
# The Republic of Cyprus

## Digital Trade Acceleration Initiative

Country Report

## Disclaimer

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document is prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

This Document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Additionally, every effort was made to collect comprehensive data for this Document, which was shared with each of the DCO Member States and, through them, with relevant government agencies. The data collected was current as of September 2024, and there may have been developments or updates since that time. DCO does not undertake any responsibility for such subsequent developments or the use of data that may no longer be current.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.
The use of this Document is solely at the User's own risk. Under no circumstances shall DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the Digital Cooperation Organization. The User shall not reproduce any content of this Document without obtaining DCO's consent or shall provide a reference to DCO's information in all cases. By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

## How to Read This Report

This comprehensive report is structured to guide readers to the information that interests them most. Three sections illuminate the regulatory assessment from different perspectives:

Section A is the core of this report. It assesses the domestic regulatory environment across twelve policy areas, with three subsections for each.

1. Our guiding questions analyse how each policy area interacts with digital trade.
2. Our summaries condense the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities.
3. Our source lists provide a repository of official sources to facilitate further analysis.

Section B provides a factsheet that describes the local digital economy across four key dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.

Section C outlines international commitments and references the international fora in which it engages on digital issues.

# Table of Contents

# Executive Summary

The purpose of this report is to provide a detailed description of the regulatory environment affecting businesses and consumers engaging in digital trade. We illuminate the regulatory environment from three perspectives:

01 A comprehensive regulatory assessment explains the regulatory environment across twelve policy areas.

02 A factsheet describes the local digital economy across four dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.

03 An overview of existing international commitments characterises efforts to accelerate digital trade.

The regulatory assessment is the main contribution of this report and provides the following findings:

### Data Protection:

A legal basis is required for data processing, including user consent and contractual necessity. Data subjects are granted the rights to information, access, rectification, deletion, objection, and portability. Data processors must designate a data protection officer and establish representation within the European Union, but are not required to register.

### Cross-Border Data Transfers

Data flows to the European Union (EU) are unrestricted. Outside the EU, data transfers are only allowed to countries whose data protection level is equivalent, which are designated via adequacy decisions by the European Commission. In the absence of adequacy, transferors need to implement safeguards such as standard contractual clauses or binding corporate rules. Without safeguards, transfers are only allowed through derogations, including consent to the transfer

### Location of computing facilities:

Data localisation is not mandated in general but a specific mandate applies to telecommunications services. The data protection law foresees a mechanism for the government to restrict transfers of special categories of data. To date, no localisation mandates were established based on this mechanism.

### Online Consumer Protection:

Cyprus regulates online consumer protection via its general consumer protection framework, which prohibits making misrepresentations. Automatic direct marketing messages are only allowed if subscribers have given prior consent and with an unsubscribe option.

### Electronic Transactions:

Electronic transactions are considered equivalent to paper-based transactions, albeit with exceptions such as real estate and inheritance transactions. The framework distinguishes between electronic signatures, advanced electronic signatures, and qualified electronic signatures.

### Trade Facilitation with Digital Means:

Cyprus provides trade administration documents for imports in electronic form and enables electronic submission. The operational single window, as well as a computerised customs system, automates customs procedures.

### Cybersecurity:

Artificial Intelligence: Cyprus does not have a national AI regulatory framework but the EU AI Act will apply. The AI Act establishes obligations based on AI risk categories, mainly focusing on "high-risk AI systems." The AI Act also establishes technology-specific rules for general purpose AI models.

### Artificial Intelligence:

Cyprus does not have a national AI regulatory framework but the EU AI Act will apply. The AI Act establishes obligations based on AI risk categories, mainly focusing on "high-risk AI systems." The AI Act also establishes technology-specific rules for general purpose AI models.

### Source Code:

The intellectual property law protects software, providing economic and moral rights to authors, with exceptions for "fair use." The EU AI Act further demands source code access for authorities when 1) access is necessary to assess conformity of a high-risk AI system, and 2) testing and auditing procedures based on other documentation have proven insufficient.

### Digital Economy Taxation and Customs Duties:

Digital services/products are subject to value-added tax. E-commerce imports are subject to customs duties and value-added tax. Differential regimes apply for other EU member states compared to non-EU countries. Cyprus does not impose specific direct taxes on providers of digital services and products.

### Electronic Payments:

Cyprus applies both general payment rules and specific rules on electronic payments, deriving the latter from EU acts. Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payment providers.

### SMEs and Digital Inclusion:

Cyprus has implemented several initiatives to support SMEs and disadvantaged groups in accessing digital trade opportunities. These efforts are primarily driven by national strategies and EU programmes, focusing on digital skills development, infrastructure enhancement, and financial support for digital upgrades.

# 01 Domestic Regulatory Environment Assessment

# Domestic Regulatory Environment Assessment

For thriving digital trade among the members of the Digital Cooperation Organization, their regulatory environment should be comprehensive and adaptive. Absence of fundamental regulatory building blocs, regulatory divergence, or explicit barriers can hinder the DCO MS's digital trade reaching its potential.

This section assesses the regulatory environment across twelve policy areas on three layers. First, we answer guiding questions to analyse each policy area's impact on digital trade. Second, we summarise the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities. Third, we provide a repository of official sources to facilitate further analysis.

## We conduct this assessment for the following policy areas:

01 Data Protection

02 Cross-Border Data Transfers

03 Location of Computing Facilities

04 Online Consumer Protection

05 Electronic Transactions

06 Trade Facilitation with Digital Means

07 Cybersecurity

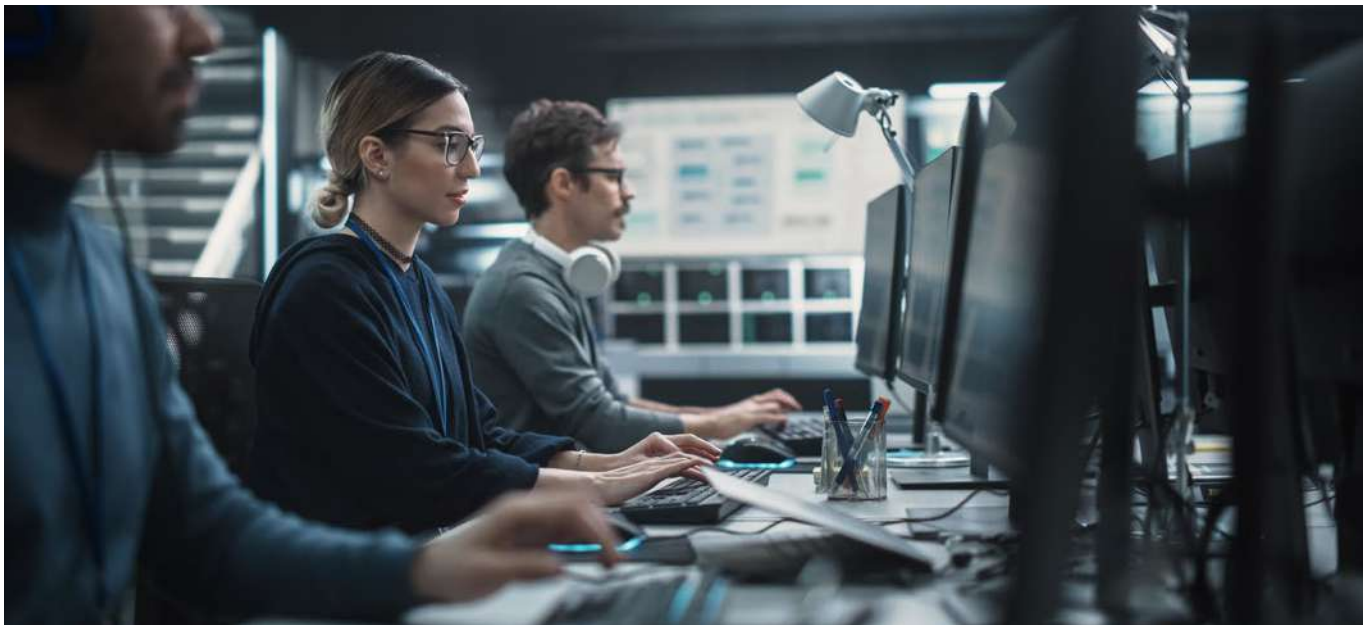
08 Artificial Intelligence

09 Source Code

10 Digital Economy Taxation and Customs Duties

11 Electronic Payments

12 SMEs and Digital Inclusion



# Data Protection

The purpose of this section is to comprehensively characterise the conditions for domestic data collection and processing. Alignment with international best practices in data protection is important for fostering trust whilst facilitating market access. Deviation from these practices could potentially impact digital trade. If the data protection requirements within the member state are too low, that diminishes trust. If data protection requirements are too high, that may delay market entry from international service providers.

## Guiding Questions

We analyse whether user consent is required for the processing of personal data. We then delineate the rights of data subjects and obligations for those processing data, specifically on local representation and registration. Finally, we identify the authority responsible for overseeing and enforcing data protection regulations.

Cyprus requires a legal basis for data processing, including user consent and alternatives such as contractual necessity and legitimate interest. Data subjects are granted the rights to information, access, rectification, deletion, object, and portability. Data processors must designate a data protection officer and establish a representation in the European Union, but don't have to register. The Commissioner for Personal Data Protection is in charge of oversight and regularly publishes enforcement action, including 11 fines, as well as several reprimands and warnings since 2023.

## Summary

- The Cyprus data protection law implements the EU General Data Protection Regulation (GDPR). It ensures the protection of personal data, setting requirements for lawful processing, and data security. Data subjects are granted the rights to access, information, rectification, deletion, objection, and portability. Data processing requires a legal basis, such as user consent, contractual necessity, or legitimate interest. Finally, data processors are required to appoint a data protection officer and establish a representative within the EU.

