.

CYS Experts, including Maria Raphael, author of this guide, contribute to key committees such as CEN-CENELEC JTC 13 (Cybersecurity and Data Protection), CEN/CLC/JTC 21 (Artificial Intelligence) and ETSI TC Cyber which develop harmonized standards in support of Union Harmonisation legislation.

This involvement is particularly significant given the increasing reliance of EU legislation, including the Cyber Resilience Act (CRA) and the Artificial Intelligence Act (AI Act), on harmonised standards to provide presumption of conformity and facilitate conformity assessment processes for regulated products entering the EU market. Through its expert engagement, Cyprus contributes to the development of standards that reflect national needs and strategic interests.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

According to NIS 2 Directive 'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

The definition given by the NIS 2 Directive for a 'large-scale cybersecurity incident' is an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.

Article 23 of NIS 2 provides that each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those

services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

42. How are cybersecurity laws in your jurisdiction typically enforced?

In addition to the response provided in Question 1 above, the cybersecurity laws are enforced through the Secondary Legislation 251/2021 of DSA which was issued during the period of NIS1 applicability and which determines the procedure for the imposition of an administrative fine.

This Decision is expected to be updated to align with the provisions and requirements of NIS2 Directive.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under the NIS 2 Voted Law the DSA has the power to supervise compliance with the obligations imposed by the provisions of this Law and/or the provisions of the Decisions issued pursuant to the provisions of this Law, in the important and/or essential entities.

The DSA may, on its own initiative, conduct an investigation into the activities and functions of any important and/or essential entity, which are deemed not to be in compliance with the provisions and with the implementation of this Law and consequently to make recommendations and issue Decisions, as in its opinion, are appropriate.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

The NIS2 Directive and the Voted Law amending the NIS law set minimum thresholds for administrative fines based on the classification of the entity:

Essential entities (e.g., energy, transport, health, digital infrastructure): Fines up to €10 million or 2% of global annual turnover, whichever is higher.

Important entities (e.g., food, manufacturing, digital services): Fines up to €7 million or 1.4% of global annual turnover, whichever is higher.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

DSA published the Decision 251/2021 (issued when NIS 1 was in force) which constitutes Secondary Legislation and is referred as the Information Gathering and Enforcement Administrative Fine Decision of 2021. This Decision determines the procedure for the imposition of an Administrative Fine against a person who carries out an act or is in omission in violation of the provisions of the Law.

This Decision is expected to be updated to align with the provisions and requirements of NIS2 Directive.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

According to Article 52 of NIS2 Voted Law any decision of the DSA is subject to judicial review by appeal to the Administrative Court in accordance with Article 146 of the Constitution and the Law on the Establishment and Operation of the Administrative Court.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

The implementation of the NIS2 Directive is a central regulatory priority in Cyprus, reflecting the country's commitment to strengthening its national cybersecurity framework in alignment with evolving EU legislation. The NIS2 Directive replaces the original NIS Directive and significantly enhances cybersecurity requirements across the EU. On 10 April 2025, the National NIS2 Voted Law (hereinafter ''the NIS2 Voted Law'') was approved by the Plenary of the House of Representatives. Its official publication in the Official Gazette is expected within the coming weeks.

The DSA is also in the process of amending the Secondary Legislation which had been issued under the NIS Directive to have it aligned with the NIS2 Directive.

The DSA continues to serve as the national competent authority and single point of contact under NIS2, responsible for adopting and implementing the national cybersecurity strategy, which will be subject to approval

by the Council of Ministers. The DSA is also responsible for identifying entities falling within the scope of the Directive, classified as "essential" or "important'', based on specific risk-based and sectoral criteria.

To support structured implementation, the DSA has operationalised the Cybersecurity Maturity Assessment Framework (CMAAF). This framework evaluates the cybersecurity posture of Operators of Essential Services (OES) and Critical Information Infrastructures (CIIs), assigning maturity levels from 0 (non-existent) to 5 (optimised). Achieving Level 3 indicates that an organisation complies with core legal obligations under NIS2. The framework is also used for sectoral and national capability assessments and is supported by a professional certification scheme for cybersecurity maturity assessors, managed in cooperation with the Cyprus Certification Company.

Additional support measures include:

Publication of an NIS2 Summary Guide

The DSA has issued a concise guide outlining the core elements of the NIS2 Directive, including:

- The sectors falling within the scope of NIS2;
- The incident notification process;
- Cybersecurity risk management measures;
- The supervision regime for essential and important entities;
- Applicable sanctions; and
- Management responsibilities.

Launch of an NIS2 Self-Assessment Tool

The DSA developed an online self-assessment tool designed to help organisations determine whether they fall within the scope of NIS2. The tool provides:

- An initial indication of whether a public or private sector organisation may qualify as an essential or important entity;
- Basic guidance on categorisation criteria; and
- Optional access to further information and supporting materials about NIS2 compliance.

Capacity Building

A key priority in Cyprus is the continuous strengthening of national cybersecurity capabilities, in line with EU strategic objectives. A notable development in this context is the launch of the N4CY2 program, a co-funded European initiative aimed at the further development of the National Cybersecurity Coordination Centre (NCC-CY) under the DSA. The program, which is the second phase of the European funded N4CY program, started on 1 January 2025 and supports enhanced national coordination, cybersecurity research and innovation, and closer alignment with the objectives of the European Cybersecurity Competence Network. These efforts reflect a broader national focus on reinforcing resilience, preparedness, and participation in cross-border cybersecurity mechanisms.

In addition, the DSA completed the country's first National Cybersecurity Risk Assessment (NCRA) to help identify, assess, and understand national-level cyber risks, as part of its strategic role in improving cyber resilience in Cyprus.

Contributors

Maria Raphael
Managing Director
maria@raphael.legal

Anastasia Georgiou
Lawyer
anastasia@raphael.legal