Legal 500
Country Comparative Guides 2024

Cyprus
Data Protection & Cybersecurity

Contributor

Nicholas Ktenas & Co
LLC

Nicholas Ktenas

Managing Partner | nicholas.ktenas@cylegal.com

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 by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The legal framework on Privacy and data protection in Cyprus mainly consists of the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR") and, by way of implementation of derogations allowed by the GDPR, the "Law Providing for The Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data" (Law 125(I)/2018) (the "Data Protection Law").

Furthermore, Law 44(I)/2019 also implements Directive (EU) 2016/680 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.

The Office of the Commissioner for Personal Data Protection ("the Data Protection Commissioner") is an independent public authority responsible for monitoring the implementation of the GDPR and other privacy laws. The Personal Data Commissioner issues guidelines and opinions from time to time for the proper application of the GDPR and these laws.

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).

The main law on Cybersecurity is the Security of Networks and Information Systems Law of 2020 (Law 89(I)/2020) (the "NIS Law"), which implements the NIS Directive, Directive (EU) 2016/1148. The Digital Security Authority (DSA) is the authority responsible for the application of this Law. Under this law, the DSA is responsible for establishing a national strategy for network and information system security and cyber security, which shall set out the strategic objectives and appropriate policy and regulatory measures, with the aim of achieving and maintaining a high level of network and information system security. Companies and organizations identified as either operators of essential services or Competent Authorities are primarily regulated under this law.

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"). The Police (Cybercrime Subdivision) is mainly responsible for enforcing these laws.

It is also worth mentioning the Protection from Harassment and Annoying Surveillance Law of 2021 114(I)/2021, which criminalises, inter alia, the monitoring of the use of e-mail and/or any other electronic communication of another person, the posting on social media concerning a person's private life and the interfering with a person's postings on the Internet.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

The expected implementation of the NIS2 Directive in October 2024 and the application of the Digital Operational Resilience Act in January 2025 are the most important changes in the data protection laws in 2024-2025. These are considered in more detail along with other expected changes in Question 48 below.

3. Are there any registration or licensing requirements for entities covered by these data

protection laws, and if so what are the requirements? Are there any exemptions?

There are no registration or licensing requirements relevant to the processing of personal data, however certain notification and consultation requirements may apply. These are discussed below.

As regards Cybersecurity, all natural and corporate persons who are digital services providers residing or having their corporate seat in the Republic of Cyprus have an obligation to register with the DSA for the purpose of monitoring the regular approach for the security of information.

4. How do these data protection laws define “personal data,” “personal information,” “personally identifiable information" or any equivalent term in such legislation (collectively, “personal data”) versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

The definition of 'personal data' and all other key definitions under Article 4 of the GDPR are adopted.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or “fair information practice principles" in detail.

The principles related to the general processing of personal data in Article 5 of the GDPR apply.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Consent is required where no other lawful basis for the processing applies, in accordance with Article 6 of the GDPR.

Where the processing of genetic and biometric data is based on a data subject's consent, the further processing of such data requires the separate consent of the data subject.

7. 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)?

Except in the case of direct marketing (see Question 29 below), where special considerations apply under Cyprus law, the rules relating to consent under Article 7 of the GDPR apply.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

Sensitive information is classified as 'special category data' under the GDPR and certain requirements apply to the processing of such data.

The processing of personal data or special categories of personal data or personal data relating to criminal convictions and offenses, which is carried out for journalistic or academic purposes or for purposes of artistic or literary expression, is permitted, provided that those purposes are proportionate to the aim pursued and respect the essence of the rights as set out in the in the Charter of Fundamental Rights of the EU and in the European Convention of Human Rights and Fundamental Freedoms, as these have been ratified by Cyprus law and the Constitution.

The transfer to a third country of special category personal data requires prior notification to the Commissioner. Where such transfer is based of the derogations provided for in Article 49 of the GDPR for specific situations, it requires a DPIA and prior consultation with the Commissioner.

When the transfer is based on appropriate safeguards provided for in Article 46 of the GDPR or on binding corporate rules provided for in Article 47 of the GDPR, the controller or processor must inform the Commissioner of the intended transfer before the data is transferred and the Commissioner may, for important reasons of public interest, impose explicit limits to the controller or the processor.

The processing of special categories of data is permitted and is lawful when it is carried out for the purpose of publishing or issuing a decision of any court or when it is necessary for the purpose of delivering justice.

The combination of filing systems which concern special categories of personal data or data concerning criminal convictions or to be used with an identification card number or any other general application identity information require a DPIA and prior consultation with the Commissioner.