- The law of Electronic Communications and Postal Services, amended in 2022, addresses data controllers in relation to call recording, and stipulates the conditions of access to information stored on user terminal equipment (e.g. cookies). Cyprus has also incorporated the EU Directive on completing and specifying the institutional framework for the protection of personal data in the electronic communications sector.

- The Commissioner for Personal Data Protection is an independent public authority responsible for implementing EU and national data protection legislation. The Commissioner conducts audits and inspections of data controllers and processors; imposes fines, and collaborates with other national authorities and international organisations to enhance data protection standards. Since 2023, the Commissioner has issued 11 fines; several warnings and reprimands.

- Cyprus has issued a number of instructions, all based on the EU's directives and regulations, including guidelines on data protection officers and the right to data portability. It publishes instructions on the identification of the lead supervisory authority of controllers or processors, data protection impact assessment, and codes of conduct and monitoring bodies.

# SOURCES

**Primary Legislation**

- Law 125(I)/2018 | Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement
- Law 26(I)/2022 (amendment of law 125(I)2018)
- Law 23(I)/2022 | Regulation of electronic communications and postal services (amendment of law 112(I)/2004)
- Directive (EU) 2016/679 | General Data Protection Regulation (GDPR) - consolidated
- Directive (EU) 2009/136/EC | ...the processing of personal data and the protection of privacy in the electronic communications sector...

**Guidelines**

- Commissioner for Personal Data Protection: Guideline on Data Protection Officers
- Commissioner for Personal Data Protection: Guidelines on the Right to data portability
- Commissioner for Personal Data Protection: Guidelines for the identification of the lead supervisory authority of controllers or processors
- Commissioner for Personal Data Protection: Guidelines for Data Protection Impact Assessment (DIA)
- Commissioner for Personal Data Protection: Guidelines on automated decision-making and profiling for the purposes of Regulation 2016/679
- Commissioner for Personal Data Protection: Guidelines on the notification of personal data breaches under EU Regulation 2016/679
- Commissioner for Personal Data Protection: Guidelines on transparency under EU Regulation 2016/679
- Commissioner for Personal Data Protection: Guidelines 05/2020 on consent under Regulation 2016/679
- Commissioner for Personal Data Protection: Guideline 2/2019 on the processing of personal data
- Commissioner for Personal Data Protection: Guideline 1/2019 on Codes of Conduct and Monitoring Bodies under EU Regulation 2016/679
- Commissioner for Personal Data Protection: Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
- Commissioner for Personal Data Protection: Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)
- Commissioner for Personal Data Protection: Guideline 1/2018 on the certification and definition of criteria in accordance with Articles 42 and 43 of the Regulation 2016/679
- EU Working Party: Working Document 02/2013 providing guidance on obtaining consent for cookies
- Office of the Commissioner for Personal Data Protection: Decisions
- EU Working Party: Opinion 04/2012 on Cookie Consent Exemption

**Oversight Authorities**

- The Commissioner for Personal Data Protection

# Cross-Border Data Transfers

The purpose of this section is to analyse the conditions for the cross-border transfer of personal information. On the one hand, data flows are the bloodline of the digital economy. On the other hand, data flows are a controversial subject in geopolitical discussions, as governments worry that transferring data across borders may jeopardise its protection. How a government regulates data transfers reveals the balancing act between free data flows and protection of data abroad.

## Guiding Questions

We differentiate whether the framework treats cross-border transfers differently from in-country transfers. We then analyse the specific conditions for cross-border transfers, ranging from data subject consent, to governmental adequacy decisions, to certification and contractual mechanisms. Finally, we delineate conditions for specific types of cross-border transfers and distil public policy objectives invoked by the government, where explicitly stated.

The GDPR distinguishes between data transfers within the EU and outside the EU. Within the EU, data flows are unrestricted. Outside the EU, data is only allowed to countries whose data protection level is equivalent, which are designated via adequacy decisions by the European Commission. In the absence of adequacy, transferors need to implement safeguards such as standard contractual clauses or binding corporate rules. Without safeguards, transfers are only allowed through derogations, including consent to the transfer or individual transfer approval by the government based on public interest. However, under Cypriot Data Protection Law, the Commissioner can impose limitations on transferring sensitive personal data for public interest reasons, despite GDPR rules.

## Summary

- In Cyprus, cross-border data transfers are regulated under the General Data Protection Regulation (GDPR), applicable across the EU. The Cypriot Data Protection Law of 2018 mandates the Office of the Commissioner to oversee and ensure GDPR compliance. The GDPR generally allows free data flow between EU member states and establishes three types of mechanisms for data data transfers outside the EU: adequacy, safeguards, and derogations. However, under Cypriot law, the Commissioner has the authority to restrict the transfer of sensitive personal data for reasons of public interest, even if such transfers would be allowed under GDPR regulations.

- Transfers to countries with an adequate level of protection are generally allowed. The European Commission designates foreign countries' protection level through adequacy decisions. So far, the European Commission has adopted adequacy decisions for Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom, the United States (under the EU-US Data Privacy Framework) and South Korea.
  For transfers to countries without adequate data protection, the EU requires appropriate safeguards. Safeguards include standard contractual clauses, binding corporate rules, as well as approved codes of conduct and certifications.

- In the absence of both adequacy and safeguards, the EU provides specific derogations in which data transfers are still allowed. Derogations include the data subject's consent and the necessity to uphold public interest or vital interest, among others. Finally, in specific situations where none of the mechanisms above apply, single transfers can be approved by the government.

- There are no public, official sources on secondary legislation and guidelines in Cyprus. The country aligns with the EU's guidelines.

# SOURCES

**Primary Legislation**

- Law 125(I)/2018 | Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement
- Directive (EU) 2016/679 | General Data Protection Regulation (GDPR) - consolidated
- Directive (EU) 2016/680 | The protection of natural persons with regard to the processing of personal data

**Guidelines**

- European Data Protection Board (EDPB): Guidelines on International Transfers of Data
- European Data Protection Board (EDPB): Endorsed WP29 Guidelines
- European Commission: Adequacy decisions
- EU: General Data Protection Regulation (GDPR) | Third Countries
- Data Privacy Framework (DPF) Program

# Location of Computing Facilities

The purpose of this section is to crystallise instances in which data must be stored in local computing facilities. Data localisation mandates require foreign providers to invest in or rent local infrastructure. This can create a significant barrier to digital trade due to burdensome procedural requirements or costs. Such requirements are thus subject to international scrutiny regarding their justification and scope.

## Guiding Questions

We analyse whether the framework generally requires data to be stored in the national territory. We then analyse whether data localisation requirements apply to specific data types, such as infrastructure or health data. For each identified localisation requirement, we distil the public policy objective invoked by the government, if it is explicitly stated.

Cyprus does not mandate data localisation in general. A localisation requirement applies to telecommunications services in Cyprus. A similar requirement was invalidated at the EU level. In addition, the data protection law foresees a mechanism for the government to restrict transfers of special categories of data, for important reasons of public interest. To date, no localisation mandates were established based on this mechanism.

## Summary

- Neither the EU General Data Protection Regulation nor Cypriot data protection laws mandate general data localisation. However, a specific localisation requirement applies regarding telecommunications services.

- The EU Data Retention Directive originally required the localisation of data retained from electronic communications services, but was invalidated by the Court of Justice of the EU in a 2014 ruling. The Cypriot Law on the Retention of Telecommunications Data for the investigation of serious criminal offences, which incorporated the EU Data Retention Directive, still requires telecommunications providers to retain data they generate or process in their jurisdiction. While the Supreme Court of Cyprus invalidated certain provisions of the Directive and the Law in 2011, the rest of the Law, including the localisation requirement, is still in force.

- In addition, the Data Protection Law grants the government the authority to impose specific restrictions on data transfers for special categories of personal data, for public interest. Special categories include genetic and biometric data for purposes of health and life insurance. No localisation mandates were issued.

# SOURCES

- Law 125(I)/2018 | Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such data
- Law 183(I)/2007 | The Retention of Telecommunications Data for the Investigation of Serious Criminal Offences Law of 2007
- Directive (EU) 2006/24/EC | on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks...[no longer in force]
- Court of Justice (EU) | Judgement of 8 April 2014 - Digital Rights Ireland, Joined Cases C-293/12 and C-594/12
- Decision on the application of Law 183(I)/2007 on the disclosure of telecommunications data

# Online Consumer Protection

This section provides a detailed overview of the approach to protecting online consumers.
A well-regulated online consumer protection framework is crucial for fostering trust and confidence in online transactions. In the context of international trade, the implementation of strong online consumer protection regulations enables secure cross-border transactions and promotes the expansion of e-commerce.

## Guiding Questions

We contour whether the online consumer protection framework is specific to online consumption or applies general rules thereto. We then delineate the practices that are considered violations of consumer protection and distil any special obligations for e-commerce platforms. We further analyse the regulatory approach regarding spam. Finally, we explain which authority oversees online consumer protection.

Cyprus regulates online consumer protection via its general consumer protection framework, especially the consumer protection law. The law prohibits several practices, including making misrepresentations and failing to deliver products or provide services after charging consumers.
E-commerce platforms are not subject to indirect obligations but must adhere to transparency and non-discrimination requirements, in ranking lists.
Spam is governed by a dedicated regulation, which establishes that automatic direct marketing messages are only allowed if subscribers have given prior consent and that spam emails must contain a free and easy unsubscribe option. The Consumer Protection Service, under the Ministry of Energy, Trade and Industry, oversees consumer protection and has issued four fines since January 2023.

## Summary

- The Consumer Protection Law safeguards consumers rights and ensures fair business practices. It prohibits unfair commercial practices, including providing false information and charging consumers without permission. The 2022 amendment aligns Cypriot legislation with EU standards and adapts it to digital circumstances. E-commerce platforms are not subjected to indirect obligations but are required to be transparent and non-discriminatory, for example in ranking lists.