The processing of genetic and biometric data for purposes of health and life insurance is prohibited.

9. How do the data protection laws in your jurisdiction address health data?

Health data are considered special category data under Article 9 of the GDPR and Cyprus law.

The Data Protection Commissioner has issued a list of activities which require an impact assessment, including the processing by hospitals of patients' genetic and health data (hospital information system).

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

The processing which is carried out by a controller or a processor for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be used for taking a decision which produces legal effects concerning the data subject or similarly significantly affects him or her.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

When providing information society services directly to a child based on the child's consent, the processing of personal data is lawful if the child is at least 14 years old.

For a child under the age of 14, the processing of personal data is lawful following consent provided or approved by the person having parental responsibility for the child.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

Online safety concerns in Cyprus are mainly addressed by the NIS Law and the Cybercrime Laws.

Regulations issued under the NIS Law address certain online safety issues such the obligation of operators of essential services, operators of critical information infrastructures, and digital service providers to notify incidents, which have a significant impact on the continuation of their services, the obligation of Electronic Communication Network Providers to notify the DSA about Personal Data breaches, minimum additional obligations relating to the security of networks and information systems which providers operating electronic communications networks and/or services must comply with, etc.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

The Data Protection Commissioner is the regulator responsible for personal data in Cyprus, including children's and teenager's personal data. Its enforcement powers for children's personal data are the same as for the personal data of adults. In addition, the Commissioner for Children's Rights, established under the Commissioner for Children's Rights Law (Law 74(I)/2007, as amended) has the mission to protect and promote all children's legal rights in general under Cyprus law and international conventions. The Commissioner for Children's Rights has a wide range of statutory powers, including to inform and make children aware of their rights, check that the policies and practices of governmental and non-governmental bodies are compatible with the rights of the child and make recommendations for their improvement, represent children in judicial and administrative proceedings, etc.

This Commissioner for Children's Rights has the power to report to the relevant authorities (including the Data Protection Commissioner), on its own initiative any complaints for violations of children's rights for investigation, to assess the result of such investigations and generally to cooperate with respective bodies and authorities of other EU member states and the Council of Europe, on all matters relevant to its authority.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

In February 2024, in response to a recent wave of cyber-attacks in Cyprus against critical government infrastructures, including the Land Registry Department, the DSA announced the creation of a comprehensive toolkit of policy/procedure standards, seeking to strengthen the critical infrastructures of the Republic of Cyprus in relation to cyber security by offering guidance for compliance with the requirements and obligations of Decision Regulation 389/ 2020 on Security of Networks and Information Systems.

The toolkit can be downloaded from the official website of the DSA and is offered as a general guide for use by either critical government departments or any other organization that would like to use it to build a structured approach to effectively defend against cyber threats. The toolkit has been designed in such a way that each user, through the instructions, can complete and adapt it for their needs in simple and comprehensive steps.

In addition to the legislative changes discussed in Question 48 below, together with the enforcement actions of the DSA and the Data Protection Commissioner the Toolkit is expected to contribute to the enhancement of the online safety landscape in Cyprus in 2024-2025.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

In addition to the requirements of data protection by design under Article 25 of the GDPR, Cyprus law requires the controller and the processor to provide a description of the technical and organizational security measures provided for in Articles 24, 25, 28 and 32 of the Regulation when carrying out an impact assessment and prior consultation with the Data Protection Commissioner for transfers of special data to third countries.

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

The requirement of the GDPR for internal records and processes apply.

A sample Record of Processing Activities (required under Article 30 of the GDPR) and guidance for its completion have been published by the Data Protection Commissioner on its website. Controllers and processors who fail to maintain this record, keep it up to date or make it available to the Commissioner upon request or who provide false, inaccurate, incomplete or misleading information to the Commissioner in relation thereto commit an offence punishable with a fine of up to €30,000 euro and/ or 3 years imprisonment.

17. 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).

The general principles of the GDPR, including the principle of storage limitation, apply.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

Certain activities require consultation with the Personal Data Commissioner. These are discussed in detail in Questions 8 above and 19 below.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Under Cyprus law, the following activities require a risk assessment (DPIA) and prior consultation with the Data Protection Commissioner:

- Implementation of measures to limit, in whole or in part, the rights referred to in Articles 12, 18, 19, and 20 of the GDPR;
- exemption from the obligation to communicate a personal data breach to the data subject, wholly or partly, for one or more of the purposes referred to in Article 23, paragraph 1

of the Regulation;
- transfers of special categories of personal data to third countries or international organizations based on derogations in Article 49 of the GDPR;
- the combination of filing systems relating to special categories of personal data or data concerning criminal convictions or to be used with an identification card number or any other general application identity information; and
- the enactment of laws or regulations which provide for a particular act or series of personal data processing acts.

Furthermore, the Data Protection Commissioner issued a list of activities which require an impact assessment, the Cyprus DPIA Blacklist, which, in addition to the above, includes the following activities:

- the establishment of a credit reference database or a national level credit rating or fraud database;
- systematic monitoring of employees' activities, including the monitoring of the employees' work station, internet activity, and the use of GPS on employees' vehicles;
- the processing of patients' genetic and health data by hospitals;
- systematic and large-scale monitoring of public places by means of cameras;
- gathering of public social media data for generating profiles (profiling);
- the use of new technologies, including the processing of large amount of data obtained via smart devices;
- applications which offer to the users the possibility to store documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications; and
- any processing activities involving biometric and genetic data.

DPIAs should be carried out in accordance with the requirements of Article 35 of the GDPR.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The appointment of data protection officers and their legal responsibilities are governed by the provisions of Articles 37-39 of the GDPR.

21. 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).

Under the GDPR an organization is required to ensure that its employees receive regular and appropriate training about its privacy policies and procedures and their responsibilities.

22. 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).

The requirements of Articles 13-14 of the GDPR apply.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The distinction is drawn by the GDPR. Obligations on processors are placed by the GDPR as well as through flow-down contractual requirements.

Processors and controllers share certain common obligations and restrictions under Cyprus law, such as the obligation to notify the Data Protection Commissioner and/ or carry out a DPIA in relation to the transfer of special category data to a third country, discussed above.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Processors have an obligation under the Data Protection Law to:

- Carry out a DPIA and prior consultation with the Data Protection Commissioner where this is required under Cyprus law (discussed in Question 19 above).

- Maintain and update the record of processing activities.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

This is regulated by Article 28 of the GDPR.

26. 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 terms defined, and what restrictions on their use are imposed, if any?

The systematic monitoring of employees' activities and the systematic and large-scale monitoring of public places by means of cameras require a DPIA.

Cyprus also ratified the 'European Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data of 1981' and its Amending Protocols.

The Data Protection Commissioner issued Guidance on the use of cookies, which refers to the relevant legislative provisions implementing Directive 2009/136/EC. According to this Guidance, storing information or gaining access to already stored information on the subscriber's or user's terminal equipment is permitted only if the respective subscriber or user has given his consent based on clear and comprehensive information unless the sole purpose is to carry out the transmission of a communication via an electronic communications network, or when it is absolutely necessary for the information society service provider to provide the specific service that the subscriber or user has expressly requested.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Targeted and cross-contextual behavioral advertising is governed by the GDPR and the relevant guidelines issued at EU level.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

The general requirements of the GDPR apply in relation to the sale of personal data.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The protection from unsolicited marketing communications with the use of electronic media, including automated call systems, electronic mail (email), messages on mobile phones (sms) and fax machines, extends to legal persons (companies) by means of an Order issued by the Electronic Communications Commissioner. The Data Protection Commissioner also clarified that if the messages contain a company name or product or service then they are considered advertising.

Under the GDPR the use of electronic mail for the purposes of direct marketing is permissible only in the case of addressees who have given their prior consent. However, according to the Data Protection Commissioner's guidance on direct marketing, under the Electronic Communications Law, where a sender has been provided by a customer with an email address in the course of a sale of goods or services, individuals or legal entities that obtain their customers' personal data (e.g. e-mail addresses) may use it for direct promotion of their own similar products or services so long as customers are aware of this practice and are given the opportunity to decline receipt of future communications.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

The processing of genetic and biometric data, as defined in Article 4 of the GDPR, for purposes of health and life insurance is prohibited.

Where the processing of genetic and biometric data is based on a data subject's consent, the further processing of such data requires the separate consent of the data subject.

According to the Data Protection Commissioner's Opinion on the use of biometric systems (facial recognition or fingerprinting) by employers, the use of such data for the purpose of checking the time of attendance and departure of employees to their workplace is prohibited. The employer must choose other means less intrusive/burdensome for the human dignity than the collection and use of fingerprints or facial recognition.

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

There are currently no data protection laws in Cyprus addressing artificial intelligence or machine learning ("AI").

32. 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?)