- The Consumer Protection Law is complemented by other Cypriot laws. The law of Electronic Communications and Postal Services requires consent for automatic direct marketing messages (including spam), and mandates transparency. The law on Alternative Dispute Resolution for Consumer Disputes ensures that disputes on sales of goods between consumers and traders are submitted to an alternative dispute resolution body. The law on Protection of Collective Interests of Consumers authorises entities to initiate actions on behalf of consumers to address violations of collective interests in the digital marketplace. The law on Sales of Goods aligns with EU directives and establishes rules on sales contracts between the seller and the consumer and prohibits misleading advertising practices. The Regulatory Administrative Act of 2017 regulates online dispute resolution through online platforms in cross-border online transactions.

- As a member of the EU, Cyprus incorporates several EU consumer protection rules. Recently the amended Consumer Protection law transposed the EU directive on Modernisation of Union Consumer Protection Rules. Other Cyprus laws have transposed the EU directives on consumer rights in the digital space, online dispute resolution, and rules concerning cooperation between online platforms and national authorities to enforce consumer protection.

- In addition, the Contracts for the Supply of Digital Content and Digital Services Law 2021 incorporated certain provisions certain of the EU Digital Services Act, including tiered obligations for intermediary services, hosting services, online platforms, and "very large" online providers with at least 45 million average monthly users in the EU.

- The Consumer Protection Service is the primary consumer protection authority in Cyprus. It operates under the Ministry of Energy, Trade and Industry and oversees market compliance and handles consumer complaints. Since January 2023, CPS has issued four fines.

- The Influencer Marketing Strategy, published by the Advertising Control Agency of Cyprus, ensures transparency and authenticity in influencer marketing to protect consumers from misleading or deceptive advertising. Consumers should be informed whether the content they are exposed to on social networks is promotional.

# SOURCES

**Primary Legislation**

- Law 112(I)/2021 | Consumer Protection Law 2021
- Law 46(I)/2022 | 1st Amendment of Law 112(I)/2021
- Law 166(I)/2022 | 2nd Amendment of Law 112(I)/2021
- Law 112(I)/2004 - Regulation of electronic communications and postal services
- Law 23(I)/2022 | Last Amendment of Law 112(I)/2004
- Law 85(I)/2017 | Alternative Dispute Resolution for Consumer Disputes
- Law 154(I)/ 2020 | Cooperation between Competent Authorities for the Enforcement of Consumer Protection Legislation
- Law 155(I)/2021 | Contracts for the Supply of Digital Content and Digital Services
- Law 154(I)/2021 | Sales of goods
- Law 101(I)/2023 | Amendment of Law 154(I)/2021 | contracts on the sales of goods
- Law 91(I)/2023 | Protection of Collective Interests of Consumers
- Regulation (EU) 524/2013 | Online Dispute Resolution for consumer disputes
- Regulation (EU) 2022/2065 | The Digital Services Act
- Regulation (EU) 2018/302 | Unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market
- Regulation (EU) 2017/2394 | Cooperation between national authorities responsible for the enforcement of consumer protection laws
- Directive (EU) 2019/771 | Contracts for the Sale of Goods
- Directive (EU) 2020/1828 | Representative actions for the protection of the collective interests of consumers
- Directive (EU) 2019/2161 | Better Enforcement and Modernization of Union Consumer Protection Rules
- Directive (EU) 2019/770 | Digital Content & Digital Services
- Directive (EU) 2013/11/EU | Online Dispute Resolution
- Directive (EU) 2014/92/EU | on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features

**Secondary legislation**

- Regulatory Administrative Act 69/2017 | Determination of penalties for violations of EU Regulation 524/2013

**Guidelines**

- Influencer Marketing Strategy
- Administrative fine of €20,000 to Thowra Limited | Consumer Protection Service (CPS)
- Administrative fine of €20,000 to Gan Direct Insurance | Consumer Protection Service (CPS)
- Administrative Fine €15.000 to SCB DIY Company Ltd (decision after a hierarchical appeal) | Consumer Protection Service (CPS)
- Administrative fine of €30,000 to Dixons South - East Europe S.A. (decision following a hierarchical appeal) | Consumer Protection Service (CPS)

**Oversight Authorities**

- Consumer Protection Service - CPS

# Electronic Transactions

The purpose of this section is to identify whether there are any regulatory hurdles to electronic transactions compared to paper-based or face-to-face transactions of equivalent substance. A transaction contains different aspects such as the validity of the contract, signature, and authentication.

## Guiding Questions

We focus on whether the electronic transactions framework is binding and whether it recognises electronic transactions as equivalent to paper-based transactions. We then differentiate the various types of electronic signatures in the framework. Finally, we distil whether electronic authentication is permitted and whether the government provides such authentication.

Cyprus's electronic transactions framework comprises several binding legal acts at the national and EU level. Electronic transactions are considered equivalent to paper-based transactions, albeit with exceptions such as real estate and inheritance transactions. The framework distinguishes between electronic signatures, advanced electronic signatures, and qualified electronic signatures, which are recognised as equivalent to hand-written signatures. Cyprus recognises foreign-issued electronic signatures and establishes a mechanism to recognise foreign "trust service providers." Finally, the government provides an authentication service and recognises authentication provided by other EU member states .

## Summary

- Cypriot and European law recognise and regulate electronic transactions. The law on Establishing the Framework on Electronic Signatures of 2004 states that an advanced electronic signature, based on a recognised certificate and created using a secure signature creation device, is considered legally equivalent to a handwritten signature. Additionally, the Law recognises "trust service providers" recognised within the EU and establishes a mechanism for the mutual recognition of trust services from third countries. The Cypriot law incorporating the EU Regulation on Electronic Identification of 2018 mandates that an electronic signature has equivalent legal force to a handwritten signature. Additionally, the law on Information Society Services and E-commerce of 2004 includes provisions on e-transactions and recognises the validity of contracts concluded by electronic means.

- The Cypriot framework follows the EU's rules, which also accepts electronic transactions, differentiates three types of electronic signatures (electronic signature, advanced electronic signature and qualified electronic signature) and recognises authentication. The EU's harmonisation efforts include the mutual recognition of trust service providers across EU countries, as well as the acceptance of electronic identification issued by other member states.

- Cyprus and the EU have issued several pieces of secondary legislation on electronic transactions (see list below) that specify requirements and define procedures for electronic identification, including international cooperation. Cyprus has also issued several administrative acts for the harmonisation of the national legislation with the EU regulation on e-transactions.

- The Department of Electronic Communications of the Deputy Ministry of Research, Innovation and Digital Policy was established in 2003. It regulates and supervises trust service providers, facilitates electronic signatures and other e-identification services, and complies with EU regulations. It also manages the national list of certified trust service providers which are recognised and valid across the EU.

- The Deputy Ministry of Research, Innovation and Digital Policy has issued guidelines on the verification of valid approved electronic signatures. In addition, the Department of Information and Technology services of the Ministry, has published the national eID framework on authentication and remote signature.

# SOURCES

**Primary Legislation**

- Law 156(I)/2004 | The Regulation on Certain Aspects of Information Society Services and in particular Electronic Commerce and Related Matters
- Law 97(I)/2007 | The Regulation on Certain Aspects of Information Society Services and in particular Electronic Commerce and Related Matters| amendment of Law 156(I)/2004
- Law 188(I)/2004 | regulatory framework for electronic signatures and other matters
- Law 55(I)/2018 | providing for the application of the regulation EU 910/2014
- Law 60(I)/2021 | Amendment of Law 55(I)/2018 | providing for the application of the regulation EU 910/2014
- Regulation (EU) No 910/2014 | on electronic identification and trust services for electronic transactions in the internal market
- Regulation (EU) 2015/1502 | on setting out minimum technical specifications and procedures for assurance levels for electronic identification
- Regulation (EU) 2015/1501 | on the interoperability framework on electronic identification
- Directive (EU) 2000/31/EC | on certain legal aspects of information society services, in particular electronic commerce
- Directive (EU) 2014/55/EU | electronic invoicing in public procurement

**Secondary legislation**

- Normative Administrative Act 167/2018 | Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
- Normative Administrative Act 157/2021 | amending Normative Administrative Act 167/2018 | The provisions on the implementation of Regulation (EC) No 910/2014
- EU Commission Decision 2009/767/EC | setting out measures facilitating the use of procedures by electronic means through the 'points of single contact'
- Decision (EU) 2022/2481 | 2030 Digital Decade Policy Agenda
- Decision (EU) 2015/1505 | laying down technical specifications and formats relating to trusted lists
- Decision (EU) 2015/1506 | laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies
- Decision (EU) 2015/1984 | defining the circumstances, formats and procedures on electronic identification trust services for electronic transactions in the internal market
- Decision (EU) 2015/296 | establishing procedural arrangements for cooperation between Member States on electronic identification
- Decision (EU) 2016/650 | laying down standards for the security assessment of qualified signature and seal creation devices

**Oversight Authorities**

- Department of Electronic Communications

**Guidelines**

- Cyprus National eID Framework
- Operating Guide: Verification of Valid Approved Electronic Signature

# Trade Facilitation with Digital Means

This section analyses how well the domestic regulatory environment is set up to welcome goods and services trade made possible through digital tools. This includes the use of electronic trade documentation, as well as measures designed to support "trade in parcels" and streamline cross-border transactions in the digital economy.

## Guiding Questions

We analyse whether trade administration documents for imports are available and can be submitted in electronic form. We then focus on single windows, enabling persons to submit documentation for import, export, or transit through a single entry point to authorities. Specifically, we outline whether a single window system is operational for trade documentation and whether this system supports international data or document exchange. Finally, we highlight expedited or simplified customs procedures for low-value shipments.