Transfers of personal data outside of Cyprus to a recipient in a third country or to an international organization are governed by the provisions of Chapter 5 of the GDPR.

Under Cyprus law when the controller or the processor intends to transfer special categories of personal data to a recipient in a third country or to an international organization under certain circumstances the controller or processor must carry out a DPIA and/ or notify the Data Protection Commissioner (see Question 8 above).

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

Personal data controllers and processors in Cyprus have an obligation to implement appropriate technical and organizational measures to ensure an appropriate level of security, as required under Article 32 of the GDPR.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

The Data Protection Law has adopted the definition of 'personal data breach' under the GDPR.

The NIS Law has adopted the definition of 'incident' under Directive 2016/1148/EU;

Data breaches must be handled in accordance with the GDPR. Under Cyprus law, however, an impact assessment and prior consultation with the Data Protection Commissioner should be carried out where a controller may be exempt from the obligation to communicate a personal data breach to the data subject, wholly or partly, for one or more of the purposes referred to in Article 23, paragraph 1 of the Regulation, as explained in Question 16 above.

Cybersecurity incidents are addressed by the DSA's Decision of 2022 (39/2022), which implements Commission Implementing Regulation (EU) 2018/151 and is applicable to all operators of basic services, critical information infrastructure operators, electronic communications providers and digital service providers. This Decision specifies the conditions under which a security incident is considered as having a serious and/or significant impact on the provision of services to oblige these entities and their providers to submit a notification to the DSA. Furthermore, it regulates the notification submission process, and in particular the content of the notifications, the manner of submission and the deadlines that must be observed.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

The GDPR and the Data Protection Law apply to all sectors, industries, and technologies.

The relevant provisions of the Telecoms Law apply to telecommunication services providers.

The NIS Law applies to companies and organizations identified as operators of essential services.

The Cybercrime Laws apply to all sectors.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable

regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

Breaches of personal data must be reported to the Data Protection Commissioner and/ or the data subjects in accordance with the GDPR and the Data Protection Law.

Each provider of electronic communications has a duty to notify without undue delay to the DSA any security-related incident that has a significant impact on the operation of electronic communications networks or services, taking into account the number of users affected, the duration of the incident, the geographical extent, the impact on health and safety, national security, the economy, social and political well-being and the environment.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

The authorities and the Cyprus police (Cybercrime Subdivision) issue announcements and provide guidance from time to time through their official websites, public events (seminars/ conferences) and the media.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The Digital Security Authority (DSA), supervised by the Commissioner and the Deputy Commissioner of Electronic Communications, is the regulatory authority responsible for the application of the NIS Law.

The Cyber Security Incident Response Team (CSIRT) under the DSA is activated upon the occurrence of a catastrophic event, where there is loss of service or information. It coordinates and assists owners/managers, banking organizations and internet service providers to ensure (at least) a minimum level of security by implementing proactive and reactive security services to reduce risks from their internal network and cyber security incidents, as well as to respond to such types of incidents when they occur. It also undertakes awareness-raising actions to educate the local population and national stakeholders about the adverse effects of cyber threats. It provides timely advice to all its members and makes efforts to introduce advanced security services such as security testing, vulnerability scanning and active network monitoring.

Furthermore, the DSA cooperates with the Deputy Ministry of Research, Innovation and Digital Policy to facilitate the implementation of the government's Security Operations Centre (SOC) for the protection of the critical data infrastructures in the private and the public sector.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

The individual data privacy rights provided in Chapter 3 of the GDPR apply.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Individual data privacy rights in Cyprus are enforced through both the judicial system and the Data Protection Commissioner.

The Commissioner has the power to impose administrative fines in accordance with Article 83 of the GDPR. The Courts have the power to impose fines and/ or imprisonment sentences for the violation of certain offences under the GDPR and the relevant data protection laws. Claims for compensation for violation of individual privacy rights are decided by the Cyprus courts.

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

Any person whose legal rights to privacy have been violated has a private right of action before the Cyprus Courts.

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

Monetary compensation and/ or interim relief can be

ordered by the Cyprus courts in civil litigation proceedings. Compensation can be claimed either as special (actual) damages and/ or general damages. Quantifiable economic losses can be recovered as special damages while losses that cannot be quantified, such as psychological harm, pain and suffering or damage to one's private life can be recovered as general damages and are subject to the discretion of the Courts.

43. How are data protection laws in your jurisdiction enforced?

The Data Protection Commissioner and the Electronic Communications Commissioner are responsible for enforcing data protection laws.

Cybersecurity laws are enforced by the DSA.