Cyprus provides trade administration documents for imports in electronic form and enables electronic submission. Cyprus provides an operational single window as well as a computerised customs system (THESEAS) to automate the processing of customs import declarations. Imports from other EU countries are not subject to customs duties, while imports from other non-EU countries are subject to a duty de minimis threshold of EUR 150, exempting goods valued below this amount from customs duties.

## Summary

- Cyprus has an operational National Customs Single Window (NCSW), which is part of the EU Single Window Environment for Customs. This system aims to streamline the submission of customs documentation and permits, allowing businesses and traders to provide data through a single portal. The NCSW aims to enhance coordination between customs and other governmental bodies responsible for trade and border management.

- The Cyprus Customs and Excise Department operates under the Ministry of Finance and is responsible for imposing and collecting import duties, excise duties for goods entering Cyprus from third countries or other EU member states. Since 2003, the THESEAS system has been an integrated, computerised platform of the Cyprus Customs & Excise Department, aimed at automating and improving customs operations. It enables the electronic submission and processing of customs declarations, and provides a web-based platform for users. THESEAS also simplifies official documentation and integrates the EU customs systems, enabling cross-border trade within the EU. In 2020, it published a manual for the electronic submission of the application for a certificate of customs for EU Goods.

- The 2008 EU decision on a paperless environment for customs and trade, required the Commission and member states to establish secure, integrated and accessible electronic customs systems. It aimed to facilitate the exchange of data from customs declarations, accompanying documents, certificates, and other information. The Union Customs Code (UCC) established the legal framework for customs regulations and procedures within the EU customs territory, designed to align with contemporary trade practices. The 2013 regulation on UCC mandated that all exchanges of information between customs authorities and economic operators must be conducted and stored using electronic data-processing techniques. It required member states to collaborate with the Commission to develop, maintain, and utilise electronic systems for exchanging and storing information between customs authorities and the Commission. The 2015 regulation then mandated the establishment of a European Union Single Window. It provides electronic services at union and national levels and enhances information exchange between national single window environments for customs and union non-customs systems.

- The Cypriot trade facilitation framework is based on EU rules, which differentiates between trade within the EU and trade with third countries. For trade within the EU, Cyprus complies with the EU Single Window environment and utilises the New Computerised Transit System, enabling electronic submission of required documents and fostering cross-border data exchange. The EU Union Customs Code (UCC) mandates that no customs duties or tariffs are applied to goods traded between EU member states. The Common Customs Tariff (CCT) applies to goods imported from non-EU countries, with a duty de minimis threshold of EUR 150, exempting goods valued below this amount from customs duties.

# SOURCES

**Primary Legislation**

- The Customs Code Laws from 2004 to 2022
- Decision No 70/2008/EC | on a paperless environment for customs and trade
- Regulation (EU) 2022/2399 | establishing the European Union Single Window Environment for Customs
- Regulation (EU) No 952/2013 | laying down the Union Customs Code (UCC)
- Regulation (EU) 2015/2447 | laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 laying down the Union Customs Code
- Directive (EU) 2017/2455 | as regards certain value added tax obligations for supplies of services and distance sales of goods

**Guidelines**

- Manual for the Electronic Submission of the Application for a Certificate of Customs for EU Goods
- European Commission | Technical support for the preparation of the national customs single window in Cyprus
- EU: Electronic Customs Multi-Annual Strategic Plan for Customs 2023
- European Commission: Customs formalities for low value consignments (duty de minimis threshold)
- European Commission: VAT One Stop Shop
- European Commission: Buying goods online coming from a non-European Union country

**Oversight Authorities**

- Department of Customs and Excise
- "THESEAS" Cyprus Customs computerised Systems

# Cybersecurity

This section aims to assess whether the cybersecurity requirements of the member state broadly align with international best practices. While cybersecurity is a critical component of digital policy, its relevance to digital trade is limited. Cybersecurity primarily concerns national defence, critical infrastructure, cybercrime prevention, and system integrity. However, alignment with international cybersecurity standards is essential for creating a secure environment conducive to digital trade. Insufficient cybersecurity standards can undermine trust, while overly stringent requirements may hinder market entry for international service providers.

## Guiding Questions

We outline whether there is a regulatory framework regarding cybersecurity. We explain whether this framework is risk-based, creating tiered obligations depending on the extent of cybersecurity risk. We then analyse whether and to whom incident notification is required. Finally, we explain which authority oversees cybersecurity.

Cybersecurity rules are enshrined in the national Network and Information Systems Security Law and several EU legal instruments. The Law requires cybersecurity rules that are commensurate to the risk level and demands incident notification to users and government authorities. In addition, personal data breaches must be notified to authorities and data subjects. Cybersecurity oversight is divided between the National Computer Security Incident Response Team, the Digital Security Authority, and the Directorate for Cybersecurity. The CSIRT regularly publishes public data on incidents and alerts.

## Summary

The Network and Information Security Law of 2020 is the main legal framework governing cybersecurity in Cyprus. The law establishes the Digital Security Authority (DSA) and its main responsibilities and regulates digital service providers. It also facilitates communication between stakeholders during cybersecurity incidents and specifies penalties for organisations that fail to comply with cybersecurity obligations. Furthermore, the law mandates that operators shall notify the authorities on incidents that disrupt the continuity of the delivered services. They shall also inform the public to prevent the occurrence of an incident.

**Cyprus, as a member of the EU, incorporated several cybersecurity rules in its legal framework:**

01 Cyprus has participated in consultations for the transposition of the EU regulation on European Cybersecurity, Industrial, Technology and Research Competence Centre Regulation 2021.

02 Cyprus incorporated the NIS Directive on the measures on high common level of security of network and information systems of 2016 and the regulation on the establishment of the European Union Agency for cybersecurity (ENISA).

03 The EU's latest NIS 2 Directive is expected to be incorporated into Cypriot legislation by 2024. Among other obligations, the NIS 2 Directive requires essential and important entities to inform government authorities and users on cybersecurity incidents.

04 In January 2025, the EU Digital Operational Resilience Act (DORA), will come into effect, introducing a comprehensive set of cybersecurity requirements for the financial sector that applies directly since DORA is an EU Regulation.

05 Additionally, the EU Cyber Resilience Act is set to enter into force in the second half of 2024, applying directly since the Act an EU Regulation. The Act aims to protect consumers and businesses purchasing or using products or software with digital components. Member states, including Cyprus, are expected to adhere to new EU regulations in around 24 months after the official adoption of the acts.

06 Finally, the EU General Data Protection Regulation requires personal data breaches to be notified to authorities and data subjects.

**Several government authorities cover cybersecurity:**

01 The Digital Security Authority (DSA) is the designated National Cybersecurity Coordination Centre of Cyprus. Established in 2018, this independent governmental agency operates under the supervision of the Commissioner of Communications. The DSA fosters collaboration between the public and private sectors and enforces cybersecurity regulations. It also strengthens the resilience of national digital infrastructure against cyber threats and attacks.

02 The National Computer Security Incident Response Team of Cyprus (National CSIRT), is incorporated in the DSA and was established in 2016. It coordinates critical information infrastructure (CII) owners and administrators to ensure a baseline level of security for cybersecurity incidents. The National CSIRT is responsible for responding to such incidents, processing data, and notifying the competent authorities. The National CSIRT-CY received 21,984 alert emails from intelligence gathering platforms. After analysing and identifying mitigation measures, it forwarded around 3,000 emails to critical intelligence infrastructures, containing 146,016 suspicious IP addresses, to inform stakeholders and facilitate any necessary actions.

03 The Directorate for Cybersecurity operates under the Deputy Ministry of Research, Innovation and Digital Policy. It is tasked with developing the national cybersecurity strategy and strengthening cybersecurity structures.

- The regulatory administrative acts of 2020, 2022 and 2024 complement the Security of Networks and Information Systems Law of 2020. They prescribe security measures for key service providers and operators of critical information infrastructure and cybersecurity incident reporting.

- The Ministerial Decree of 2010 established the immediate response bodies for incidents and events related to network and information security (CSIRT / CERT). Additionally, the Regulatory Administrative Acts of 2020 and 2021 introduce security requirements designed to mitigate risks associated with next-generation electronic communications networks and services 5G.

- The Cybersecurity Capacity Review outlines key areas for enhancing national cybersecurity, focusing on improving legal frameworks, incident response capabilities, and public awareness.The Cybersecurity Strategy of 2020, which is currently under review, is anticipated to be released for public consultation. The Strategy aims to establish a comprehensive legislative framework and mechanisms. It also prioritises measures on the preparation, protection, detection and response to cyber threats. The Cyprus Strategic Roadmap for the Digital Decade (2023), developed by the Deputy Ministry of Research, Innovation and Digital Policy, outlines the strategic goals to be achieved by 2030. It includes the establishment of a cybersecurity skills academy to support business digitalization. In addition, the Cyprus National Action Plan 2021-2025 on digital skills, encompasses initiatives for training courses designed to enhance capacity building and cybersecurity threat protection.

# SOURCES

**Primary Legislation**

- Cyprus
- Law 89(I)/2020 | Network and Information Systems Security Law of 2020
- Law 17(I)/2018 | The Network and Information Systems Security Act of 2018
- EU
- Regulation (EU) 2019/881 | ENISA and on information and communications technology cybersecurity certification
- Regulation (EU) 2021/887 | European Cybersecurity, Industrial, Technology and Research Competence Centre
- Regulation (EU) 2022/2554 | Digital Operational Resilience Act (DORA)
- Proposal for Regulation EU on Cyber Resilience Act | on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
- Directive (EU) 2016/1148 | Measures for a high common level of security of network and information systems
- Directive (EU) 2022/2555 | Measures on high common level of cybersecurity(NIS 2)

**Oversight Authorities**

- Digital Security Authority | Office of Commissioner of Communications
- National CSIRT (National Computer Security Incident Response Team of Cyprus)
- Directorate for Cybersecurity | Deputy Ministry of Research, Innovation and Digital Policy
- European Union Agency for Cybersecurity (ENISA)

**Secondary legislation**

- Digital Security Authority: Regulatory Administrative Act 389/2020 | Security of Networks and Information Systems Law
- Digital Security Authority: Regulatory Administrative Act 39/2022 | Security of Networks and Information Systems Law
- Digital Security Authority: Regulatory Administrative Act 245/2024 | Security of Networks and Information Systems Law
- Digital Security Authority: Decree of KDP 358/2010 (2010) | Security of Networks and Information Systems Law
- Digital Security Authority: Regulatory Administrative Act 408/2020 | Security of Networks and Information Systems Law
- Digital Security Authority: Regulatory Administrative Act 310/2021 | Security of Networks and Information Systems Law

**Guidelines**

- Digital Security Authority: Cybersecurity Capacity Review 2017
- Digital Security Authority: Cybersecurity Strategy 2020
- National Digital Decade | Strategic Roadmap 2023
- Digital Skills | National Action Plan 2021-2025
- Digital Security Authority: Annual Report 2021

# Artificial Intelligence

This section offers an overview of how artificial intelligence (AI) is regulated in the member state. The focus is on the policy response to the rise of widely accessible AI, covering both AI-specific regulatory frameworks and the application of existing laws to AI technologies. From a digital trade perspective, the key consideration is whether the member state aligns with emerging international practices.

## Guiding Questions

We outline whether there is a specific regulatory framework addressing AI. If so, we analyse whether the framework is risk-based, meaning it establishes obligations based on the level of AI risk. We also analyse whether the framework is technology-based, meaning it establishes rules based on specific AI technologies. Finally, we reference guidance released by regulatory agencies on how the existing, non-AI-specific framework, applies to AI providers.

Cyprus does not have a national AI regulatory framework but, as an EU member, the AI Act will apply. The AI Act establishes obligations based on AI risk categories, mainly focusing on "high-risk AI systems." The AI Act also establishes technology-specific rules for general purpose AI models. No regulatory agencies have published guidance on how existing rules apply to AI providers. Several government strategies and action plans emphasise the potential of AI but do not specify guardrails.

## Summary

Currently, Cyprus does not have a national AI regulatory framework. As a member of the EU, Cyprus applies the Artificial Intelligence (AI) Act, which entered into force in August 2024, and will be implemented over the coming years. The AI Act establishes tiered obligations depending on AI systems' risk classification. AI systems posing unacceptable risk levels, for example social scoring, are prohibited starting February 2025. High-risk AI systems, for example AI systems used in critical infrastructure, education, and employment, are subject to a range of obligations. Obligations cover impact assessment, risk management, testing, data governance, cybersecurity, conformity assessment, and post-market monitoring, among others. In addition, the AI Act includes transparency obligations for AI systems that interact with natural persons and rules for general-purpose AI models. In addition to the AI Act, the EU is currently deliberating a directive adapting liability rules to AI and recently adopted the General Product Safety Regulation, which aims to counter AI-related product risks starting December 2024.

**Cyprus does not currently have a dedicated AI authority yet but is currently deliberating several frameworks that propose such a governance authority:**

01 The National Strategy for AI 2020 outlines a plan to leverage AI for the country's economic and societal development. Published by the Department of Electronic Communications and the Ministry of Transport Communications and Works, it enhances AI research infrastructure. It also establishes ethical guidelines and metrics

02 and key performance indicators (KPIs) to monitor the progress and impact of the AI strategy. Reportedly, the government is currently revising the Strategy to include the formation of an AI Task Force under the Deputy Ministry of Research, Innovation, and Digital Policy.

03 The Strategic Plan 2023-2025 of the Deputy Ministry of Research, Innovation and Digital Policy, formulates, coordinates and monitors the implementation of actions for the development and exploitation of cutting-edge technologies including AI.

04 The National Digital Decade Strategic Roadmap 2023 also includes plans to establish an AI Policy Unit at the Deputy Ministry of Research, Innovation and Digital Policy to increase the use of AI by business and public sector.

# SOURCES

**Primary Legislation**

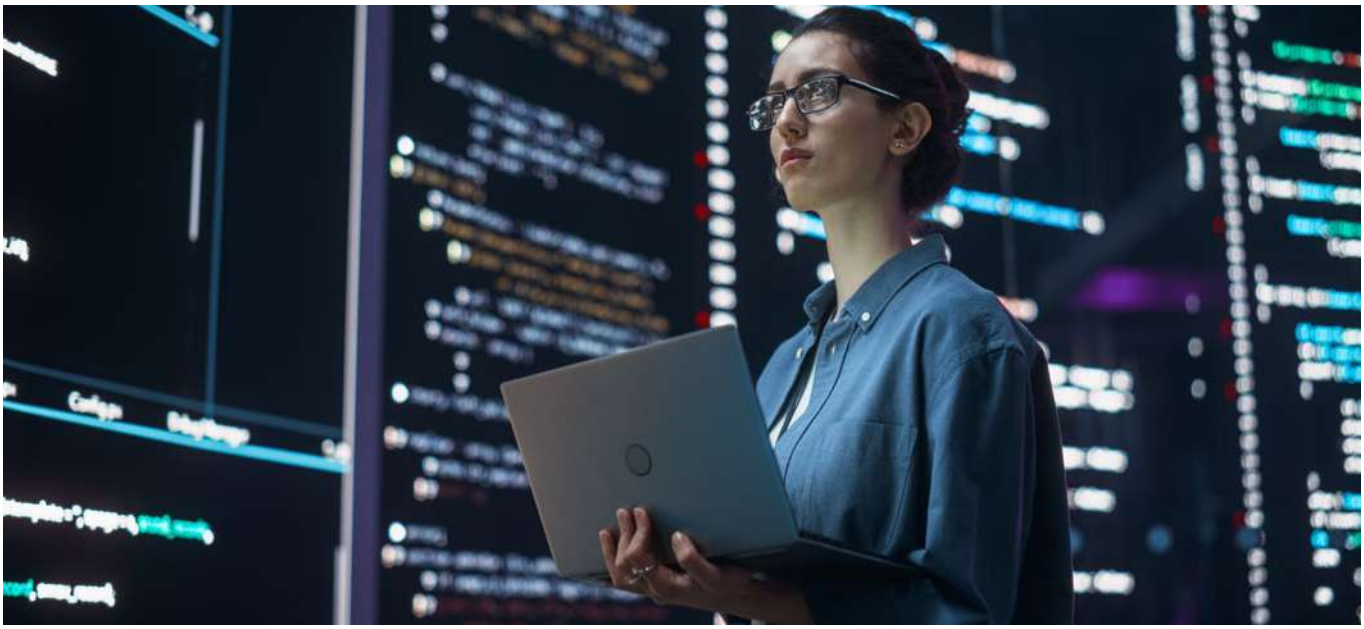
- Regulation (EU) 2024/1689 of the European Parliament and of the Council | EU Artificial Intelligence Act
- Proposal for Directive (EU) | on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)
- Regulation (EU) 2023/988 | on general product safety...

**Guidelines**

- News report: Cyprus revises the National Strategy for Artificial Intelligence [third party source]
- National Strategy for Artificial Intelligence 2020
- Strategic Plan 2023 – 2025 of Deputy Ministry of Research, Innovation and Digital Policy
- National Digital Decade Strategic Roadmap 2023

**Oversight Authorities**

- Deputy Ministry of Research, Innovation, and Digital Policy



# Source Code

Source codes are among the essential trade secrets of the digital economy. Potential disclosure requirements toward the government or domestic private companies can be a major hurdle to market access. The purpose of this section is to identify regulatory or enforcement requirements that risk the required disclosure of source code.

## Guiding Questions

We explain whether source code is generally protected under the intellectual property framework and whether there are exceptions to this protection. We then identify potential source code sharing requirements, explaining the circumstance and specific software to which they apply. Where explicitly stated, we reference the public policy objective invoked by the government.

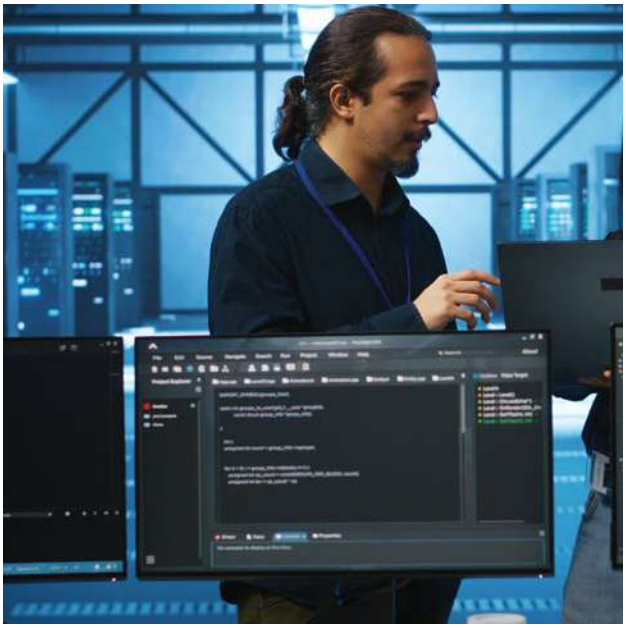
The intellectual property law protects software, providing economic and moral rights to authors. Exceptions to these exclusive rights include “fair use”, for example for research and education. The EU AI Act further demands that market surveillance authorities receive access to source code upon reasoned requests when 1) this access is necessary to assess conformity of a high-risk AI system, and 2) testing and auditing procedures based on other documentation proved insufficient.