Both authorities can carry out investigations and impose administrative fines for certain violations within their respective areas of competence.

The Courts of Cyprus can impose fines and/ or imprisonment where criminal offences are committed under any of the Data Protection laws or Cybersecurity laws.

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

The Data Protection Commissioner can impose administrative fines of 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, depending on the nature of violation and the circumstances of each case.

A person convicted by a Court for an offence under the Data Protection Law is subject to imprisonment up to 5 years and/ or a fine up to €50,000, depending on the offence.

The DSA can impose administrative fines up to €200,000, depending on the seriousness of the violation, and, in case of repetition, a fine up to €10,000 for each day the violation continues.

An administrative fine up to €300,400, and in case of repetition of the violation, up to €200,000, can be imposed by the DSA for violation of the provisions of any Decisions and/or Regulations of the European Union.

A person convicted by a Court for an offence under the NIS Law is subject to imprisonment up to 3 years and/ or a fine up to €15,000, depending on the offence.

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

The authorities and the courts have discretion to determine the extent of administrative fines and sanctions, taking into account the seriousness of the violation and the circumstances of each case.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Every natural or legal person has the right to an effective judicial remedy against a decision of the Commissioner concerning them before the Administrative Court.

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

In July 2023, a new Memorandum of Cooperation was signed between the Data Protection Commissioner and the Commissioner for Communications for matters related to their joint or separate powers, the purpose of which is to define a framework of procedures and to adopt and implement appropriate mechanisms for more efficient and effective cooperation between the two Commissioners, when receiving and/or processing:

a. Notification of personal data breach incidents by providers of publicly available Electronic Communications Services and,
b. Incidents by operators of essential services, critical infrastructure operators and digital service providers that lead to breaches of personal data.

In the past year the Office of the Data Protection Commissioner intensified GDPR enforcement by conducting random audits across various organizations, reviewing their cookie policies and practices and their websites' policies to ensure that they comply with data protection laws and respect user privacy. It also organized and carried out training sessions, with the aim of increasing awareness and understanding of data protection laws.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

On 17th March 2023 the Digital Security Authority (DSA) announced its commitment to improving the security landscape at the national level and aligning the Cyprus Security Strategy with the NIS2 Directive, as well as with the Cybersecurity Act and the Cyber Resilience Act. This was followed in July of 2023 by an announcement for a public consultation procedure which is expected to result in the enactment of new legislation which will bring the existing NIS Law in line with the provisions of the NIS2 Directive.

The Digital Operational Resilience Act (DORA) is an EU Regulation aimed at enhancing the operational resilience of the financial sector against cyber threats. DORA establishes technical standards and requires financial services entities and their critical third-party technology service providers in all EU Member States to implement these standards in their ICT systems by 17 January 2025.

It is also worth noting that in May and December 2023 the Cyprus Securities and Exchange Commission (CySec) issued Circulars C571 and C609 respectively, directing Cyprus Investment Firms to align with the European Banking Authority's Information and Communication Technology guidelines published in 29 November 2019, by June 2024.

On a rather personal protection level, a 2021 proposal for a new law is under consideration by the House of Representatives, which will amend the Criminal Code by introducing the offences of sending messages and making phone calls, through a public communications network, of an offensive, obscene and/or threatening nature and/or with false content, with the aim of causing annoyance, harassment or even unnecessary worry to another person (without however limiting the general right to freedom of expression, which is the main point of controversy). It is worth noting that when this proposal was initially presented such offences were regulated under the Telecoms Law but were removed from it in 2022 with the intention of introducing them into the Criminal Code. However, this did not happen yet, thereby leaving a gap in the legal framework. The amendment is long overdue and as the Attorney General of the Republic has recently stated “I think it's time for the Parliament to take that brave step, to vote on it because I think it's unthinkable that certain actions and behaviours which when done in public places are criminally punishable, while if they are done via the internet – which has greater impact – do not equally constitute criminal offences".

The recent wave of cyber-attacks in Cyprus has revealed that cybercriminals can be very smart and technologically advanced, posing an imminent threat to the security infrastructure of businesses and government services as well as to individuals' privacy rights. Unfortunately, the widespread use of technology both for business and for social/ recreational purposes is accompanied by an inevitable rise in Cybercrime incidents, which increases the demand for Cybersecurity and data protection measures and compels organisations to invest in enhancing their Cybersecurity infrastructures to keep up with the fast-paced evolving technological and legal landscape.

Contributors

Nicholas Ktenas
Managing Partner

nicholas.ktenas@cylegal.com