## Summary

- The Intellectual Property Law, including its latest amendment in 2022, establishes that software falls under copyright protection. This protection grants authors economic and moral rights, including fair and proportionate remuneration. Exceptions to these rights apply for "fair use" of the protected work, for example for the purpose of criticism, news reporting, research, and education. Copyrighted works may be used without the permission of the copyright owner for such purposes, with proper accreditation of original authors.

- The Intellectual Property Section of the Department of the Registrar of Companies and Intellectual Property (DRCIP), operates under the Ministry of Energy, Commerce, and Industry. It is responsible for the registration and protection of national and EU trademarks, patents, copyright and industrial designs.

- Regarding source code sharing, the EU AI Act states that market surveillance authorities shall be granted access to the source code of a high-risk AI system, if two conditions are fulfilled. First, access must be necessary to verify compliance with specific requirements. Second, all other testing, auditing, or verification methods have been exhausted or proven insufficient. Source code access is granted only upon a reasoned request. Generally, the EU requires member states to protect computer programs under their intellectual property frameworks.



# SOURCES

**Primary Legislation**

- Law 59/1976 | The Intellectual Property and Related Rights Law of 1976
- Law 155(I)/2022 | The Intellectual Property and Related Rights (Amendment) Act 2022
- Regulation (EU) 2024/1689 of the European Parliament and of the Council | EU Artificial Intelligence Act
- Directive (EU) 2009/24/EC | on the legal protection of computer programs

**Guidelines**

- Open Source Software Country Intelligence Report Cyprus 2020 | European Commission

**Oversight Authorities**

- Intellectual Property Section | Republic of Cyprus

# Digital Economy Taxation and Customs Duties

The purpose of this section is to identify how the digital economy is taxed domestically and at the border. This covers direct taxes, indirect taxes, and customs duties, applicable to both digital services/products and e-commerce imports. We focus on whether a) requirements are applied identically to digital services/products as to their analog equivalents and b) requirements are applied identically to domestic and foreign suppliers.

## Guiding Questions

We explain whether customs duties apply to digital services/products as well as e-commerce imports. We then analyse whether indirect taxes, such as value-added-tax, apply to digital services/products as well as e-commerce imports. In addition, we identify any direct taxes imposed specifically on providers of digital services/products, such as digital service taxes. For each tax or duty, we mention whether electronic registration is possible for foreign providers.

Cyprus does not apply customs duties to digital services or products but applies value-added tax (VAT) thereto. Regarding e-commerce imports, Cyprus applies customs duties as well as VAT. Cyprus has adopted the EU's e-commerce VAT package, which removed the VAT de minimis threshold and established a one-stop-shop VAT registration scheme. Imports from other EU countries are not subject to customs duties, while imports from other non-EU countries are subject to a duty de minimis threshold of EUR 150, exempting goods valued below this amount from customs duties. Cyprus does not impose specific direct taxes on providers of digital services and products. Tax registration can be obtained electronically.

## Summary

- Customs duties, which apply e-commerce imports but not to digital services/products, are regulated by the EU Union Customs Code (UCC). The UCC mandates that no customs duties or tariffs are applied to goods traded between EU member states, while the Common Customs Tariff (CCT) applies to goods imported from non-EU countries. For such imports from non-EU countries, a duty de minimis threshold of EUR 150 applies, exempting goods valued below this amount from customs duties. The EU's integrated tariff database (TARIC) provides details on the applicable tariffs and measures for all goods imported into the EU.

**Regarding indirect taxes, Cyprus adheres to the novel EU e-commerce VAT regime, enacted in 2021. With the aim of simplifying VAT procedures, the regime introduced several changes:**

01 The VAT de minimis threshold of EUR 22 was removed, meaning all goods imported into the EU are subject to VAT.

02 The One Stop Shop (OSS) was created for online sellers to register for VAT in only one EU Member State, covering all distance sales within the EU.

03 The Import One Stop Shop (IOSS) was created to simplify VAT declaration and payment regarding distance sales of goods imported from third countries valued below EUR 150. For goods above this value traditional customs and VAT procedures apply.

04 The thresholds for distance sales of goods within the EU were replaced by a new EU-wide threshold of EUR 10,000. Below this threshold, supplies of telecommunications, broadcasting, and electronic services, as well as distance sales of goods within the EU, remain subject to VAT in the Member State where the taxable person is established.

- Starting from January 2024, platform providers must adhere to new EU tax reporting rules. Providers must verify and send information to tax authorities, including an overview of amounts paid and platform commissions. Another EU proposal would standardise VAT reporting, establish a Single VAT Registration and expand record-keeping obligations to short-term accommodation rental and business-to-business supplies providers.

- Regarding direct taxes, Cyprus does not impose specific direct taxes on providers of digital services and products. In 2021, the EU consulted on but then postponed a proposed "digital levy" in view of negotiations on the OECD/G20 Inclusive Framework. From 2024, the directive requires member states to implement the Framework's minimum taxation rules, namely the Income Inclusion Rule and the Undertaxed Payment Rule under Pillar 2 (Global Anti-Base Erosion Rules). The rules affect companies with a global annual turnover of over EUR 750 million.

- The Cyprus Tax Department was established in 2014 and operates under the Ministry of Finance. The Department enforces tax-related laws, collects government revenues and oversees the application of Double Taxation Agreements. It also facilitates the exchange of tax information through European Directives and international conventions. The department has published instructions on VAT rules for cross border trade.

- Cyprus has further issued ministerial decrees on VAT special regimes for intra-community distance sales of goods, for persons not established in the EU and for special schemes for sales of goods imported from third countries. The European Commission has also issued several explanatory notes and guidelines on VAT e-commerce rules, and excise duty exemptions.

# SOURCES

**Primary Legislation**

- Law 95 (I)/2000 | The Value Added Tax Law (including all latest amendments)
- Law 70(I)/2014 | The Department of Taxation Law of 2014
- Regulation (EU) No 952/2013 | laying down the Union Customs Code (consolidated)
- Commission Delegated Regulation (EU) 2015/2446 | supplementing Regulation (EU) No 952/2013...as regards detailed rules concerning certain provisions of the Union Customs Code (consolidated)
- Commission Implementing Regulation (EU) 2015/2447 | laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (consolidated)
- Commission Delegated Regulation (EU) 2016/341 | supplementing Regulation (EU) No 952/2013...as regards transitional rules for certain provisions of the Union Customs Code where the relevant electronic systems are not yet operational and amending Delegated Regulation (EU) 2015/2446 (consolidated)
- Regulation (EU) 282/2011 | measures for Directive 2006/112/EC on the common system of value added tax (2022 consolidated version)
- Regulation (EU) 2017/2459 | laying down implementing measures for Directive 2006/112/EC on the common system of value added tax
- Directive (EU) 2006/112/EC | on the common system of value added tax
- Directive (EU) 2017/2455 | as regards certain value added tax obligations for supplies of services and distance sales of goods
- Directive (EU) 2019/1995 | amending Directive 2006/112/EC as regards provisions relating to distance sales of goods and certain domestic supplies of goods
- Directive (EU) 2022/2523 | on ensuring a global minimum level of taxation for multinational enterprise groups and large-scale domestic groups in the Union (consolidated)
- Directive (EU) 2021/514 | amending Directive 2011/16/EU on administrative cooperation in the field of taxation
- Proposal for Regulation (EU) amending Regulation (EU) No 904/2010 | as regards the VAT administrative cooperation arrangements needed for the digital age
- Decision (EU) 2021/942 | rules for the application of Council Directive 2006/112/EC as regards the establishment of the list of third countries with which the Union has concluded an agreement on mutual assistance

# SOURCES

**Secondary Legislation**

- Decree 503/2021 : The Value Added Tax (Special Regime for Services Supplied by Persons Not Established in the Community) Regulations 2021
- Decree 501/2021: The Value Added Tax (Special Regime for Intra-Community Distance Sales of Goods, for Supplies of Goods within the Republic made through Electronic Interfaces Facilitating Such Supplies and for Services Provided by Taxable Persons Established in the Republic but Not Established in the Member State of Consumption) Regulations of 2021
- Decree 500/2021 : The Value Added Tax (Special Scheme for Distance Sales of Goods Imported from Third Territories or Third Countries) Regulations 2021

**Guidelines**

- Brochure_ New VAT Rules for Cross-border Trade | Tax Department Cyprus
- Explanatory Notes on VAT e-commerce rules | European Commission
- Buying goods online – EU Member States' rules for customs declarations, customs value, excise duty exemptions, returns and prohibited/restricted goods | European Commission
- Remarks by Commissioner Gentiloni at the Eurogroup press conference | European Commission
- Buying goods online coming from a non-European Union country
- VAT One Stop Shop | European Commission
- The One Stop Shop | European Commission
- Explanatory Notes on VAT e-commerce rules | European Commission
- Oversight Authorities
- Cyprus Tax Department I Ministry of Finance

# Electronic Payments

This section evaluates the key aspects of the regulatory environment governing electronic payments and its openness to processing payments across borders. Electronic payments are a critical enabler of digital and digitally facilitated trade. While data protection, data flows, and electronic transactions play a significant role in electronic payments, they have been addressed previously. This section focuses on whether a) digital payment services/products are subject to the same requirements as their analogue equivalents, and b) whether these requirements are applied equally to domestic and foreign providers.

## Guiding Questions

We outline whether there is a regulatory framework specifically addressing electronic payments. We then distil know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to electronic payments. In addition, we delineate licensing requirements and procedures for entities that offer electronic payment services. Finally, we reference special regulatory requirements for cross-border electronic payments.

Cyprus applies both general payment rules and specific rules on electronic payments, deriving the latter from EU acts. The EU Payment Services Directive specifies know-your-customer, anti-money-laundering, and counter-terrorism-financing rules for electronic payment providers, which are enshrined in several other EU Directives. Cyprus has transposed these EU rules and demands an operating licence by the central bank to provide payment services.

## Summary

Cyprus's Electronic Payments Framework is based on several EU directives that were transposed into national law.

01 The EU directive on payment services establishes the regulatory framework for electronic payments across the EU. It specifies know-your customer (KYC), anti-money laundering (AML), and counter-terroism-financing (CTF) rules that apply to electronic payments.

02 The EU Directive on the use of the financial system for the purposes of money laundering or terrorist financing also includes provisions in electronic payments. If an entity cannot meet customer due diligence requirements, it must refrain from conducting a transaction through a bank account or forming a business relationship. For cross-border business relationships, additional obligations apply, including gathering information about the counterpart and assessing its reputation and AML and CFT controls. The European Banking Authority has issued several opinions and guidelines specifying these requirements.

03 The Cypriot law on the prevention and combating of money laundering incorporated the 2015 EU Directive on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing.

The Central Bank of Cyprus (CBC) is responsible for the licensing and supervision of Electronic Money Institutions (EMIs). It also imposes sanctions, revokes licences and ensures that electronic money institutions comply with the e-money laws of 2012 ans 2018. In 2012, the CBC published a directive on the supervision of the business of EMIs

# SOURCES

**Primary Legislation**

- Law 81(I) of 2012 | Electronic Money Law
- Law 30(I)/2018 | The Electronic Money (Amendment) Law of 2018
- Laws of 2018 to 2023 | The Provision and Use of Payment Services and Access to Payment Systems ( (unofficial consolidation)
- Law of 2017 62(I)/2017 (SEPA Law) | The Single Euro Payments Area Implementation (Amendment)
- Law 13 (I) of 2021 | The Prevention and Combating of Money Laundering (Amendment) Law of 2021
- Regulation (EU) 2017/2055 | supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for the cooperation and exchange of information between competent authorities relating to the exercise of the right of establishment and the freedom to provide services of payment institutions
- Regulation (EU) 2021/1230 | on cross-border payments in the Union
- Directive (EU) 2015/2366 | Payment Services Directive (PSD2)
- Directive (EU) 2015/2366 | Payment Services Directive (PSD2) | 2024 Consolidated Version
- Directive (EU) 2015/849 | the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (2024 consolidated version)

**Guidelines**

- The Electronic Money Institutions Directive of 2012
- Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2
- Opinion of the European Banking Authority (EBA) on obstacles to the provision of third party provider (TPPs) services under article 32(3) of the Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC)
- Opinion of the European Banking Authority (EBA) on the blocking of the provision of Payment Services by Third Party Providers, pursuant to Article 32(3) of Delegated Regulation (EU) 2018/389
- Opinion of the European Banking Authority (EBA) on the appropriate supervisory actions to ensure the removal of barriers to access to payment accounts, in accordance with PSD2 (Law 4537/2018)
- Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card based payment transactions
- EBA PSD2 eIDAS certificates | National identification codes to be used by qualified trust service providers for identification of competent authorities in an eIDAS certificate for PSD2 purposes

# SOURCES

- EBA Registers | Type of identification numbers used in the EBA PSD2 Register and the EBA Credit Institutions Register
- EBA PSD2 DAS certificates | List of email addresses of the national competent authorities that will follow the process for requesting revocation of eIDAS certificates as set out in the EBA Opinion on the use of eIDAS certificates (EBA-OP-2018-7)
- Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2
- EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers
- Single Euro Payments Area (SEPA) | European Central Bank

**Oversight Authorities**

- The Central Bank of Cyprus (CBC)

# SMEs and Digital Inclusion

Digital trade holds the potential to open global markets to SMEs and disadvantaged groups. By leveraging digital technologies, small businesses, rural enterprises, and minority-owned businesses can overcome traditional barriers to international trade, such as high costs, limited market access, and logistical challenges. E-commerce platforms, digital payment systems, and online marketing tools enable these businesses to reach international customers, integrate into global value chains, and attain economies of scale previously limited to larger corporations. This section highlights recent support measures targeted to helping SMEs and disadvantaged groups capitalise specifically on the opportunities of the global digital economy.

## Guiding Questions

We analyse whether the government has established specific programs or initiatives to support SMEs or disadvantaged groups in participating in the digital economy or digital trade. For each program, we distil the objective of the support, the form of support provided, and the target group of the program.

Cyprus has implemented several initiatives to support SMEs and disadvantaged groups in accessing digital trade opportunities. These efforts are primarily driven by national strategies and European Union programmes, focusing on digital skills development, infrastructure enhancement, and financial support for digital upgrades. The initiatives range from broad policy frameworks to specific grant schemes targeting various sectors and business types.

2

## Summary

- The Digital Strategy for Cyprus 2020-2025, adopted in June 2020, establishes the overarching policy framework for the country's digital transformation. In 2023, Cyprus published an updated National Digital Decade Strategic Roadmap, aligning with the European Union's Digital Decade Policy Programme 2030. This roadmap sets a target for over 90% of SMEs to achieve a "basic level" of digital intensity by 2030.

- Under the Digital Europe programme, Cypriot SMEs have access to digital skills training and improved data infrastructure. The Digital Innovation Hub Cyprus, funded through this programme, functions as a centralised resource for SMEs seeking digitalisation support. The Hub offers services including trial platforms for new digital applications and training programmes to enhance digital competencies.

- In Cyprus_tomorrow, the country's recovery and resilience plan approved in 2021 as part of the European Union's Next Generation EU economic recovery package, includes targeted initiatives for SMEs. One such initiative is a scheme supporting the modernisation and digitalisation of agricultural enterprises. This scheme provides financial grants to SMEs involved in the manufacturing and trading of agricultural products for digital upgrading and process digitalisation activities.

- In 2022, Cyprus further launched the 'Digital Upgrade of Enterprises' programme, partially funded by the recovery and resilience plan. This programme offers operational assistance and financial support to SMEs for digital upgrades and investments in e-commerce or advanced digital technologies.

- As residents of the European Union, Cypriot SMEs and minority-owned businesses can access various EU-wide programmes aimed at enhancing competitiveness in the digital economy. These include financial support schemes, digital skills programmes for entrepreneurs, and regulatory support initiatives.

# SOURCES

- Digital Strategy for Cyprus 2020-2025
- National Digital Decade Strategic Roadmap
- European Union Digital Decade Policy Programme 2030
- Cyprus_tomorrow - National Recovery and Resilience Plan
- European Commission: Scheme for modernisation and digitalisation of enterprises engaged in manufacturing and trading of agricultural products (Investment 6 [C3.1I6])
- Thalia Scheme for Businesses Digital Upgrade
- Digital Innovation Hub Cyprus

# 02
# Digital Economy Factsheet

# Digital Economy Factsheet

This factsheet describes Cyprus's digital economy across four key dimensions: digital economy size and activities, digital infrastructure and connectivity, digital skills, and digital government.

# Size and Activities of the Digital Economy

To describe the size and activities of Cyprus's digital economy, we used data provided by the World Trade Organization and conducted our own calculations. We specifically analyzed the share of advanced technology products in total trade, cross-border trade in telecommunications, computer, information and audiovisual services, and total digitally delivered services.

Advanced technology products accounted for 11.31% of Cyprus's imports. The share of advanced technology products in exports was higher at 13.36%, indicating a relatively balanced technology trade.

**Figure 1:**

Telecommunications, Computer, Information and Audiovisual Services

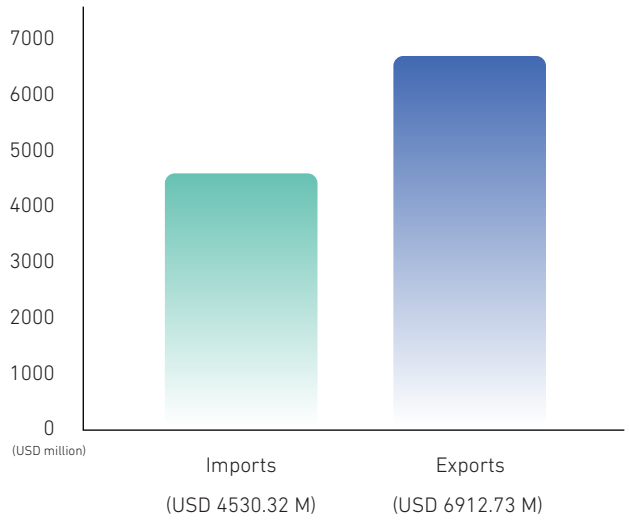



*Figure 1 provides data for Cyprus's telecommunications, computer, information, and audiovisual services in 2022.*

**Figure 2:**

Digital Delivered Services

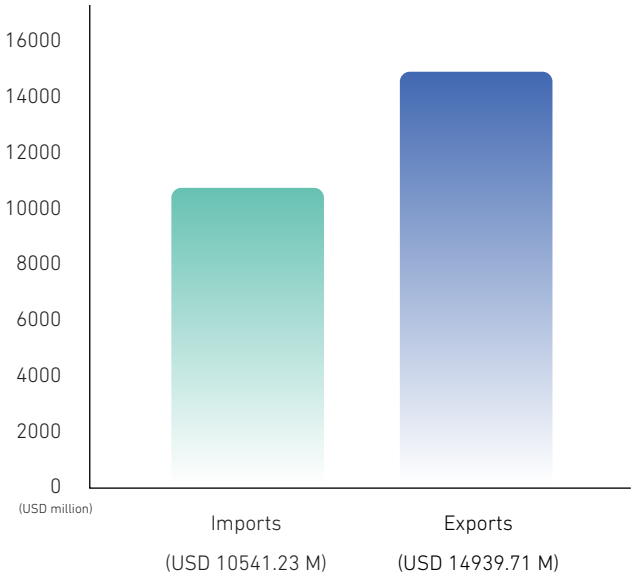



*Figure 2 provides data for the total digitally delivered services in 2023.*

# Digital Infrastructure and Connectivity (2022)

To analyze Cyprus's digital infrastructure and connectivity, we analyzed data provided by the International Telecommunications Union. We focused on internet access, broadband coverage, and traffic, as well as mobile phone ownership.

**Figure 3:**
Digital Infrastructure and Connectivity

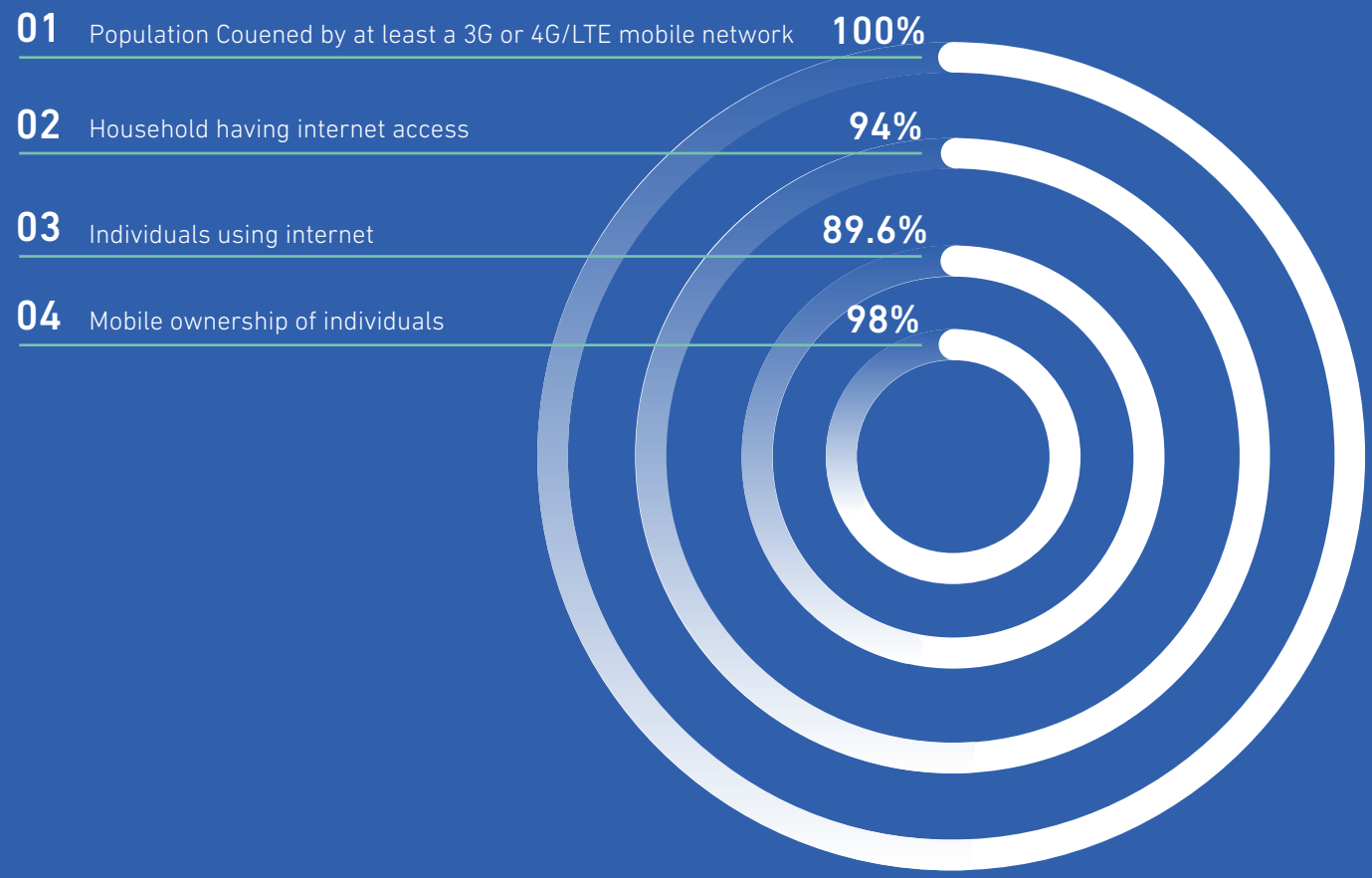



*Figure 3 provides data to analyze Bahrain's digital infrastructure and connectivity in 2022.*

# Digital Skills

To document Cyprus's digital skills, we draw on data by UNESCO. We use data points relevant to digital skills, beginning with general education and moving to specific digital skills.

The upper secondary education completion rate in Cyprus was 88.66% in 2021. Gross tertiary education enrollment ratio stood at 98.30% in 2022, indicating very high participation in higher education. The adult literacy rate was 99.36% in 2021. Government expenditure on education as a percentage of GDP was 5.24% in 2021.

**The proportion of youth and adults with basic digital skills in Cyprus showed relatively high competency levels:**

**47.92%**
were able to copy or move a file or folder (2019).

**27.04%**
had created electronic presentations with presentation software (2019).

**43.88%**
could find, download, install and configure software (2019).

# Digital Government

To examine the state of digital government in Cyprus, we rely on the World Bank's GovTech dataset. Specifically, we analyze how Cyprus provides digital government services, establishes institutions, and drafts strategies.

In terms of digital government services in 2022, Cyprus had only a cloud strategy/policy with no platform yet. It had implemented a government interoperability framework. It did not have a government open-source software policy or action plan. Cyprus did not maintain an open government portal but did have an open data portal.

Regarding institutional frameworks for digital government in 2022, Cyprus had established a government entity focused on government technology or digital transformation. It had planned or had in progress a government entity focused on public sector innovation. Cyprus had institutionalized a whole-of-government approach to public sector digital transformation.

**Finally, Cyprus had drafted various strategies to advance digital government in 2022:**

01 It had a current government technology or digital transformation strategy

02 It had both a strategy and program to improve digital skills in the public sector

03 It had both a strategy and program to improve public sector innovation

# 03 International Commitments and Collaboration

# International Commitments and Collaboration

The purpose of this section is to outline the existing international commitments of the member state and the international fora in which it engages. We focus on international commitments and collaboration with a digital component, meaning a connection to the pertinent policy areas explained above.

To outline international commitments, we analyse binding free trade agreements and conventions, as well as non-binding guidelines/recommendations/principles and model laws. We also reference other commitments, both binding and non-binding. For each commitment, we explain to which policy area(s) it is pertinent. Regarding international fora, we analyse participation in discussions at the pluri- and multilateral level.

# Commitments

## Free Trade Agreements

Cyprus has not signed any free trade agreements, which include provisions related to digital trade.

## Conventions

**Cyprus is party to the following conventions and agreements:**

01 International Covenant on Civil and Political Rights (Data Protection)

02 Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185) (Cybersecurity)

03 Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) (Cybersecurity)

04 Council of Europe Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS No. 224) (Cybersecurity)

05 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Data Protection)

06 Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) (Data Protection)

07 Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181) (Data Protection)

08 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Artificial Intelligence)

09 G20/Organisation for Economic Co-operation and Development Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (Taxation)

10 Berne Convention for the Protection of Literary and Artistic Works (Source Code)

## Guidelines, Recommendations, and Principles

**Cyprus is a member state of the United Nations, which has adopted the following frameworks:**

01 United Nations Guidelines for Consumer Protection (Online Consumer Protection)

02 United Nations Educational, Scientific and Cultural Organization Recommendation on the Ethics of Artificial Intelligence (Artificial Intelligence)

**Cyprus is a member state of the European Union that participates in the Group of 20 countries (G20), which has adopted the following frameworks:**

01 G20/Organisation for Economic Co-operation and Development High-Level Principles on SME Financing (SMEs and Digital Inclusion)

02 G20 Artificial Intelligence Principles (G20 Ministerial Statement on Trade and Digital Economy, 2019) (Artificial Intelligence)

## Models

**Cyprus has adopted or been influenced by the following model frameworks:**

01 - Commonwealth Model Law on Computer and Computer Related Crime (Cybersecurity)

02 - Commonwealth Model Provisions on Data Protection (Data Protection)

## Other commitments

- Cyprus is a member of the World Trade Organization and as such is subject to the Moratorium on Customs Duties on Electronic Transmissions (Customs Duties), the Trade Facilitation Agreement (Trade Facilitation) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (Source Code). In addition, Cyprus is a participant in the Joint Statement Initiative which has finalised a stabilised text on the Agreement on Electronic Commerce on 26 July 2024.

- Cyprus is a member state of the European Union that participates in the Global Partnership on Artificial Intelligence. (Artificial Intelligence)

- Additionally, Cyprus is a member state of the European Union that participates in the Hiroshima AI Process Friends Group (Artificial Intelligence).

**Cyprus is a member of the International Organization for Standardization, which has issued various technical standards including:**

- ISO/IEC 22989:2022 (Information technology — Artificial intelligence — Artificial intelligence concepts and terminology) (Artificial Intelligence)
- ISO/IEC 42001:2023 (Information technology — Artificial intelligence — Management system) (Artificial Intelligence)
- ISO 22376:2023 (Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal data format for authentication, verification and acquisition of data carried by a document or object) (Cybersecurity)
- ISO 31700-1:2023 (Consumer protection — Privacy by design for consumer goods and services) (Consumer protection)
- ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity)
- ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)
- ISO 23195:2021 (Security objectives of information systems of third-party payment services) (Electronic payments)
- ISO 32111:2023 (Transaction assurance in E-commerce — Principles and framework) (Electronic transactions)

# Fora

**Cyprus participates in the following international fora that touch upon digital issues:**

- United Nations Global Digital Compact (Cross-cutting)


@dcorg | www.dco.org